Министерство образования и науки Российской Федерации
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Сборник
трудов

II Всероссийская научно-техническая конференция

ПРОБЛЕМА КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СОВЕРШЕНСТВОВАНИЕ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ СИЛОВЫХ СТРУКТУР

Санкт-Петербург, 2011

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

6–8 октября 2011 г.

МЕЖВУЗОВСКИЙ СБОРНИК ТРУДОВ

II Всероссийская научно-техническая конференция

ПРОБЛЕМА КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
И СОВЕРШЕНСТВОВАНИЕ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ
ПОДГОТОВКИ СПЕЦИАЛИСТОВ СИЛОВЫХ СТРУКТУР

Санкт-Петербург
2011

Проблема комплексного обеспечения информационной безопасности и совершенствование образовательных технологий подготовки специалистов силовых структур. Межвузовский сборник трудов II Всероссийской научно-технической конференции ИКВО НИУ ИТМО / Под редакцией Жигулина Г.П., Будько М.Б. – СПб : НИУ ИТМО, 2011. – 222 с.

Конференция проводилась 6–8 октября в целях ознакомления научной общественности и представителей предприятий и организаций с результатами научно-исследовательских работ (проводимых, в том числе, в содружестве с предприятиями и организациями Санкт-Петербурга) и научными достижениями в области обеспечения информационной безопасности и совершенствования образовательных технологий подготовки специалистов силовых структур, а также в целях обмена мнениями и опытом для повышения эффективности научно-исследовательской деятельности и качества подготовки бакалавров и магистров НИУ ИТМО по заявленному направлению (090900 Информационная безопасность).

Сайт конференции: http://confib.ifmo.ru/.

Рекомендовано к печати Ученым советом факультета Институт комплексного военного образования (ИКВО) НИУ ИТМО, протокол №1 от 30 января 2012 г.

По всем организационным вопросам обращаться в Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики: 197101, Санкт-Петербург, пр. Кронверкский, д. 49, факультет ИКВО, оргкомитет конференции «Проблема комплексного обеспечения информационной безопасности и совершенствование образовательных технологий подготовки специалистов силовых структур».

E-mail: ikvo@grv.ifmo.ru.

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики».

СТРУКТУРА

Сборник включает 52 статьи и разделен на три тематические секции.

Секция А. Информационная безопасность, моделирование и прогнозирование информационных угроз.
Председатель: Жигулин Г.П.

Секция В. Пути совершенствования эксплуатации вооружения и военной техники.
Председатель: Глотов И.В.

Секция С. Совершенствование образования технической подготовки специалистов в области обороны.
Председатель: Гончаров А.Д.

Статьи упорядочены по фамилиям авторов в рамках каждой секции. Перечисление соавторов – также в алфавитном порядке.

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ КОНФЕРЕНЦИИ

Жигулин Г.П. – декан ИКВО;

Прожерин В.Г. – заведующий базовой кафедрой ИТЗИ;

Хромов И.Н. – заведующий базовой кафедрой СПЗИ;

Бутин М.Д. – студент кафедры МиПИУ;

Гиллунг А.И. – студент кафедры МиПИУ;

Исаев А.С. – студент кафедры МиПИУ;

Маковецкий А.В. – студент кафедры МиПИУ;

Павлова Ю.В. – студентка кафедры МиПИУ;

Цепелев С.Д. – студент кафедры МиПИУ.

ПРОГРАММНЫЙ КОМИТЕТ КОНФЕРЕНЦИИ

Васильев В.Н. – ректор Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики – *председатель*;

Жигулин Г.П. – декан факультета ИКВО – *зам. председателя*;

Иванов А.Ю. – проректор по УиВР;

Колесников Ю.Л. – проректор по УО и АР;

Никифоров В.О. – проректор по развитию;

Шалковский А.Г. – проректор по работе с оборонно-промышленным комплексом;

Шехонин А.А. – проректор по УМР;

Бардаев Э.А. – заместитель начальника 8-го управления ГШ ВС РФ;

Глотов И.В. – начальник военной кафедры;

Гончаров А.Д. – заместитель начальника военной кафедры;

Прожерин В.Г. – заведующий базовой кафедрой ИТЗИ;

Репин Г.А. – заместитель генерального директора ФГУП «НПП «Сигнал» – начальник КБ СП;

Сарычев В.А. – заместитель генерального директора ОАО «НПП Радар-ммс» по науке, куратор базовой кафедры Бортовых приборов вооружения и военной техники;

Хромов И.Н. – заведующий базовой кафедрой СПЗИ;

Ивановский Р.И. – профессор кафедры МиПИУ;

Будько М.Б. – доцент кафедры МиПИУ;

Будько М.Ю. – доцент кафедры МиПИУ;

Бузинов А.С. – доцент кафедры МиПИУ;

Гирик А.В. – доцент кафедры МиПИУ;

Серебров А.И. – доцент кафедры МиПИУ;

Яковлев А.Д. – доцент кафедры МиПИУ.

РЕДАКЦИОННАЯ КОМИССИЯ

Жигулин Г.П. – декан ИКВО;

Гончаров А.Д. – заместитель начальника военной кафедры;

Глотов И.В. – начальник военной кафедры;

Прожерин В.Г. – заведующий базовой кафедрой ИТЗИ;

Хромов И.Н. – заведующий базовой кафедрой СПЗИ;

Будько М.Б. – доцент кафедры МИПИУ;

Гатченко Н.А. – студент кафедры МиПИУ;

Гиллунг А.И. – студент кафедры МиПИУ;

Исаев А.С. – студент кафедры МиПИУ;

Цепелев С.Д. – студент кафедры МиПИУ.

СОДЕРЖАНИЕ

Секция А. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, МОДЕЛИРОВАНИЕ И ПРОГНОЗИРОВАНИЕ ИНФОРМАЦИОННЫХ УГРОЗ

Секция В. ПУТИ СОВЕРШЕНСТВОВАНИЯ ЭКСПЛУАТАЦИИ ВООРУЖЕНИЯ И ВОЕННОЙ ТЕХНИКИ

Секция С. СОВЕРШЕНСТВОВАНИЕ ОБРАЗОВАНИЯ ТЕХНИЧЕСКОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ОБОРОНЫ

Секция А. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, МОДЕЛИРОВАНИЕ И ПРОГНОЗИРОВАНИЕ ИНФОРМАЦИОННЫХ УГРОЗ

УДК 004.9

ЗАКЛЮЧИТЕЛЬНЫЕ ЭТАПЫ ПРОГНОЗИРОВАНИЯ НА ОСНОВЕ ТРЕНД-СЕЗОННОЙ МОДЕЛИ – ИНТЕРВАЛЬНОЕ ОЦЕНИВАНИЕ И ВЕРИФИКАЦИЯ

Будько М.Б., Будько М.Ю.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В настоящее время прогнозирование используется в различных областях науки и практики. Одной из таких областей, которая немыслима без прогнозирования, является информационная безопасность.

Навык выполнения научно обоснованного прогноза является обязательным умением студентов, обучающихся по настоящему направлению. Известно, что при составлении прогноза на основе тренд-сезонных моделей методом экстраполяции (продолжения динамики) основными являются следующие этапы: предварительный анализ данных (анализ грубых погрешностей); формирование набора моделей, оценка их адекватности и точности, выбор наилучшей по заранее заданным критериям, собственно составление прогноза (точечного и интервального) и его верификация.

В докладе акцентируется внимание на таких неотъемлемых этапах как интервальное прогнозирование и верификация.

Доклад носит информационный характер. Его целью является показать, что при составлении прогноза завершающие этапы являются не менее ответственными, нежели построение «качественной» модели исследуемого ряда и продолжение этой динамики в будущее.

Так, например, формулы расчета доверительного интервала для линейных и разных нелинейных трендовых моделей различны, но каждая из них предполагает увеличение неопределенности прогнозируемого процесса с ростом периода упреждения, которая проявляется в постоянном расширении доверительного интервала. Немаловажным является выбор значения уверенности для расчета доверительного интервала прогноза.

Верификация модели представляет собой набор критериев оценки качества получаемого прогноза. Здесь затрагиваются, например, такие понятия как: точность прогноза (выявляемая на основе прогнозирования уже существующих ретроспективных данных по более ранним элементам ряда), качество прогноза (наиболее простой мерой которого является отношение

числа случаев, при которых интервальный прогноз покрывал фактическое значение, к общему числу прогнозов).

Внимание уделяется еще одному важному моменту: сам факт наличия прогноза способен оказывать значительное влияние на будущее. Имея прогноз, организация или отдельная личность посредством своих действий или бездействия могут поддерживать сложившуюся тенденцию для осуществления прогноза или изменять ее для неосуществления. Именно поэтому для придания большего приоритета последним тенденциям в прогнозировании используются адаптивные модели.

УДК 004.056.53

БЕЗОПАСНОСТЬ СУБД

Бушманова А.В.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Научный руководитель – к.т.н., доц. Жигулин Г.П.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В статье рассматриваются уязвимости безопасности баз данных Oracle 9i, 10g. Предлагаются предложений для повышения конфиденциальности и целостности баз данных. Статья представляет интерес для всех, кто работает с базами данных.

Ключевые слова: безопасность баз данных, уязвимости Oracle 9i и 10g, целостность, конфиденциальность данных.

На сегодняшний день все больше технологий используют в своей основе различные базы данных и компании сталкиваются с проблемой защиты информации, хранящейся в них. В данной статье проанализированы наиболее критичные уязвимые места на примере систем, построенных на базе данных Oracle.

База данных Oracle – одна из распространенных в корпоративной среде систем, поэтому она и была выбрана в качестве примера, а точнее, версии OracleDatabase 9i и 10g.

Уязвимости сетевого взаимодействия

Удаленный доступ к базе данных предоставляет сервис Oracle TNS Listener (по умолчанию порт 1521). Листенер принимает клиентские запросы на соединение и направляет их для обработки в соответствующий серверный процесс. Обычно Листенер рассматривается как первый этап на пути вторжения в базы данных. Плохо сконфигурированный незащищенный Листенер подвержен различным атакам, включая удаленное выполнение команд и отказ в обслуживании. В версии Oracle ниже 10g по умолчанию возможно осуществление анонимного подключения и, как следствие, удаленное управление сервисом.

В дефолтной конфигурации злоумышленник может:

– получить детальную информацию об атакуемой системе(SID, версия СУБД, путь к log-файлам, операционная система, на которой установлена СУБД);
– произвести DoS-атаку;
– выполнять SQL-команды от имени DBA;
– получить удаленный доступ к системе.

Для подключения к Листенеру применяется стандартная утилита lsnrctl, входящая в набор тулз, устанавливаемых с клиентом для СУБД Oracle. Для получения информации используется команда status.

DoS-атака может быть осуществлена с помощью утилиты lsnrctl. Командой stop удаленный неавторизированный пользователь может остановить TNS Listener. (Начиная с версии 10g, по умолчанию, администратор не может управлять прослушивателем удалено, пока отключена аутентификация на локальном уровне операционной системы).

Обеспечение защиты прослушивателя в Oracle 9i, 10g и выше

В связи с изменениями в Oracle 10g и появлением локальной аутентификации установка пароля прослушивателя и установка ADMIN_RESTRICTIONS не являются обязательными. Если же требуется максимальная безопасность, то пароль и ADMIN_RESTRICTIONS устанавливаются.

– установка пароля прослушивателя. Эта мера является обязательной и позволит остановить большинство попыток атак. Обычно это простой процесс, вам требуется установить пароль в lsnrctl, который будет хранится в файле listener.ora в зашифрованном виде, или установить параметр PASSWORDS_, тогда пароль будет хранится в открытом виде;
– установка ADMIN_RESTRICTIONS. Действие является обязательным, и позволяет запретить любые изменения прослушивателя во dремя работы. Достигается установкой параметра ADMIN_RESTRICTIONS_ в значение ON в файле listener.ora;
– установка обновлений и исправлений. Это позволит избежать ряда проблем и закрыть уязвимые места;
– использование брандмауэров. Настройка межсетевых экранов таким образом, что бы пропускать только трафик от известных приложений и серверов, блокируя все постороннее и незнакомое;
– защита директории $TNS_ADMIN. Эта мера является обязательной. Пароль прослушивателя хранится в файле listener.ora. Легким редактированием файла можно убрать парольную защиту. Если же пароль добавлялся вручную, то он хранится в открытом виде. Если средствами lsnrctl, то в виде зашифрованной строки. Разрешения на файлы listener.ora, sqlnet.ora и protocol.ora в директории $TNS_ADMIN (обычно $ORACLE_HOME/network/admin) должны быть чтение/запись/исполнение только для учетной записи владельца oracle;
– защита tnslsnr и lsnrctl. Эта мера призвана ограничить разрешения на исполняемые файлы tnslsnr и lsnrctl;
– изменение порта TNS. Смена номера порта с 1521, который используется по умолчанию, на номер из диапазона 1521–1550 и 1600–1699, позволит обойти некоторые автоматические атаки и заставить злоумышленника потратить время на определение порта;
– установка проверки узлов. Зависит от типа приложения и конфигурации сети и может быть мощным средством по ограничению трафика. Большинство web приложений требуют

доступа с серверов приложений и только несколько клиентов для администрирования. Следовательно можно ограничить доступ по IP адресу;

– регулярная проверка журнала прослушивателя По умолчанию журналирование отключено, параметр LOG_STATUS=OFF. Когда журналирование включено, директория по умолчанию $ORACLE_HOME/network/admin, и журнальный файл называется .log. Журнал содержит историю команд прослушивателя, выполненных локально и удаленно. Регулярный мониторинг журнала прослушивателя на наличие ошибок TNS-01169, TNS-01189, TNS-01190 или TNS-12508 поможет обнаружить потенциальную угрозу и попытки проникновения.

Подключение к СУБД

Для подключения к СУБД кроме имени и пароля необходимо знать имя базы данных (SID). Незащищенный Листенер по умолчанию выдает имена баз данных без аутентификации. Достаточно воспользоваться утилитой lsntctl с опцией services.

На случай если на Листенер установлен пароль или включена опция LOCAL_OS_AUTHENTICATION, существует множество способов получения имени базы данных.

Вот наиболее распространенные:

1) поиск информации в сторонних приложениях:

– например, СУБД Oracle 10g R2 по умолчанию устанавливает OracleApplicationServer, который работает на порту 1158. Этот сервер доступен для удаленного подключения и выдает вместе с окном ввода логина и SID базы данных;

– при установке Oracle в связке с системой SAP/R3 узнать SID базы данных можно, подключившись к приложению SAP web-management, обычно висящему на порту 8001/TCP и отвечающему за управление системой SAP. На запрос несуществующего файла, сервер выдает страницу ошибки, на которой содержится SID базы данных;

2) имя базы данных является стандартным, словарным или частично/полностью совпадает с DNS/NETBIOS-именем хоста, например ORCL;

3) имя базы данных состоит из малого количества символов;

4) имя базы данных можно узнать по ссылке из другой базы данных, из файла tnsnames.ora на взломанном хосте, а также, например, прослушивая сетевой трафик.

Уязвимости учетных записей

Получив SID базы данных, мы можем пытаться подобрать пароли учетных записей пользователей. СУБД Oracle при установке создает множество системных учетных записей со стандартными паролями, и обычно администраторы забывают отключать или хотя бы менять пароли. Список стандартных аккаунтов насчитывает порядка 600 имен и доступен в интернете (http://www.petefinnigan.com/default/default_password_list.htm или утилита oscanner http://www.cqure.net/tools/oscanner_bin_1_0_6.zip), например, приводятся такие пары идентификатор/пароль, как system/manager, Scott/Tiger, internal/oraclesys/change_on_install.

Поэтому настоятельно рекомендуется использовать длинные пароли, вперемешку с цифрами и специальными символами, что позволит существенно усложнить атаку перебором или по словарю.

Есть несколько моментов, благодаря которым перебор паролей в СУБД Oracle приносит успех:

1) многие системные имена пользователей известны, что позволяет подбирать только пароли;

2) по умолчанию ограничений на длину и сложность пароля не установлено;

3) перебор паролей к учетным записям не блокируется;

4) базы данных обычно содержат много учетных записей, а нам достаточно подобрать хотя бы одну (не обязательно административную);

5) кроме того, все пароли учетных записей для СУБД Oracle хранятся в файле orapwXXX (для UNIX) или pwdXXX.ora (для Windows), где XXX – это SID. И хотя в этом файле хранятся зашифрованные значения паролей учетных записей, они могут быть подвергнуты атаке BruteForce, позволяющей подобрать правильное значение пароля. Мало того, одно неизвестное зашифрованное значение пароля может быть заменено на другое зашифрованное, но известное значение, что откроет дорогу злоумышленнику к базе данных.

Переполнение буфера

Переполнение буфера (bufferoverflow) – наверное, одна из самых интересных и широко распространенных уязвимостей. Ошибка заключается в том, что в каком-либо месте программы происходит копирование данных из одного участка памяти в другой без проверки того, достаточно ли для них места там, куда их копируют. Область памяти, куда копируются данные, принято называть буфером. Таким образом, если данных слишком много, то часть их попадает за границы буфера – происходит «переполнение буфера». Умелое использование того, куда попадают «лишние данные» может позволить злоумышленнику выполнить любой «свой» код.

Повышение уровня привилегий

Обычно для повышения привилегий используют уязвимости класса SQL-injection во встроенных процедурах СУБД Oracle.

Поскольку многие из этих процедур выполняются от имени их владельца, которым является пользователь SYS, то, внедрив свой код, мы сможем выполнять произвольные действия от имени системного пользователя.

Рекомендации по повышению уровня защищенности Oracle:

1) Установить пароль на доступ к сервису TNS Listener.

2) Включить протоколирование подключения к Листенеру для обнаружения попыток перебора паролей.

3) Не используй словарные, легко угадываемые SID-имена.

4) Ограничь доступ к системам, через которые можно узнать SID.

5) Проведи аудит используемых учетных записей: удалить или отключить неиспользуемые учетные записи и сменить стандартные пароли системных учетных записей.

6) Внедрить корпоративную парольную политику в СУБД.

7) Установить последние критические обновления и ограничь доступ пользователей на запуск потенциально опасных процедур.

8) Проанализировать привилегии и роли пользователей, руководствуясь принципом наименьших привилегий.

9) Если возможно, отключить возможности доступа пользователей Oracle к файловой системе.

10) Ограничьте доступ к СУБД Oracle по IP-адресам, разрешив доступ только с веб-сервера, если база данных используется в связке с веб-сервером, или только с подсети пользователей СУБД.

11) Эти действия помогут наиболее полно защитить СУБД без использования дополнительных программно-аппаратных средств, позволяющих избежать неожиданных хакерских нападений.

Литература

1. Нокс Д. Создание эффективной системы безопасности для OracleDatabase 10g. – М. : «Символ», 2007. – 556 с.

2. Oracle: Статьи – Безопасность [Электронный ресурс]. – Режим доступа: http://www.all–oracle.ru/content/view/?part=1&section=14 (дата обращения 11.07.2011).

3. Кайт Т. Oracle для профессионалов: архитектура, методики программирования и особенности версий 9i, 10g и 11g. 2-е издание. – М. : «Вильямс», 2011. – 848 с.

УДК 004.371

АНАЛИЗ МЕТОДИК ОЦЕНКИ ЗАТРАТ НА СОЗДАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Войтик А.И., Прожерин В.Г.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В первое десятилетие XXI века значение информации многократно возросло, информация приобрела огромную ценность не только с точки зрения государственной таны, но и в коммерческом плане, сокращение времени на проектирование, жесткая конкуренция на рынке IT технологий, многократное увеличение продукции на рынке телекоммуникационных систем и устройств увеличило риск выпуска «неконкурентной» продукции, желание заглянуть, «а что там разрабатывается у соседей», привело к широкомасштабному проникновению в бизнес систем и методик, заимствованных из военных структур.

Зачастую технологии на «гражданском» рынке опережают и военные разработки. Соответственно каждая самостоятельная фирма стремиться обезопасить себя от «нежелательных наблюдателей». И здесь возникает проблема, как рассчитать стоимость затрат на безопасность? Где та золотая середина между финансовыми потерями от недостаточной информационной защищенности организации и банкротства от чрезмерного удорожания систем и средств защиты?

Решению этой проблемы экономистами уделяется огромное значение. Предложено большое количество методик и разработок для расчета стоимостных показателей

информационной безопасности. Как правило, они сводятся к трем основным направлениям: определения степени значимости (секретности) той или иной информации, исходя из требования законодательных документов и, или решения руководства фирмы и установление соответственно определенных весов тем или иным угрозам. При этом в описаниях угроз ИБ и программных средствах их оценки, широко представленных на рынке зарубежными и отечественными разработчиками, используются классификации и алгоритмы, основанные на распространенных в методиках, стандартах и руководящих документах, имеющие, как правило, отраслевой или законодательный «крен» и напрасно не отражающие специфику угроз верхнего уровня ИБ.

Сложность задач экономического анализа практически во всех областях деятельности, обуславливается тем, что многие ключевые параметры экономических моделей не возможно достоверно оценить, т.к. они носят вероятностный характер. Необходимо также учитывать то обстоятельство, что сам по себе такой анализ может оказаться достаточно ресурсоемкой процедурой и потребовать привлечения дополнительных специалистов и сторонних консультантов, а также усилий со стороны различных специалистов, работающих на самом предприятии, – все эти затраты, в конечном счете, должны быть оправданы.

В процессе текущей деятельности предприятиям постоянно приходится сталкиваться с теми или иными изменениями: уточняются бизнес-процессы, меняется конъюнктура рынков сбыта и рынков потребляемых материальных ресурсов и услуг, появляются новые технологии и т.д. В этих условиях управленцам приходится постоянно анализировать происходящие изменения и адаптировать свою работу к постоянно меняющейся ситуации. Однако при всем разнообразии возможных моделей поведения в меняющейся среде, почти все их объединяет один важный общий методологический элемент: в большинстве случаев реакция бизнеса на новые угрозы и новые возможности предполагает осуществление новых инвестиций в определенные организационные и/или технические мероприятия.

Таким образом, в ситуации, когда необходимо осуществить некоторые новые организационные или технические мероприятия, основной задачей лиц, отвечающих за эффективную организацию ИБ, является четкое соотнесение затрат, которые придется понести в связи с реализацией этого мероприятия, и дополнительных денежных потоков, которые будут получены. В данном случае под денежным потоком может пониматься экономия затрат, предотвращение убытков, а также дополнительный доход предприятия.

Рассмотрим различные методики оценки экономической эффективности от внедрения систем защиты информации.

Одной из первых рассмотрим базовую методологию “Total Cost of Ownership” (TCO).

Эта методика ориентирована на обеспечение полноты анализа издержек, связанных с ИТ и ИС, в ситуациях, когда необходимо оценить экономические последствия внедрения и использования таких систем.

В общем случае суммарная величина TCO включает в себя затраты на:

- проектирование информационной системы;
- приобретение аппаратных и программных средств;
- разработку программного обеспечения и его документирование, а также на исправление ошибок и доработку в течение периода эксплуатации;

- текущее администрирование информационных систем;
- техническую поддержку и сервисное обслуживание;
- расходные материалы;
- телекоммуникационные услуги;
- затраты на обучение;
- издержки, связанные с потерей времени пользователями в случае сбоев в работе информационных систем.

Также в расчет затрат на повышение уровня ИБ необходимо включить расходы на реорганизацию бизнес-процессов и информационную работу с персоналом. Кроме того, при анализе расходов необходимо также учесть, что в большинстве случаев внедрение средств защиты информации предполагает появление дополнительных обязанностей у персонала предприятия и необходимость осуществления дополнительных операций при работе с информационными системами. Значение ТСО в каждом конкретном случае необходимо определять индивидуально с учетом особенностей проекта, который предстоит реализовать: основной востребованной функциональности, существующей инфраструктуры, количества пользователей и других факторов. В общем случае данной методикой могут быть определены затраты, связанные с реализацией мероприятий по обеспечению информационной безопасности. Однако наибольшую сложность представляет определение положительного эффекта от внедрения средств защиты информации. Как правило, эффект от внедрения ИС определяется тем, что они обеспечивают автоматизацию и ускорение различных бизнес-операций, что позволяет сократить затраты труда, приобрести конкурентные преимущества и, таким образом, повысить общую эффективность хозяйственной деятельности. Однако внедрение средств защиты информации само по себе, не обеспечивает сокращения затрат – достижение положительного эффекта от их использования зависит от множества трудно контролируемых факторов как внутри предприятия, так и вне его. Более того, реализация мероприятий, связанных с обеспечением ИБ, может привести к дополнительным нагрузкам на персонал предприятия и, соответственно, к снижению производительности труда. Одним из немногих способов, который может помочь предприятию определить эффект от осуществления мероприятий в сфере защиты информации, является денежная оценка того ущерба, который может быть нанесен информационным ресурсам предприятия, и который может быть предотвращен в результате реализации предлагаемых мероприятий. Таким образом, предполагаемый предотвращенный ущерб и будет составлять полученный экономический эффект или дополнительный денежный поток. При таком подходе большинство расчетов могут быть только оценочными и носить приблизительный характер. Это связано с тем, что активность злоумышленников, являющихся источниками угроз для ИБ, практически не предсказуема: невозможно достоверно предсказать стратегии нападения, квалификацию нападающих, их конкретные намерения и ресурсы, которые будут задействованы для совершения тех или иных действий, а также намерения в отношении украденной информации. Соответственно, для осуществления всех необходимых расчетов необходимо сделать множество допущений и экспертных оценок в контексте деятельности данного конкретного предприятия, а также по возможности изучить статистическую информацию, касающуюся атак на информационные ресурсы, аналогичные защищаемым. Таким образом, экономическая оценка эффективности мер по защите информации предполагает:

– оценку существующих угроз для информационных активов, которых коснется реализация защитных мер;
– оценку вероятности реализации каждой из выявленных угроз;
– экономическую оценку последствий реализации угроз.

Для осуществления такого анализа, как правило, используются следующие базовые понятия:

– оценочная величина единовременных потерь (Single Loss Expectancy, SLEi) – предполагаемая средняя оценочная сумма ущерба в результате одного нарушения информационной безопасности *i*-го типа. Она может быть определена как произведение общей стоимости защищаемых информационного активов AV (Active Value) на коэффициент их разрушения вследствие нарушения информационной безопасности EFi (Exposure Factor);
– количество нарушений информационной безопасности за год (Annualized Rate of Occurrence, AROi) – оценочная частота, с которой в течение года происходят нарушения информационной безопасности *i*-го типа;
– оценочная величина среднегодовых потерь (Annualized Loss Expectancy, ALEi) – суммарный размер потерь от нарушений информационной безопасности (реализации рисков) *i*-го типа в течение года.

На основе этих данных может быть определен суммарный эффект от реализации мероприятий в сфере информационной безопасности и продемонстрировано, насколько оправданными и целесообразными являются вложения в те или иные средства защиты информации в условиях конкретного предприятия с учетом всех особенностей его функционирования.

Несмотря на все трудности процесса оценки целесообразности внедрения средств защиты, описанная методология позволяет получать обоснованные оценки и делать формализованные выводы относительно того, насколько оправданными являются вложения в определенные средства защиты информации, а также определить основные приоритеты расходования средств, предусмотренных в бюджете на обеспечение информационной безопасности.

Исходя из этой методики одной из основных задач руководителей, отвечающих за принятие решений в сфере информационной безопасности, является подбор наиболее квалифицированных и опытных специалистов, поскольку от качества их работы будет зависеть не просто безопасность отдельных элементов информационных активов в определенные моменты времени, а эффективность всей системы защиты информации в среднесрочной, а иногда и в долгосрочной перспективе.

Оценка ИБ заключается в выработке оценочного суждения относительно пригодности (зрелости) процессов обеспечения ИБ, адекватности используемых защитных мер или целесообразности (достаточности) инвестиций (затрат) для обеспечения необходимого уровня ИБ на основе измерения и оценивания критических элементов (факторов) объекта оценки.

Наряду с важнейшим назначением оценки ИБ – создание информационной потребности для совершенствования ИБ, возможны и другие цели проведения оценки ИБ такие, как:

– определение степени соответствия установленным критериям отдельных областей обеспечения ИБ, процессов обеспечения ИБ, защитных мер;

– выявление влияния критических элементов (факторов) и их сочетания на ИБ организации;

– сравнение зрелости различных процессов обеспечения ИБ и сравнение степени соответствия различных защитных мер установленным требованиям.

Результаты оценки ИБ организации могут также использоваться заинтересованной стороной для сравнения уровня ИБ организаций с одинаковым бизнесом и сопоставимым масштабом.

Способ оценки ИБ по эталону сводится к сравнению деятельности и мер по обеспечению ИБ организации с требованиями, закрепленными в эталоне. По сути дела проводится оценка соответствия СОИБ организации установленному эталону. Под оценкой соответствия ИБ организации установленным критериям понимается деятельность, связанная с прямым или косвенным определением выполнения или невыполнения соответствующих требований ИБ в организации. С помощью оценки соответствия ИБ измеряется правильность реализации процессов системы обеспечения ИБ организации и идентифицируются недостатки такой реализации.

В результате проведения оценки ИБ должна быть сформирована оценка степени соответствия СОИБ эталону, в качестве которого могут быть приняты (в совокупности и отдельно):

– требования законодательства Российской Федерации в области ИБ;

– отраслевые требования по обеспечению ИБ;

– требования нормативных, методических и организационно-распорядительных документов по обеспечению ИБ;

– требования национальных и международных стандартов в области ИБ.

Основные этапы оценки информационной безопасности по эталону включают выбор эталона и формирование на его основе критериев оценки ИБ, сбор свидетельств оценки и измерение критических элементов (факторов) объекта оценки, формирование оценки ИБ.

Риск-ориентированная оценка ИБ организации представляет собой способ оценки, при котором рассматриваются риски ИБ, возникающие в информационной сфере организации, и сопоставляются существующие риски ИБ и принимаемые меры по их обработке. В результате должна быть сформирована оценка способности организации эффективно управлять рисками ИБ для достижения своих целей.

Основные этапы риск-ориентированной оценки информационной безопасности включают идентификацию рисков ИБ, определение адекватных процессов менеджмента рисков и ключевых индикаторов рисков ИБ, формирование на их основе критериев оценки ИБ, сбор свидетельств оценки и измерение риск-факторов, формирование оценки ИБ.

Способ оценки ИБ на основе экономических показателей оперирует понятными для бизнеса аргументами о необходимости обеспечения и совершенствования ИБ. Для проведения оценки в качестве критериев эффективности СОИБ используются, например, показатели совокупной стоимости владения (Total Cost of Ownership – TCO).

Под показателем TCO понимается сумма прямых и косвенных затрат на внедрение, эксплуатацию и сопровождение СОИБ. Под прямыми затратами понимаются все материальные затраты, такие как покупка оборудования и программного обеспечения, трудозатраты соответствующих категорий сотрудников. Косвенными являются все затраты на обслуживание

СОИБ, а также потери от произошедших инцидентов. Сбор и анализ статистики по структуре прямых и косвенных затрат проводится, как правило, в течение года. Полученные данные оцениваются по ряду критериев с показателями ТСО аналогичных организаций отрасли.

Оценка на основе показателя ТСО позволяет оценить затраты на информационную безопасность и сравнить ИБ организации с типовым профилем защиты, а также управлять затратами для достижения требуемого уровня защищенности.

Основные этапы оценки эффективности СОИБ на основе модели ТСО включают сбор данных о текущем уровне ТСО, анализ областей обеспечения ИБ, выбор сравнимой модели ТСО в качестве критерия оценки, сравнение показателей с критерием оценки, формирование оценки ИБ.

Однако этот способ оценки требует создания общей информационной базы данных об эффективности СОИБ организаций схожего бизнеса и постоянной поддержки базы данных в актуальном состоянии. Такое информационное взаимодействие организаций, как правило, не соответствует целям бизнеса. Поэтому оценка ИБ на основе показателя ТСО практически не применяется.

Модель оценки общей стоимости владения, используемая для информационных систем

Эта модель содержит ряд базовых компонентов: капитальные затраты, стоимость поддержки и администрирования информационной системы.

Капитальные затраты включают в себя расходы на приобретение и модернизацию аппаратного и программного обеспечения и определяются довольно просто.

Стоимость поддержки подсчитать значительно труднее, поскольку состоит она исключительно из трудозатрат. Для учета этих расходов нужно проанализировать сценарии поддержки: соответствующие процедуры управления, роли, обязанности, трудозатраты и оклады сотрудников, участвующих в обеспечении функционирования системы. Сюда нужно добавить и стоимость услуг сторонних организаций в тех случаях, когда организация не в состоянии справиться с задачами поддержки собственными силами. Необходимо учитывать также затраты на премии и другие поощрительные выплаты.

В категорию администрирования включаются расходы на управление ИТ-ресурсами, реализацию принятой политики и процедур использования информационных технологий. Кроме того, к этой категории относятся затраты на юридическую поддержку и аудит: оценку контрактов и ведение переговоров, проверку правильности функционирования системы, использования лицензий на программное обеспечение и др.

Следует заметить, что основные проблемы при анализе затрат обычно связаны с наличием видов деятельности, не вписывающихся ни в одну стоимостную категорию модели.

Модель ОСВ для системы информационной безопасности

Предлагаемая Gartner Group методика включает формирование учетных карт, содержащих перечень всех затратных компонентов системы ИБ. Учетные карты составляются для каждого из 29 видов деятельностей по обеспечению ИБ, указанных в методических рекомендациях Gartner, и включают расходы на аппаратное и программное обеспечение, персонал и внешние сервисы.

В данной модели определено понятие экономической эффективности, как категории, характеризующей результативность экономической системы, выражаемой в отношении качественно и количественно определенных экономических эффектов от ее применения к суммарным затратам на обеспечение ее функционирования. Это предопределило этапы определения в тех же единицах измерения получаемых и планируемых эффектов и этап их сопоставления. Таким образом предложен итеративный подход, позволяющий уточнять оценку экономической эффективности и на ее основе производить оптимизацию затрат, Анализ установил, что в качестве метода оценки затратной части проекта целесообразно использовать метод «совокупной стоимости владения» (ССВ), который позволяет достаточно полно оценить затраты, разделяя их по категориям. Как правило, при подсчете стоимости ССВ определение размера прямых затрат не представляет сложностей, в отличие от задачи по подсчету косвенных издержек, преимущественно через определение стоимостного эквивалента времени незапланированных простоев.

Помимо затрат на внедрение СИБ, в его процессе возникают побочные явления, такие как ущерб от простоя во время этапа пусконаладочных работ (DL1), потери от вывода финансовых активов из оборота (DL2), возможное снижение производительности оборудования, которое можно компенсировать его заменой или модернизацией, что тоже потребует затрат (DL3), ущерб от задержки восстановления работоспособности информационной инфраструктуры СК в случае вывода ее из строя в результате сетевой атаки, вирусной эпидемии (DL4) и т.п.

Несмотря на некоторые трудности применения в условиях современной России, методика ССВ позиционируется как инструмент комплексной оценки экономической эффективности мероприятий ИБ. В то же время она не позволяет проводить оценку тех выгод, которые составляют получаемый в строительстве от применения СИБ экономический эффект. По этой причине существует объективная необходимость уточнения и разработки адекватной целям исследования методики оценки экономических эффектов применения СИБ с дальнейшей оценкой ее экономической эффективности в рамках деятельности СК.

Так как финансовые ресурсы на обеспечение ИБ СК выделяются из прибыли, то целесообразно установить верхний предел этих затрат в виде доли от прибыли. Как показывает практика, средний нормативный показатель затрат на обеспечение ИБ коммерческой деятельности крупных компаний (ISC) находится в пределах 0,12–0,18 и определяется на основании принятой нормы приемлемого уровня рисков ИБ. Норма прибыли также задается руководством СК в виде показателя нормы прибыли PN. В строительной отрасли этот показатель имеет очень большой разброс значений в зависимости от региона, типа проектов, конъюнктуры спроса и предложения на рынке и множества прочих факторов.

Методика определения жизненного цикла использования информации

Для наиболее эффективного использования информации за время ее жизненного цикла, в течение которого она является актуальной, необходимо выбрать такой режим ее распространения, при котором эффект от использования информации с учетом позитивных и негативных последствий достигал бы максимальной величины. При таком подходе ограничение распространения информации на определенное время является одним из способов управления информационным ресурсом собственника в интересах достижения максимального эффекта от его использования.

Следует учитывать, что оценка позитивных и негативных последствий от ограничения распространения информации представляет значительные трудности. Эти последствия могут проявляться в различных сферах деятельности предприятия, оцениваться в различных шкалах и единицах измерения.

Для сопоставления сведений с точки зрения необходимости ограничения доступа к ним предлагается:

– оценить эти сведения по степени проявления всей совокупности угроз в случае их свободного распространения и возможных издержек (или упущенной выгоды) при ограничении доступа к ним;

– ранжировать или определить «веса» угроз, выгод и затрат с тем, чтобы получить единую меру, характеризующую интегральный эффект от ограничения распространения сведений (для решения этой задачи необходимо определить перечни возможных угроз от несанкционированного распространения информации, выгод (преимуществ) свободного распространения информации и статей затрат на ее защиту);

– с учетом всех этих факторов необходимо выбрать такой режим распространения информации, который бы на конец периода ее активного жизненного цикла обеспечивал бы максимальный эффект от использования информации.

Для определения «веса» ущербов, выгод и затрат целесообразно прибегнуть к помощи экспертов, хорошо понимающих ценность сведений и их взаимосвязь с указанными факторами. Возможность проявления различных факторов в динамике жизненного цикла информации оценивается субъективной вероятностью.

На основе сравнительных оценок отдельных факторов с учетом возможности их проявления вычисляется значение интегрального показателя выбранного режима распространения информации

В случае если рассчитанное значение интегрального показателя оказывается больше нуля, то включение рассматриваемой информации в перечень сведений, отнесенных к информации ограниченного доступа, целесообразно.

Отнесение информации к информационным ресурсам, подлежащим защите от несанкционированных и непреднамеренных воздействий, целесообразно, если величина предотвращаемого при этом ущерба превышает величину затрат на ее защиту.

В условиях стабильной экономики государственный заказ для предпринимателя по засекречиванию информации выглядит приоритетным, поскольку он не связан с рыночным риском реализации продукции. Финансирование мероприятий по защите государственной тайны осуществляется в основном за счет средств, получаемых «при выполнении работ, связанных с использованием сведений, составляющих государственную тайну» в соответствии с Федеральным Законом РФ «О государственной тайне». Требования к условиям и уровню защиты задаются государственными нормативными документами и являются императивными.

Исходные условия задач защиты государственной и коммерческой тайны

Обладатель коммерческой тайны заинтересован в максимально высоком уровне защиты своей коммерческой тайны и минимизации затрат на ее защиту. Это требует определения им допустимого риска и поиска оптимального решения. Определить размер целесообразных затрат

на обеспечение безопасности информации можно с помощью следующего подхода. Допустим, что для каждой из возможных неприятностей известны размеры и величины ущерба, если никакое противодействие не предпринимается. Индекс ноль означает, что неприятность не произошла. В первой колонке этой матрицы стоят затраты на противодействие данной неприятности при разном уровне противодействия. Индекс ноль в этом случае означает, что никаких затрат не производится ($V_{11} = 0$). Считается, что противодействие R_i способно предотвратить все неприятности S_j такие, что $i \geq j$ и совсем не способно уменьшить неприятность S_k при $i < k$.

Первичный поверхностный анализ позволяет сделать некоторые выводы

Пусть, например, финансовые возможности производителя ограничены, и он может организовать противодействие степени не больше, чем R_2, в то время как ожидать надо неприятность степеней $S_{3.}$. Затраты на какое-либо противодействие лишь увеличат потери производителя.

Другой исход имеет место, если подрядчик производителя готов выполнить работу лишь большого объема и высокой степени противодействия, например R_3. Если можно ожидать неприятность не более, чем степени $S_{1,}$ то от бездействия ущерб будет меньше, чем от противодействия, которое доступно производителю. В том случае, когда у производителя есть возможность маневра, он обычно может выбирать и путь решения стоящей перед ним задачи.

Выбор способа минимизации затрат зависит от того, какова исходная информация о различных степенях неприятности.

Математическая модель задачи принятия решений определяется множеством состояний {Sj}, множеством стратегий (противодействий) $\{R_i\}$ и матрицей возможных результатов $||V_{ij}||$.

В отдельных задачах рассматривается матрица рисков $||r_{ij}||$. Риск – мера несоответствия между разными возможными результатами принятия определенных стратегий. Элементы матрицы рисков $||r_{ij}||$ связаны с элементами платежной матрицы производителя. Таким образом, риск – это разность между результатом, который можно получить, если знать действительное состояние внешней среды, и результатом, который будет получен при *i*-ой стратегии.

Для принятия решения в условиях неопределенности используется ряд критериев.

Критерий Лапласа опирается на то, что все состояния внешней среды S_j полагаются равновероятными. В соответствии с этим принципом каждому состоянию S_j ставится вероятность q_j, определяемая по формуле:

Критерий Вальда опирается на принцип наибольшей осторожности и основывается на выборе наилучшей из наихудших стратегий R_i.

Критерий Сэвиджа использует матрицу рисков $||r_{ij}||$. Независимо от того, является ли V_{ij} доходом или затратами, r_{ij} определяет величину потерь предприятия и является мерой несоответствия между разными возможными вариантами стратегий. Критерий Сэвиджа рекомендует в условиях неопределенности выбирать ту стратегию R_i, при которой величина риска принимает наименьшее значение в самой неблагоприятной ситуации (т.е. используется минимаксный критерий).

Критерий Гурвица устанавливает баланс между случаями крайнего пессимизма и крайнего оптимизма. Использование данного критерия основано на том, что внешняя среда может находится в самом выгодном состоянии с вероятностьюα и в самом невыгодном состоянии с вероятностью $(1 - \alpha)$, при этом $0 \leq \alpha \leq 1$ Если $\alpha = 0$, то получаем пессимистический критерий Вальда.

Выбор конкретного критерия для принятия решений о размерах целесообразных затрат в условиях неопределенности является наиболее ответственным этапом Критерий выбирается с учетом конкретной ситуации, специфики решаемой задачи и в соответствии с целями предприятия, а также опираясь на прошлый опыт. Если даже минимальный риск недопустим, то следует применять критерий Вальда. В случае, когда определенный риск вполне приемлем, то можно воспользоваться критерием Сэвиджа.

Литература

1. Закон о государственной тайне от 21.06.1993 г. № 5485-1.
2. Федеральный закон о коммерческой тайне от 29.07.2004 г. № 98-ФЗ.
3. Симонов С.В. Технологии и инструментарий для управления рисками. – Jet Info, N2, 2009.
4. Петренко С.А., Симонов С.В. Экономически оправданная безопасность. – Изд. ДМК, Москва, 2008.
5. Цуканова О.А., Смирнов С.Б. Экономика защиты информации: Учебное пособие. – СПб : СПб ГУИТМО, 2007.

ОБЗОР ИНФОРМАЦИОННЫХ УГРОЗ МНОГОПОЛЬЗОВАТЕЛЬСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ И МЕТОДОВ ИХ ПРЕДОТВРАЩЕНИЯ

Гавриш Н.В.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Научный руководитель – к.т.н. Косяков М.С.

В данной статье будет проведен обзор информационных угроз многопользовательских информационных систем и методов их предотвращения. Будут рассмотрены основные виды информационных угроз, степень их опасности для информационной системы, степень угрозы нанесения ущерба персональным данным и другим данным системы. Под таким ущербом мы будем прежде всего понимать несанкционированный доступ к персональным данным и другим данным информационной системы, уничтожение части или всех персональных данных или других данных информационной системы. Последствиями таких действий злоумышленника могут быть потеря всех или части персональных или иных данных информационной системы, а так же получение доступа к персональным данным или другим данным информационной системе третьими лицами, которым данная информация не предназначалась. В качестве третьих лиц могут выступать заинтересованные в получении персональных данных и других данных, хранящихся в информационных системах, пользователи и организации. Например, конкурирующие

коммерческие организации заинтересованы в получении конфиденциальной информации друг друга. В качестве другого примера можно привести получение доступа к данным, составляющим государственную тайну, иностранными разведками. Не так давно широко стал известен инцидент с утечкой SMS-сообщений, отправленных с сайта мобильного оператора «Мегафон». В результате плохой организации безопасности информационной системы отправки SMS-сообщений на интернет-сайте оператора «Мегафон» в открытый доступ попало порядка 3000 SMS-сообщений, представлявших собой конфиденциальную информацию клиентов оператора сотой связи «Мегафон».

1) **Пользователи**

В контексте информационной безопасности целесообразно рассматривать любых пользователей информационной системы как две группы:

- добросовестные пользователи;
- недобросовестные пользователи.

При проектировании многопользовательской информационной системы следует считать по умолчанию всех пользователей недобросовестными и соответствующим образом строить систему безопасности, аутентификации и авторизации пользователей.

2) **Модель угроз**

Чтобы грамотно построить безопасную и надежную информационную систему, необходимо учесть все возможные виды угроз для этой системы. Для этого используется модель угроз. Модель угроз принято делить на два вида:

- базовая;
- частная.

Любая модель угроз описывает угрозы информационной безопасности системы. Базовая модель угроз утверждена ФСТЭК России. С ней можно ознакомиться на сайте организации «Иноформзащита» по адресу http://zki.infosec.ru/law/personal/144. Несмотря на то, что эта модель утверждена ФСТЭК, найдется не так много информационных систем, угрозы безопасности для которых она описывала бы полностью. Поэтому для конкретной информационной системы строят частные модели угроз. Частные модели угроз описывают угрозы конкретной информационной системы.

Для описания информационных угроз в современном мире компания Microsoft разработала модель STRIDE, описывающую все возможные информационные угрозы в современном мире. На базе этой модели можно строить частные модели угроз.

Название модели STRIDE – это аббревиатура из названий информационных угроз:

- Spoofing identity (aka phishing). Подделка идентификатора. В качестве примера можно привести нелегальное получение пользовательской аутентификационной информации и получение доступа к ресурсам, для которых эта информация требовалось. Такими ресурсами могут являться аккаунты от электронных почтовых сервисов или информация, представляющая собой государственную тайну;
- Tampering with data. Это подделка данных. Так, например, это может быть нелегальные, неавторизованные изменения в базе данных информационной системы, которые в последствии

могут привести к утечке информации, выходе из строя информационной системы, потере данных, либо служить в качестве дезинформации;

– Repudiation. Это отказ от ответственности за выполненное действие. Пользователь совершает какие-либо неправомерные действия в информационной системе таким образом, что это невозможно доказать ввиду отсутствия к примеру, логов системы или каких-либо иных средств идентифицировать нарушителя, либо доказать, что предпринятые ими действия были запрещены системой. Для защиты от такого рода угроз применяют различные средства для совершения пользователем действия подтверждения с тем, что он ознакомлен с информацией о том, что определенные дальнейшие действия пользователя могут стать причиной судебного разбирательства, и являются нелегальным;

– Information disclosure. Это утечка информации;

– Denial of service. Это известные DoS-атаки. Такой вид угроз является специфическим для web-сервисов. В результате успешно проведенной DoS-атаки сервис становится недоступным для своих конечных пользователей. Для предотвращения потерь от таких атак существуют различные стратегии по повышению надежности, доступности и стабильности системы;

– Elevation of privilege. Это превышение привилегий. То есть злонамеренный пользователь, не обладающий достаточными привилегиями для нанесения ущерба системе, нелегально получает более высокие привилегии с возможностями вплоть до уничтожения всей системы целиком.

На базе этой модели угроз компанией Microsoft было разработано специальное средство Microsoftthreatmodelingtool предназначенное для моделирования частных моделей угроз для конкретной информационной системы.

3) **Управление доступом**

В вопросе безопасности при проектировании информационных систем необходимо придерживаться принципа наименьших привилегий. Принцип наименьших привилегий – основополагающий принцип при проектировании высоконадежных информационных систем, отвечающих высоким требованиям безопасности.

Существует несколько методов разделения привилегий:

– DAC

Избирательное управление доступом (англ. discretionary access control, DAC) – управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа. Также называется дискреционным управлением доступом,контролируемым управлением доступом или разграничительным управлением доступом. Субъект доступа «Пользователь № 1» имеет право доступа только к объекту доступа № 3, поэтому его запрос к объекту доступа № 2 отклоняется. Субъект «Пользователь № 2» имеет право доступа как к объекту доступа № 1, так и к объекту доступа № 2, поэтому его запросы к данным объектам не отклоняются.

Для каждой пары (субъект – объект) должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т. д.), то есть тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу (объекту).

Возможны несколько подходов к построению дискреционного управления доступом:

– каждый объект системы имеет привязанного к нему субъекта, называемого владельцем. Именно владелец устанавливает права доступа к объекту;

– система имеет одного выделенного субъекта – суперпользователя, который имеет право устанавливать права владения для всех остальных субъектов системы;

– субъект с определенным правом доступа может передать это право любому другому субъекту.

Возможны и смешанные варианты построения, когда одновременно в системе присутствуют как владельцы, устанавливающие права доступа к своим объектам, так и суперпользователь, имеющий возможность изменения прав для любого объекта и/или изменения его владельца. Именно такой смешанный вариант реализован в большинстве операционных систем, например Unix или Windows NT.

Избирательное управление доступом является основной реализацией разграничительной политики доступа к ресурсам при обработке конфиденциальных сведений, согласно требованиям к системе защиты информации.

– MAC

Мандатное управление доступом (англ. Mandatory access control, MAC) – разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности. Также иногда переводится как Принудительный контроль доступа. Это способ, сочетающий защиту и ограничение прав, применяемый по отношению к компьютерным процессам, данным и системным устройствам и предназначенный для предотвращения их нежелательного использования.

Мандатная модель управления доступом, помимо дискреционной и ролевой, является основой реализации разграничительной политики доступа к ресурсам при защите информации ограниченного доступа. При этом данная модель доступа практически не используется «в чистом виде», обычно на практике она дополняется элементами других моделей доступа. Для файловых систем, оно может расширять или заменять дискреционный контроль доступа и концепцию пользователей и групп. Самое важное достоинство заключается в том, что пользователь не может полностью управлять доступом к ресурсам, которые он создает. Политика безопасности системы, установленная администратором, полностью определяет доступ, и обычно пользователю не разрешается устанавливать более свободный доступ к его ресурсам чем тот, который установлен администратором пользователю. Системы с дискреционным контролем доступа разрешают пользователям полностью определять доступность их ресурсов, что означает, что они могут случайно или преднамеренно передать доступ неавторизованным пользователям. Такая система запрещает пользователю или процессу, обладающему определенным уровнем доверия, получать доступ к информации, процессам или устройствам более защищенного уровня. Тем самым обеспечивается изоляция пользователей и процессов, как известных, так и неизвестных системе (неизвестная программа должна быть максимально лишена доверия, и ее доступ к устройствам и файлам должен ограничиваться сильнее). Очевидно, что система, которая обеспечивает разделение данных и операций в компьютере, должна быть построена таким образом, чтобы ее нельзя было «обойти». Она также должна давать возможность оценивать полезность и эффективность используемых правил и быть защищенной от постороннего вмешательства.

– RBAC

Управление доступом на основе ролей (англ. Role Based Access Control, RBAC) – развитие политики избирательного управления доступом, при этом права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли.

Формирование ролей призвано определить четкие и понятные для пользователей компьютерной системы правила разграничения доступа. Ролевое разграничение доступа позволяет реализовать гибкие, изменяющиеся динамически в процессе функционирования компьютерной системы правила разграничения доступа.

Такое разграничение доступа является составляющей многих современных информационных систем. Как правило, данный подход применяется в системах защиты СУБД, а отдельные элементы реализуются в сетевых операционных системах. Ролевой подход часто используется в системах, для пользователей которых четко определен круг их должностных полномочий и обязанностей. Несмотря на то, что Роль является совокупностью прав доступа на объекты компьютерной системы, ролевое управление доступом отнюдь не является частным случаем избирательного управления доступом, так как его правила определяют порядок предоставления доступа субъектам компьютерной системы в зависимости от имеющихся (или отсутствующих) у него ролей в каждый момент времени, что является характерным для систем мандатного управления доступом. С другой стороны, правила ролевого разграничения доступа являются более гибкими, чем при мандатном подходе к разграничению. Так как привилегии не назначаются пользователям непосредственно, и приобретаются ими только через свою роль (или роли), управление индивидуальными правами пользователя, по сути, сводится к назначению ему ролей.

4) **Криптография**

Теперь перейдем к краеугольному камню информационной безопасности – криптографии. Современная криптография – одна из основных областей исследований в области информационной безопасности. Целесообразность применения криптографических методов основано на одной из 7-ми нерешенных задач тысячелетия:

P ! = NP. Коротко эту задачу можно сформулировать следующим образом: всегда ли значение проще проверить, чем подобрать. Пока не доказано что P равно NP, криптография имеет смысл. В современном мире считается, что злоумышленник знает, какой алгоритм используется при шифровании – ему неизвестен только ключ.

Разделяют два вида шифрования:

Симметричное шифрование

Способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. До изобретения схемы асимметричного шифрования единственным существовавшим способом являлось симметричное шифрование. Ключ алгоритма должен сохраняться в секрете обеими сторонами. Алгоритм шифрования выбирается сторонами до начала обмена сообщениями.

Достоинства:

– скорость (по данным Applied Cryptography – на 3 порядка выше);

– простота реализации (за счет более простых операций);
– меньшая требуемая длина ключа для сопоставимой стойкости;
– изученность (за счет большего возраста).

Недостатки:

– сложность управления ключами в большой сети. Означает квадратичное возрастание числа пар ключей, которые надо генерировать, передавать, хранить и уничтожать в сети. Для сети в 10 абонентов требуется 45 ключей, для 100 уже 4950, для 1000–499500 и т.д.;
– сложность обмена ключами. Для применения необходимо решить проблему надежной передачи ключей каждому абоненту, так как нужен секретный канал для передачи каждого ключа обеим сторонам.

Для компенсации недостатков симметричного шифрования в настоящее время широко применяется комбинированная (гибридная) криптографическая схема, где с помощью асимметричного шифрования передается сеансовый ключ, используемый сторонами для обмена данными с помощью симметричного шифрования.

Важным свойством симметричных шифров является невозможность их использования для подтверждения авторства, так как ключ известен каждой стороне.

Несимметричное шифрование

Открытый ключ передается по открытому (то есть незащищенному, доступному для наблюдения) каналу, и используется для проверки электронно-цифровой подписи и для шифрования сообщения. Для генерации электронно-цифровой подписи и для расшифровки сообщения используется секретный ключ. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколах TLS и его предшественнике SSL (лежащих в основе HTTPS), в SSH. Также используется в PGP, S/MIME. Суть использования ассиметричного шифрования сводится к нескольким простым утверждениям.

Распространение ключей – одно из самых уязвимых мест в информационных системах, использующих шифрование, как средство защиты паролей. При распространении ключей по умолчанию принято считать, что канал передачи прослушивается, потому что если бы он не прослушивался, шифрование не имело бы смысла. Вероятность наличия доверенного канала для передачи ключа достаточно мала, чтобы считать, что доверенного канала передачи (который не прослушивается) нет. В таком случае применяется шифрование открытым ключом.

Данные всегда шифруются симметричным алгоритмом, так как несимметричные алгоритмы очень медленные. Несимметричным алгоритмом шифруют только ключи для симметричных алгоритмов.

Таким образом, процесс передачи секретной информации при помощи несимметричного шифрования выглядит следующим образом:

– принимающая сторона генерирует свой закрытый не скомпрометированный ключ;
– принимающая сторона публикует открытый ключ в доступном для всего мира месте;
– передающая сторона шифрует этим ключом свой пароль. Происходит передача зашифрованных этим паролем данных, и сам пароль, зашифрованный открытым ключом;

– принимающая сторона расшифровывает своим закрытым ключом пароль, а потом данные, которые были зашифрованы по симметричному алгоритму, расшифровываются расшифрованным паролем;

– в случае необходимости передать что-то передававшей стороне, достаточно будет зашифровать данные тем же паролем по симметричному алгоритму. У передававшей стороны этот пароль уже хранится – ей не требуется его расшифровать.

5) **Пароли**

В общем случае секретной информацией, которую необходимо шифровать, являются пароли. Использование паролей влечет за собой несколько проблем:

– хранение;
– защита от подбора паролей;
– двухуровневая аутентификация.

Проблема заключается в том, что любое долговременное хранилище может быть скомпрометировано. Таким образом, в открытом виде в базе пароли хранить нельзя. Некоторое время назад являлось общепринятой практикой хранить в базе MD5-хэши паролей. Хеширование – необратимая операция, проблема некоторое время казалась решенной. До тех пор, пока не появились таблицы хэшей, так называемые Rainbow-таблицы. Таким образом задача злоумышленника, после получения доступа к файлом с паролями, сводилась к подбору пароля по известной таблице хэшей. Для этой проблемы так же нашли решение – используют так называемую «соль» (от англ. salt). Salt – это случайным образом сгенерированная последовательность символов короче пароля, хранящаяся вместе с паролем. В базе данных или файле хранится уже непосредственно хеш от конкатенации хэша пароля и salt. Для увеличения надежности и безопасности системы можно salt периодически менять.

Для защиты от подбора паролей с точки зрения проектирования системы необходимо две вещи:

– запрещать пользователю создавать простые пароли на уровне регистрации;
– следить за тем, чтобы не производилось подбора пароля при помощи автоматизированных средств (ботов). Для этого, как правило, используется «капча», либо после нескольких неудачных попыток входа, выполняется блокировка либо IP адреса, либо аккаунта, либо иным способом.

Однако реальность такова, что современных вычислительных мощностей достаточно чтобы подобрать любой пароль, любой хэш в ограниченное время. Таким образом, на пароли по рассчитывать нельзя. Поэтому в серьезных информационных системах, которым предъявляются более высокие требования безопасности, чем к остальным, выполняется двухуровневая аутентификация. Двухуровневая аутентификация требует кроме ввода пароля, дополнительного действия от пользователя, например ввода кода, высланного на мобильный телефон. Так же в редких случаях применяются одноразовые пароли. Однако в случае одноразовых паролей мы имеем проблему ограниченности человеческих возможностей по запоминанию паролей либо проблему информационной безопасности хранилища таких одноразовых паролей в случае если таковое ведется. Еще одним видом двухуровневой аутентификации является анализ поведенческих паттернов. Так, например, facebook при попытке авторизоваться с другого IP-

адреса предлагает сопоставить фотографии друзей их именам. Google при авторизации из другого географического региона предлагает сменить пароль.

6) **Web**

Теперь более подробно остановимся на безопасности web-систем. Веб-системы, как один из видов многопользовательских информационных систем, имеет следующие слабые места в обеспечении информационной безопасности:

- аутентификация;
- защита канала передачи;
- уязвимости.

Традиционно существует три основных вида аутентификации web-систем:

- Basic Http auth – передача данных в открытом виде. В этом случае все действия по проверке подлинности производятся на стороне сервера;
- Digest Http auth – в большинстве web-систем не используется, так как требует установки дополнительного программного обеспечения на стороне клиента;
- Client SSL certificate auth. Такая аутентификация с использованием SSL-сертификатов часто используется в серьезных системах, связанных с финансами либо в других сферах, где требуется достаточно высоких уровень безопасности информации, например Webmoney.

Основная проблема basichttpauth состоит не в том, что данные передаются воткрытом виде, а в том, что они передаются по незащищенному каналу. В качестве защиты канала передачи можно использовать SSL.

SSL поддерживает 3 типа аутентификации:

- аутентификация обеих сторон (клиент – сервер);
- аутентификация сервера с неаутентифицированным клиентом;
- полная анонимность.

Всякий раз, когда сервер аутентифицируется, канал безопасен против попытки перехвата данных между веб-сервером и браузером, но полностью анонимная сессия по своей сути уязвима к такой атаке. Анонимный сервер не может аутентифицировать клиента. Если сервер аутентифицирован, то его сообщение сертификации должно обеспечить верную сертификационную цепочку, ведущую к приемлемому центру сертификации. Проще говоря, аутентифицированный клиент должен предоставить допустимый сертификат серверу. Каждая сторона отвечает за проверку того, что сертификат другой стороны еще не истек и не был отменен.

Опишем ряд атак, которые могут быть предприняты против протокола SSL. Однако, SSL устойчив к этим атакам.

7) **Раскрытие шифров**

Как известно, SSL зависит от различных криптографических параметров. Шифрование с открытым ключом RSA необходимо для пересылки ключей и аутентификации сервера/клиента. Однако, в качестве шифра используются различные криптографические алгоритмы. Таким образом, если осуществить успешную атаку на эти алгоритмы, то SSL не может уже считаться

безопасным. Атака на определенные коммуникационные сессии производится записью сессии, и потом, в течение долгого времени подбирается ключ сессии или ключ RSA. SSL же делает такую атаку невыгодной, так как тратится большое количество времени и денег.

8) **Злоумышленник посередине**

Также известна как MitM (Man-in-the-Middle) атака. Предполагает участие трех сторон: сервера, клиента и злоумышленника, находящегося между ними. В данной ситуации злоумышленник может перехватывать все сообщения, которые следуют в обоих направлениях, и подменять их. Злоумышленник представляется сервером для клиента и клиентом для сервера. В случае обмена ключами по алгоритму Диффи-Хелмана данная атака является эффективной, так как целостность принимаемой информации и ее источник проверить невозможно. Однако такая атака невозможна при использовании протокола SSL, так как для проверки подлинности источника (обычно сервера) используются сертификаты, заверенные центром сертификации.

Атака будет успешной, если:

- сервер не имеет подписанного сертификата;
- клиент не проверяет сертификат сервера;
- пользователь игнорирует сообщение об отсутствии подписи сертификата центром сертификации или о несовпадении сертификата с кэшированным;

Атака отклика

Злоумышленник записывает коммуникационную сессию между сервером и клиентом. Позднее, он пытается установить соединение с сервером, воспроизводя записанные сообщения клиента. Но SSL отбивает эту атаку при помощи особого уникального идентификатора соединения (ИС). Конечно, теоретически третья сторона не в силах предсказать ИС, потому что он основан на наборе случайных событий. Однако, злоумышленник с большими ресурсами может записать большое количество сессий и попытаться подобрать «верную» сессию, основываясь на коде nonce, который послал сервер в сообщение Server_Hello. Но коды nonce SSL имеют, по меньшей мере, длину 128 бит, а значит, злоумышленнику необходимо записать264 кодов nonce, чтобы получить вероятность угадывания 50 %. Но 264 достаточно большое число, чтобы сделать эти атаки бессмысленными.

Теперь рассмотрим несколько специфических уязвимостей web-систем с точки зрения программного кода:

- SQL-инъекции;
- XSS;
- CSRF.

Рассмотрим как защищаться от угроз, связанных с перечисленными уязвимостями.

SQL-инъекции

SQL-инъекции происходят, когда в не параметризованный SQL-запрос попадают данные, содержащие кавычку или апостроф (которые завершают выражение) и затем содержащие какой-то программный код, который будет выполнен после запроса, закончившегося завершающим символом. Например у нас есть такой запрос: «Select data from users where users.name = ‘” + $user_name + “’”. В случае если переменная $user_name будет содержать кавычку, мы будем

иметь дело с SQL-инъекцией. Решение проблемы с SQL-инъекции – использование параметризованных запросов. При этом параметры в этот параметризованный запрос необходимо передавать при помощи специальных вызовов.

XSS

Данный вид атаки заключается в том, что пользователь в свои пользовательские данные записывает Javascript-скрипт, который затем, будучи показанным в браузере другому пользователю, который запросил эти данные, соответственно выполняется в браузере и производит какие-то либо несанкционированные злонамеренные действия. Для решения такой проблемы достаточно использовать стандартные библиотеки, которые умеют санитизировать выдачу браузера.

CSRF

Данная уязвимость предполагает следующий сценарий:

- пользователь легально авторизован в информационной web-системе;
- затем пользователь заходит на сайт злоумышленника;
- сайт злоумышленника отправляет POST или GET запросы той системе, на которой пользователь авторизован от имени самого пользователя.

При этом злоумышленник сталкивается такими проблемами как:

- необходимость знания url-шаблона, по которому необходимо отправлять запросы;
- запросы на какое-либо действие не должны требовать подтверждения пользователя;
- в случае с POST-запросом злоумышленник так же сталкивается с проблемой кросс-доменной браузерной политики, которая в большинстве случаев не позволит совершить кросс-доменный POST-запрос. Это возможно только в том случае, если такие запросы явно разрешены, например это запрос к какому-либо public API.

В результате можно выполнить какие-либо нежелательные действия, такие как удаление чего-либо, отправка информации куда-либо и другие действия, которые информационная web-система может выполнять через свой интерфейс без подтверждения пользователя.

Можно обойти, тем не менее, ограничение кросс-доменного POST-запроса с использованием тега iframe в теле запроса. Таким образом, уязвимость сохраняется. Чтобы окончательно решить вопрос с такой уязвимостью принято при совершении POST запроса передавать через форму случайный параметр (например, число). Если при получении запроса этот параметр не найден, то имеет место CSRF-атака. Большинство имеющихся на данный момент framework-ов поддерживают такую защиту автоматически.

В данной статье мы рассмотрели основные виды угроз безопасности информационной многопользовательской системы. Из данной статьи можно сделать вывод, что современные средства обеспечения информационной безопасности теоретически позволяют справиться с любой атакой злоумышленника. Успешными бывают атаки, против которых система до их проведения не была готова. При соответствующей грамотной настройке подсистемы безопасности многопользовательской информационной системы вероятность успеха атак злоумышленника может быть сведена к минимуму.

Литература

1. Саломаа А. Криптография с открытым ключом – М. : Мир, 1995. – 318 с. – ISBN 5-03-001991-X.

2. Menezes A.J., van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. – 1997. – ISBN 0-8493-8523-7.

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си Applied Cryptography. Protocols, AlgorithmsandSourceCodeinC – М. : Триумф, 2002. – 816 с. – 3000 экз. – ISBN 5-89392-055-4.

4. Портал MSDN.MICROSOFT.COM: Microsoft Developer Network, The STRIDE Threat Model, 27.09.2011, режим доступа: http://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

УДК 378.14.015.62

БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА ОЦЕНИВАНИЯ ЗНАНИЙ

Гатченко Н.А., Исаев А.С.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Научный руководитель – доц. Королева А.А.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

С глубокой древности и по настоящее время образование являлось и будет являться одним из главенствующих вопросов, как в деятельности государства, так и в жизни каждого из нас. Именно по уровню и качеству образования можно говорить как о стране в целом, так и о конкретном человеке, но из чего складывается наше первоначальное субъективное мнение? Конечно же, из оценок, полученных каждым человеком во время его обучения. Система оценивания знаний – важнейший элемент образовательного процесса, от которого во многом зависит правильность восприятия знаний и умений учащихся после выпуска из учебного заведения, именно поэтому изучение системы оценивания знаний является одной из наиболее актуальных проблем современной педагогики.

В настоящее время в мире используется множество всевозможных шкал для оценки знаний, в некоторых из них принято использовать цифровые обозначения, допускающие и дробные оценки, другие же шкалы, как, например, американская, традиционно используют буквенные обозначения. В российской истории просвещения изначально, как и в Европе, существовала трехразрядная система оценок. Так в списке студентов Киевской духовной академии в 1737 году существовало 3 степени успехов в учебе:

– очень хорошие «Учения изрядного, надежного, доброго, честного, хорошего, похвального»;
– средние «Учения посредственного, мерного, нехудого»;
– ниже среднего «Учения слабого, подлого прехудого, безнадежного, ленивого».

Постепенно словесные оценки становились однообразнее и короче, они все чаще и чаще заменялись цифровым обозначением, что помогало не только экономить время, но и бумагу, на которой проставлялись оценки. В разное время в России применялись следующие бальные системы оценки знаний. Наиболее продуктивной и исчерпывающей по мнению большинства преподавателей являлась 5-бальная система, которая и была в 1837 году официально установлена Министерством народного просвещения, которая устанавливала: «1» – слабые успехи; «2» – посредственные; «3» – достаточные; «4» – хорошие; «5» – отличные. Однако на протяжении 20 века оценка «1» постепенно все чаще и чаще выходила из употребления, в результате чего 5–бальная система эволюционировала в современную 4–бальную систему. Эта система, пришедшая к нам со времен СССР, до сих пор повсеместно применяется в России и многих других странах постсоветского пространства. В соответствии с действующим законом Российской федерации «Об образовании» от 10 июля 1992 г. № 3266–1 , статьей 15 пунктом 3 устанавливается следующее:

«*Образовательное учреждение самостоятельно в выборе системы оценки знаний, формы, порядка и периодичности промежуточной аттестации обучающихся.*»

В соответствии с этим законом в ряде высших учебных заведений был введена балльно-рейтинговая система оценивания результатов обучения. Санкт-Петербургский государственный Университет информационных технологий механики и оптики (СПБГУ ИТМО), является одним из первых вузов, в которых данная система была внедрена и успешно функционирует. Даная система была введена постановлением ректора «О проведении текущего контроля успеваемости и промежуточной аттестации студентов СПБГУ ИТМО» и одобрена Ученым советом университета, протокол № 5 от 22 апреля 2008 года. В соответствии с которой регламентируется система оценивания знаний индивидуальных результатов обучения студентов, используемую при реализации технологий модульного обучения в университете. В результате чего оценка за семестр по каждой из дисциплин складывается из балов, заработанных каждым студентом в процессе обучения, а по окончании сессии балы суммируются и производится оценка по следующей шкале, сопоставимой с оценками ECTS (European Credit Transfer and Accumulation System – Европейская система перевода и накопления кредитов) – общеевропейская система учета учебной работы студентов при освоении образовательной программы или курса:

– «отлично», (A), если сумма баллов находится в пределах от 91 до 100 баллов включительно;

– «хорошо», (B – очень хорошо), если сумма баллов находится в пределах от 84 до 90 баллов включительно;

– «хорошо», (C – хорошо), если сумма баллов находится в пределах от 75 до 83 баллов включительно;

– «удовлетворительно», (D), если сумма баллов находится в пределах от 68 до 74 баллов включительно;

– «удовлетворительно», (E – посредственно), если сумма баллов находится в пределах от 60 до 67 баллов включительно;

– «неудовлетворительно», (F), если сумма баллов меньше 60 баллов;

– «зачтено» (при недифференцированной оценке), если сумма баллов равна или больше 60 баллов.

Таким образом, обучение каждого курса делится на 2 семестра, каждый из которых делиться на 2 модуля, максимальная сумма балов за семестр – 100.Таковой является система

оценивания знаний в ее нынешнем виде, однако прежде чем принять такую форму, система претерпела некоторые изменения. В первоначальном исполнении учебный год делился на 2 семестра: Осенний (2 модуля) и Весенний (3 модуля). В свою очередь за каждый из модулей выставлялось максимум 100 балов, средний бал за все модули семестра являлся балом за семестр. Таким образом, за семестр можно было получить по 100 усредненных балов по каждой из дисциплин. Такой подход к системе оценивания оказался избыточным и мало эффективным, в результате чего система эволюционировала до нынешнего ее состояния. До сих пор не утихают споры по поводу применения балльно-рейтинговой системы на практике, и в рамках исследования данной тематики нами был произведен социологический опрос, учащимся СПБГУ ИТМО было предложено выразить свое отношение к новой системе оценивания, а так же мотивировать свой ответ, на основании чего были выявлены следующие положительные и отрицательные стороны:

Положительные стороны:

- постепенный переход образовательной системы к общеевропейским стандартам;
- систематическое усвоение учебной программы, вследствие использования периодических аттестаций;
- выявление недостатков существующих методик образовательного процесса;
- выявление пробелов в знаниях отдельно взятых студентов;
- возможность наблюдения за ходом учебного процесса как со стороны родителей так и со стороны деканатов;
- увеличение дисциплинированности студентов;
- дополнительная мотивация студентов.

Отрицательные стороны:

- наличие усложненной системы аттестации;
- увеличение загруженности преподавателей;
- крайне затруднительно совмещать работу и учебу для студентов;
- подгон учебных программ под европейские стандарты;
- нацеленность некоторых студентов на получения баллов, а не знаний.

«Ваше отношение к балльно–рейтинговой системе?» (рис. 1)

1 – Положительное (321). 2 – Отрицательное (102). 3 – Безразличное (68). 4 – Затруднились ответить (9).

Всего опрошено 500 человек.

На основании проведенных исследований можно с уверенностью заключить, что балльно–рейтинговая система прекрасно работает в стенах нашего университета, больше половины из опрошенных студентов выразили свое положительное отношение к системе. Хочется заметить, что подавляющее большинство опрошенных являются студентами старших курсов, которые уже не первый год учатся по данному принципу. Основные недостатки легко устранимы и связаны в первую очередь с чисто организационными вопросами.

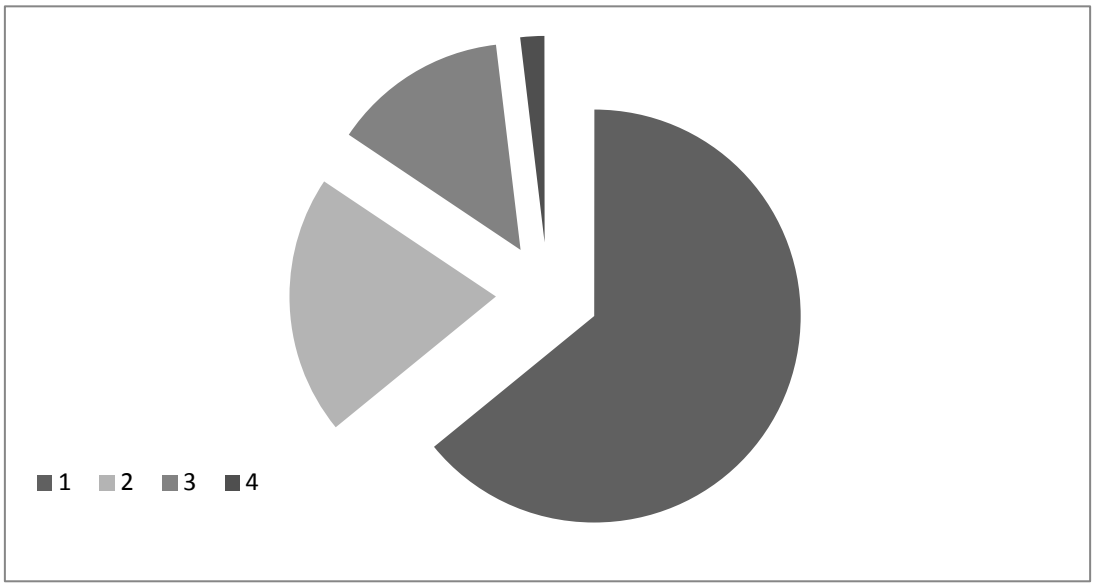


Рисунок 1. «Ваше отношение к балльно-рейтинговой системе?»

Литература

1. Болонский процесс: проблемы и перспективы / под ред. М.М. Лебедевой – Москва.
2. Закон РФ «Об образовании» от 10.07.1992 № 3266-1.
3. Положение о проведении текущего контроля успеваемости и промежуточной аттестации студентов СПБГУ ИТМО от 22.04.208.

УДК 003.26.09

СРАВНИТЕЛЬНЫЙ АНАЛИЗ БЛОЧНЫХ И ПОТОЧНЫХ СИММЕТРИЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

Гатченко Н.А., Исаев А.С.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Научный руководитель – доц. Яковлев А.Д.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

С момента изобретения симметричных способов шифрования и до появления ассиметричных алгоритмов прошел довольно значительный промежуток времени, шифры эволюционировали, приходили на смену друг другу. Как правило, последующий шифр учитывает недостатки своего предшественника и если не исключал их, то значительно усложнял процесс криптоанализа. Таким постепенным усложнением симметричные криптосистемы не только дошли до нашего времени, но и сохранили целесообразность своего применения, успешно конкурируя с ассиметричными криптосистемами. В настоящее время симметричные шифры разделяются на две концептуально различных реализации – поточный шифр и блочный шифр, и словно два враждующих племени каждый из шифров имеет своих сторонников, так

исследованием и разработкой поточных шифров в основном занимаются европейские криптографические центры, в то время как блочных – американские. Таким образом, перед нами открывается весь актуальный вопрос, за каким алгоритмом будущее, какому из алгоритмов отдать предпочтение, при организации системы защиты информации? На эти вопросы мы и постараемся ответить в нашей статье.

Симметричные криптосистемы – это способ шифрования, в котором для шифрования и расшифровывания используется один и тот же криптографический ключ, который должен сохранятся в секрете обеими сторонами, при этом алгоритм шифрования выбирается сторонами до начала обмена данными. Такие алгоритмы широко применяются в компьютерной технике, в системах сокрытия конфиденциальной и коммерческой информации от несанкционированного доступа и использования сторонними лицами. Главным принципом в таких системах является лишь одно условие – передатчик и приемник знают алгоритм шифрования и ключ, без которого информация будет представлять всего лишь набор символов, не имеющих смысла. При этом полная утрата статических закономерностей исходного сообщения является важным требованием к шифру, для этого шифр должен иметь эффект лавины (проявляется в зависимости всех выходных битов от каждого входного бита), а также отсутствием линейность, то есть условия $f(a)$ xor $f(b) = f(a$ xor $b)$), что обеспечивает проблематичность применения дифференциального криптоанализа к шифру.

Блочные шифры – разновидность симметричного шифра, обрабатывающий открытый текст блоками по несколько байт за одну итерацию (описание поэтапного процесса, в котором результаты выполнения группы операций в рамках каждого этапа используются следующим этапом). Если остаток исходного текста, или сам текст, меньше размера блока, то пред шифрованием его дополняют. Блочные шифры используют несколько основных принципов:

- рассеивание (diffusion) – то есть изменение любого знака открытого текста или ключа влияет на большое число знаков шифротекста, что скрывает статистические свойства открытого текста;
- перемешивание (confusion) – использование преобразований, затрудняющих получение статистических зависимостей между шифротектстом и открытым текстом.

Блочный шифр состоит из двух взаимосвязанных алгоритмов – алгоритмом шифрования E и алгоритмом расшифрования E^{-1} ,при этом входными данными служит блок размером n бит и ключ, размером k-бит. В результате получается n-битный зашифрованный блок. Процесс расшифрования – обратная функция к функции шифрования $E_K^{-1}\big(E_K(M)\big) = M$. Для любого ключа K, E_K является взаимно-однозначным отображением на множестве n-битных блоков. Размеры блока n являются фиксированными параметрами, типичными размерами ключа являются 40, 56, 64, 80, 128, 192, 256 бит. Для примера рассмотрим алгоритм OFB или режим обратной связи, который превращает блочный шифр в синхронный шифропоток, это генерирует ключевые блоки, которые являются результатом сложения с блоками открытого текста, таким образом, и получается зашифрованный текст. Из-за симметрии операции сложения, шифрование (рис. 1) и расшифрование (рис. 2) похожи. Следовательно, для функции стойкого блочного шифра должны быть реализованы следующие условия:

- функция расшифрования должна быть обратимой;

– не должно существовать иных методов прочтения сообщения по известному блоку, кроме как полным перебором ключей;

– не должно существовать иных методов определения ключа преобразования известного текста, кроме как полным перебором ключей.

Шифрование в режиме OFB

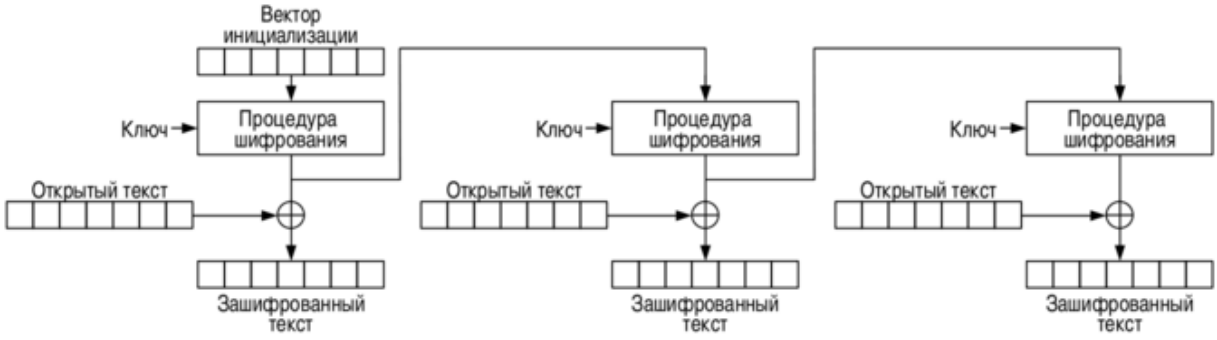


Рисунок 1. Шифрование в режиме OFB

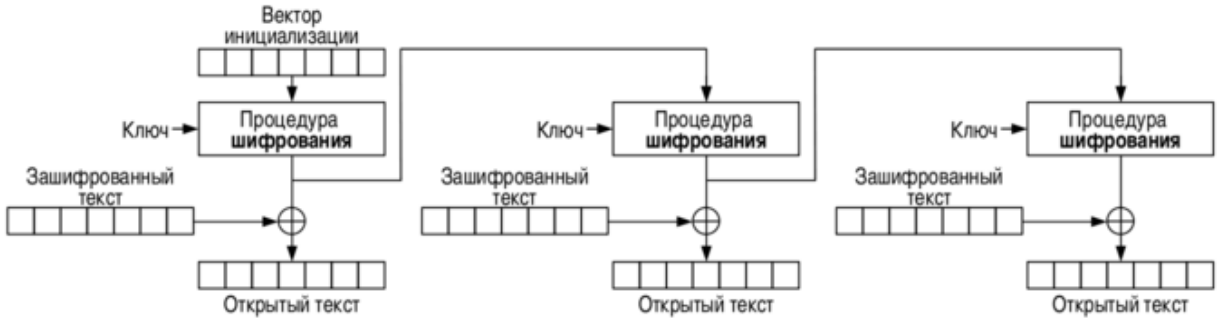


Рисунок 2. Расшифрование в режиме OFB

Поточные шифры – симметричный шифр, в котором каждый символ открытого текста преобразуется в символ шифрованного текста в зависимости не только от используемого ключа, но и от его расположения в потоке открытого текста. В случае простейшей реализации поточного шифра, генератор гаммы выдает ключевой поток $k_1, k_2, k_3, \ldots, k_L$, которые объединяются с потоком битов открытого текста $m_1, m_2, m_3, \ldots, m_L$ при помощи операции «исключающее ИЛИ»(xor), в результате чего получаем поток битов шифротекста $c_1, c_2, c_3, \ldots, c_L$, где $C_i = m_i$ xor k_i, а расшифровка $m_i = C_i$ xor k_i (рис. 3). Вполне очевидно, что если последовательность битов гаммы не имеет периода и выбранна случайно, то шифр взломать невозможно. Обычно применяется ключ меньшего размера, чем передаваемое сообщение. С его помощью генерируется псевдослучайная последовательность, которая должна удовлетворять постулатам Голомба:

– Количество «1» в каждом периоде должно отличаться от количества «0» не более чем на единицу.

– В каждом периоде 1\2 серий (из одинаковых символов) должна иметь длину 1, 1\4 должна иметь длину 2, 1\8 должна иметь длину 3 и т.д. Более того, для каждой из этих длин должно быть одинаковое количество серий из “1” и “0”.

– Предположим, у нас есть две копии одной и той же последовательности периода p, сдвинутые относительно друг друга на некоторое значение Y. Тогда для каждого Y, $0 \le Y \le p - 1$, мы можем подсчитать количество согласованностей между этими двумя последовательностями AY, и количество несогласованностей DY. Коэффициент автокорреляции для каждого Y определяется соотношением $(AY - DY) / p$ и эта функция автокорреляции принимает различные значения по мере того, как Y проходит все допустимые значения. Тогда для любой последовательности, удовлетворяющей этому предположению, автокорреляционная функция должна принимать лишь два значения.

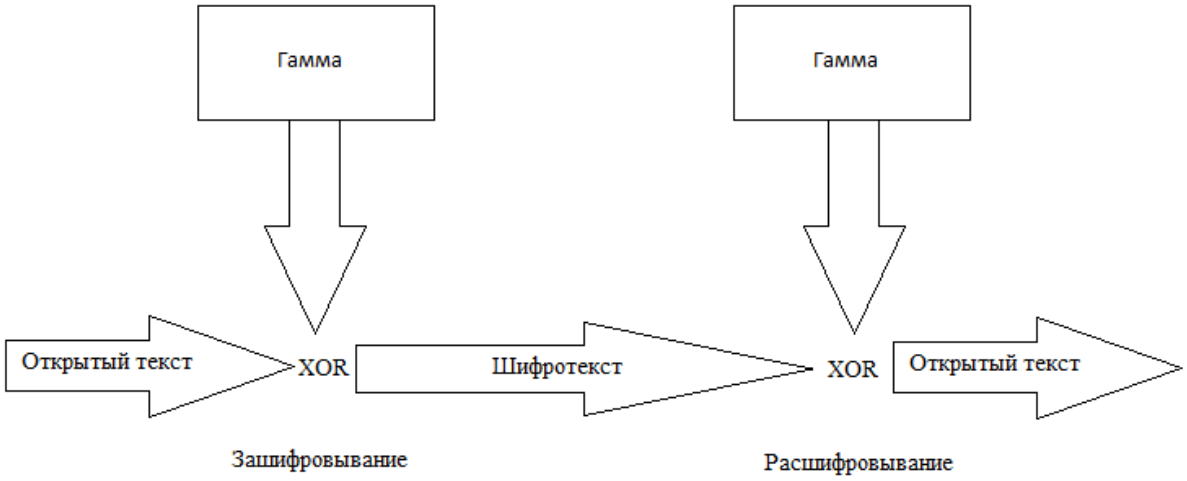


Рисунок 3. Наложение гаммы для поточных шифров

При этом необходимо заметить, что псевдослучайность гаммы может быть использована злоумышленником при атаке. Одним из основных особенностей поточного шифрования является тот факт, что в случае искажения одного знака шифротекста при его передачи по каналам связи приведет всего лишь к неправильной расшифровки этого символа, однако потеря знака при передачи приведет к неправильной расшифровки всего текста. Именно поэтому для предотвращения потерь информации применяют синхронизацию шифрования и расшифрования, так поточные алгоритмы делятся:

– синхронные поточные шифры (СПШ);
– асинхронные поточные шифры (АПШ).

СПШ – шифры, в которых поток ключей генерируется независимо от открытого текста и шифротекста. При шифровании генератор потока ключей выдает биты потока ключей, которые идентичны битам потока ключей при дешифровании. Потеря знака шифротекста приведет к нарушению синхронизации между этими двумя генераторами и невозможности расшифрования оставшейся части сообщения. Очевидно, что в этой ситуации отправитель и получатель должны повторно синхронизироваться для продолжения работы. Обычно синхронизация производится вставкой в передаваемое сообщение специальных маркеров. В результате этого пропущенный при передаче знак приводит к неверному расшифрованию лишь до тех пор, пока не будет принят один из маркеров. Этот подход имеет следующие положительные и отрицательные стороны:

Положительные:

– отсутствие эффекта распространения ошибок;

– предохраняют от любых вставок и удалений шифротекста, так как они приведут к потере синхронизации и будут обнаружены.

Отрицательные:

– уязвимость к изменению отдельных бит шифрованного текста. Если злоумышленнику известен открытый текст, он может изменить эти биты так, чтобы они расшифровывались, как ему надо.

АПШ – шифры, в которых поток ключей создается функцией ключа и фиксированного числа знаков шифротекста. Таким образом, внутреннее состояние генератора потока ключей является функцией предыдущих N битов шифротекста. Поэтому расшифрующий генератор потока ключей, приняв N битов, автоматически синхронизируется с шифрующим генератором. Реализация этого режима происходит следующим образом: каждое сообщение начинается случайным заголовком длиной N битов; заголовок шифруется, передается и расшифровывается; расшифровка является неправильной, зато после этих N бит оба генератора будут синхронизированы. Этот подход имеет следующие положительные и отрицательные стороны:

Положительные:

– размешивание статистики открытого текста.

Отрицательные:

– распространение ошибки (каждому неправильному биту шифротекста соответствуют N ошибок в открытом тексте);
– чувствительность к вскрытию повторной передачей.

Исходя из этого, мы проанализировали основные отличия поточных шифров от блочных:

1) высокая скорость шифрования поточных шифров;
2) отсутствие в поточных шифрах эффекта размножения ошибок;
3) структура поточного ключа имеет уязвимые места, дающие возможность криптоаналитику дополнительную информацию о ключе;
4) высокая эффективность взлома поточных шифров при помощи линейного и дифференциального анализа;
5) разнообразные методы взлома поточных шифров;
6) наличие четких критериев надежности для поточных шифров;
7) более динамичное исследование поточных шифров;
8) большая линейная сложность;
9) каждый бит потока ключей должен быть сложным преобразованием большинства битов ключа.

Таким образом, проведя детальный анализ симметричных алгоритмов шифрования, мы можем с уверенностью заключить, что каждый из алгоритмов имеет свои отличительные особенности, достоинства и недостатки, однако на наш взгляд наиболее перспективным направлением развития является именно поточные симметричные шифры. Ведь именно к ним относится знаменитый шифр Вернама – единственный алгоритм с доказанной абсолютной криптографической стойкостью.

Литература

1. Гатчин Ю.А., Коробейников А.Г. Основы криптографических алгоритмов. Учебное пособие.
2. Коробейников А.Г. Математические основы криптографии.
3. Панасенко С. Современные методы вскрытия алгоритмов шифрования.
4. Фергюсон Н., Шнайер Б. Практическая криптография.
5. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации.

УДК 003.26.09

ДРЕВНЕРУССКАЯ ТАЙНОПИСЬ

Гатченко Н.А., Исаев А.С., Яковлев А.Д.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Всем хорошо известна история появления и развития европейской тайнописи, но как же обстояло дело с тайнописью на Руси? На этот вопрос мы и попытаемся ответить в нашей статье.

Стоит начать с самого начала, с появления письменности, сейчас известно о том, что Кирилл и Мефодий вовсе не создатели письменности на Руси, они сотворили церковно-славянский язык, для того, чтобы переводить свою библию с греческого языка на древнеславянский. По сути, они извратили и первый язык и второй, создавая что–то среднее между ними. На Руси был один язык, но имел несколько видов записи в плоскостной системе, т. е. начертательные виды, – древнеславянская письменность:

1) Х'арийская Каруна (руника) – жреческая письменность из состава 256 рун. Упрощенные формы Каруны: а) санскрит (samckrit) – самостоятельный скрытый жреческий язык; б) футарк; в) славянские руны, руны Боянова гимна; г) сибирская (хакаская) рунница и т.д.

2) Да'арийские Тьраги. Это Образные символы, которые соединяют в себе сложные объемные знаки, передающие многомерные величины и многообразные Руны.

3) Расенские Молвицы (образно-зеркальное письмо). Данную письменность ныне называют этрусскими (тирренскими) письменами.

4) Святорусские образы (Буквица). Данное письмо было самым распространенным среди всех Славяно-Арийских родов в древности. Обладая образностью структуры и разными видами записи (буквица, глаголица, черты и резы) оно легло в основу многих европейских языков, в том числе Латыни и Английского. Письмо применялось для межродовых и междержавных договоров.

5) Глаголица или Торговое письмо, использовалась дл ведения реестров, подсчетов, оформления сделок и торговых договоров, а впоследствии они стали использоваться для записи сказаний и христианских книг.

6) Славянское народное письмо (черты и резы) – использовалось для передачи кратких сообщений на бытовом уровне.

7) Воеводское (воинское) письмо – тайные шифры.
8) Княжеское письмо – у каждого правителя свое.
9) Узелковое письмо.

Центрами развития национальной криптографии, сначала на бересте, а потом и на бумаге стали, естественно, духовно-политические центры, очаги грамотности и культуры – монастыри. Использовались, как очень сложные системы тайнописи со специальными ключами и их комбинациями, так и шифры попроще.

Считается, что тайнопись появилась в России не позднее 13 века. Появление специалистов – тайнописчиков, находящихся на государственной службе, следует отнести к 1549 г., к моменту образования Посольского приказа, осуществлявшего общее руководство внешней политикой страны. В начале 17 века на царство взошел Михаил Федорович Романов, по сути, при нем вся власть сосредоточилась в руках его отца, патриарха Филорета. При нем тайнопись перестала быт затеей, игрушкой, а стала одним из средств сохранения государственной тайны. Тайнопись развивалась и при Алексее Михайловиче, и при Петре I, и в 30-е годы 18 столетия, когда письма стали писать не шифрами, а кодами, используя цифры, а не буквы. В конце 18 века в России была создана дешифровальная служба, с 18 по конец 19 века считавшаяся лучшей в мире.

Шифровые ключи передавались из рук в руки, без свидетелей, или через абсолютно надежных посыльных, как правило, кровных родственников. Соблюдать тайну обещали высшей клятвой православных русских − «крест целовали».

Русские дореволюционные исследователи выделили семь основных систем архаической тайнописи:

1) иные письма – замена букв, общепринятого на Руси кириллического алфавита, буквами из других алфавитов – глаголицы, греческого, латинского, пермской азбуки (изобретенная, по преданию, просветителем зырян епископом пермским Стефаном, создавшим ее на основах современного кирилловского и греческого алфавитов, азбука эта не привилась на практике);

2) измененные знаки – выделяют две ее разновидности: а) систему знаков, измененных «путем прибавок» к обычным начертаниям; б) построенную на принципе, сходном с греческой тахиграфией, когда вместо буквы пишется лишь часть ее;

3) условные знаки – придумывание для букв особых начертаний. Применялись такие принципы изменения как: затемнение обычных начертаний, деформация, переворачивание, специально придуманные знаки. Замена букв треугольниками и четырехугольниками, заимствованными из решетки, составленной из двух параллельных линий, пересеченных двумя такими же линиями под прямым углом. В полученных клетках помещено по четыре и по три буквы в порядке азбуки. В тайнописи заменяются, при этом первая – простым угольником, а следующие – тем же угольником с одной, двумя или тремя точками, смотря по месту буквы в нем. Так как при таком размещении букв в клетках вся азбука не могла уместиться, то в этой тайнописи не оказывается знаков для таких букв как: ш, ь и др. Для некоторых букв взято начертание, заимствованное из греческого алфавита;

4) замены по шифровому ключу одной буквы на другую из того же алфавита. Существует два вида такой тайнописи: «простая литорея» на Руси ее прозвали тарабарской грамотой и

«мудрая литорея». Наиболее распространенной была «простая литорея», так как она была, исходя из названия, несложной. Суть ее заключается в том, что согласные буквы пишутся по порядку в два ряда, причем во втором ряду буквы расположены в обратном порядке (справа налево). Каждая буква одного ряда заменяется на соответствующую букву из другого ряда. Гласные и редуцированные ъ, ь остаются на своих местах, а греческие буквы заменяются созвучными. Ключ к «простой литорее» таков:

б в г д ж з к л м н
щ ш ч ц х ф т с р п

В «мудрой литорее» помимо замены согласных, заменялись и гласные буквы. Одной из разновидностей «мудрой литореи» является тайнопись «в квадратах». В виде ключа были таблицы из сорока квадратов, в каждом из которых помещались две разные буквы, одни были красного цвета другие черного. Кроме того, в квадратах вместе с буквами писались некоторые грамматико-орфографические термины, поясняющий смысл и характер употребления букв, что в некотором роде скрывало для непосвященных тот факт, что они имеют дело с ключом тайнописи. Эта литорея действовала следующим образом, красные буквы – это буквы обычного алфавита, черные – риторские буквы, обе азбуки идут строго по алфавиту, но риторская азбука начинается с четвертой позиции, т.е. риторская А соответствует букве Г обычного алфавита. Так как квадратов сорок то на письме заменялись все буквы.

Счетная или цифровая система: использование вместо букв цифр, т.к. в кирилловском алфавите практически все буквы, имели значение цифр. В древнерусских рукописных памятниках встречаются различные ее виды: простая цифровая система, сложная цифровая система, описательная система, система особенного применения арабских цифр, значковая система, т.е. с использование различных значков дл обозначения цифр-букв. В простой цифровой системе для каждой цифры-буквы, соответствующей желательной в обычном письме букве, дается два или несколько большей частью одинаковых слагаемых. Таким образом, чтобы получить нужную букву, надо произвести сложение, а полученная сумма, изображена соответствующей цифрой-буквой, и будет искомой буквой. Реже сумма слагается из различных цифр-букв, причем каждая группа цифр – слагаемых отделяется каким-либо знаком или пробелом о соседних. Буквы, не имеющие цифрового значения, остаются без изменений.

Старший образец такой тайнописи находится в псковском Апостоле 1307 г. (Собрание Большой Патриаршей библиотеки, № 722: «а лъ. в. в. нк. кк. дд. вв. ъ рекше. двдъ. органъ. мъ!сль. истина...». Произведя сложение попарно стоящих цифр (2 + 2 = 4, 50 + 20 = 70, 20 + 20 = 40, 4 + 4 = 8, 2 + 2 = 4) получим: д о м и д, т. е. имя Домид (рис. 1).

Арабские числа стали использоваться в качестве тайнописи лишь с того времени, как они начали входить в употребление в русской письменности, т. е. со второй половины XVI в. на русском юго-западе и с начала XVII в. на северо-востоке.

Кириллица		Кириллица	
Буквы и их названия	Цифровое значение	Буквы и их названия	Цифровое значение
А - аз	1	К - како	20
Б - буки		Л - люди	30
В - веди	2	М - мыслете	40
Г - глаголь	3	Н - наш	50
Д - добро	4	О - он	70
Є - есть	5	П - покой	80
Ж - живете		Р - рцы	100
З - зело	6	С - слово	200
Ѕ - земля	7	Т - твердо	300
И - иже	8	Оу - ук	400
І - и	10	Ф - ферт	500
Х - хер	600	Ю - ю	
Ѡ - от	800	Ꙗ - (и) я	
Ц - цы	900	Ѥ - (и) е	
Ч - червь	90	Ѧ - юс малый	
Ш - ша		Ѫ - юс большой	
Щ - ща		Ѩ - йотов. юс малый	
Ъ - ер		Ѭ - йотов. юс большой	
Ы - еры		Ѯ - кси	60
Ь - ерь		Ѱ - пси	700
Ѣ - ять		Ѳ - фита	9
		Ѵ - ижица	

Рисунок 1

В рукописном собрании Большой Московской Синодальной типографии № 199 на л. 8–33 внизу идет такая запись 1641 г. (приводим фрагмент):

3 ъ 3 1 7 1 4 9 3 7 4 4 = лъта 7149 и т. д.

Ключ к записи прост: буквы-цифры от 1 до 9 (а – 0), пишутся просто арабскими цифрами, от 10 до 90 (– ч) – теми же цифрами и обозначаются значком над ними, от 100 и до 900 – та же, с другим значком над ними, тысячи – со значком под цифрой; буквы, цифрового значения не имеющие, пишутся просто.

1) «Акростих» – стихотворение, в котором начальные буквы стихов (строк) образуют слово или фразу (часто имя автора или адресата). Наиболее часто применялся в поэзии. Истоки этой тайнописи уходят вглубь веков, ее фрагменты исследователи находят еще в эпопеях Гомера и в псалмах Ветхого завета. Одной из области применения акростиха были эпитафии, где с помощью

этой тайнописи сообщалось имя покойного, иногда имя составителя надписи или имя того кто установил надгробие. Это был именной акростих. Он составлялся не только по начальным буквам строк, но и по начальным слогам. В России пример акростишной эпитафии есть в надписи на надгробии патриарха Никона. По сути, акростих рассматривался не как тайнопись, а как «своеобразная эстетическая и даже онтологическая категория, квинтэссенция истины и гармонии».

2) Зеркальное письмо – составление послания в обратном порядке букв – справа налево.

Еще один из древнейших способов тайнописи – употребление глаголического алфавита после того, как он уступил место кириллице. Так же применялась тайнопись – криптограмма, текст записывали в виде какой-нибудь геометрической фигуры: круга, квадрата или креста. Начинать чтение надо было с заранее обусловленной буквы или строки. Еще одним способом тайнописи были монокодила – это разновидность вязи. Слово или сразу несколько слов пишут за один прием. Не отрывая пера от бумаги. При этом буквы замысловато переплетаются, появляются лишние линии. Таким образом, слова в предложении теряли привычное разделение и выделение отдельных букв было проблематично. Примером монокондил может быть первое слово в титулатуре Петра I.

Обычное место тайных надписей или записей в рукописях – в виде послесловий или приписок на особых местах – в основном, в начале или конце рукописи, часто на внутренней стороне переплета. Обычно за тайнописью скрывается имя писца, имя владельца рукописи, какое-либо замечание и т.п.

Проанализировав развитие тайнописи на Руси, мы пришли к гипотезе о том, что толчком к развитию тайнописи привел ввод в обиход кириллической азбуки. Ведь до этого тайнопись заключалась в различных формах написания языка, так торговцы не могли прочесть княжеское письмо, а князь не мог прочесть воинское письмо, так как они отличались способом написания и включали в себя определенные термины, а когда письменность стала для всех одинаковой, появилась необходимость в сокрытии важных сведений. Развитие тайнописи связано в первую очередь с развитием и совершенствованием представлений о тайном смысле, заключенном в послании и его ценности для личности, общества и государства. Таким образом, тайнопись постепенно преобразилась, плавно перетекая в современную криптографию, развиваясь параллельно с убегающими вперед технологиями.

Литература

1. Соболева Т. А. «История шифровального дела в России». – М. : ОЛМА-ПРЕСС, 2002.
2. Сперанский М.Н. «Тайнопись в юго-славянских и русских памятниках письма». – Л., 1929.
3. Сумарокова Г.В. «Затаенное имя. Тайнопись в «Слове о полку Игореве». – МГУ, 1997.
4. «История русской разведки и контрразведки», http://www.agentura.ru/culture007/story/
5. Рерих А.В. Славяно-арийская письменность, http://tvoyhram.ru/slavrelig/slavrelig28.html
6. http://ru.wikipedia.org/wiki/Древнерусские тайнописи
7. «Что такое тайнопись?», http://potomy.ru/begin/2775.html

УДК 003.26.09

ПРОБЛЕМЫ ПРАКТИЧЕСКОГО ПРИМЕНЕНИЯ ШИФРА ВЕРМАНА

Гатченко Н.А., Исаев А.С., Яковлев А.Д.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

С глубокой древности и по настоящее время мы все чаще и чаще сталкиваемся с проблемой защиты окружающей нас информации. Проблема тайной передачи сообщений является одним из приоритетных направлении в развитии существующих систем криптографической защиты информации, большинство из которых так или иначе обеспечивают достаточно высокую вероятность сохранения конфиденциальности передаваемой информации. Однако в сложившихся тенденциях развития вычислительных способностей современных суперкомпьютеров, криптостойкость данных алгоритмов стремительно уменьшается. В связи с этим, становится все более и более актуальным вопрос использования шифра Вернама – единственного алгоритма шифрования для которого доказана абсолютная криптографическая стойкость, что, по сути, означает, что шифр Вернама является самой безопасной криптографической системой из всех существующих.

Шифр Вернама или «схема одноразовых блокнотов» – это система в которой для шифрования и расшифровывания применяется один и тот же криптографический ключ(симметричное шифрование), была изобретена сотрудниками компании AT&T Мейджором Джозефом Моборном и Нильбертом Вернамом в 1917 году. Для изготовления шифротекста открытый текст объединяется с ключом при помощи операции «исключающее ИЛИ», результат такой операции будет являться истинным только в случае, если является истинным в точности один из аргументов. При этом ключ или «одноразовый шифроблокнот» должен обладать рядом критически важных свойств:

1) быть истинно случайным;
2) совпадать по размеру с заданным открытым текстом (или превосходить его);
3) применяться только один раз;
4) после использования ключ должен быть уничтожен.

В 1949 году американский инженер и математик Клод Шеннон опубликовал работу в которой смог доказать абсолютную стойкость шифра Вернама. Не трудно догадаться, что требования при реализации такой схемы достаточно сложны, поскольку необходимо обеспечить не только наложение уникальной гаммы, равной длине сообщения но и гарантированно ее уничтожить. В связи с этим широкого коммерческого применения шифр Вернама не получил, ведь в большинстве случаев цена утраты сведений, составляющих коммерческую тайну, не превышает затрат на использование данного алгоритма, однако в случае особой важности сведении целесообразность применения шифра значительно увеличивается. В основном используется для передачи секретной информации государственными структурами. Область фактического применения достаточно велика, на практике можно один раз физически передать носитель информации с длинным истинно случайным ключом, а затем по мере необходимости пересылать сообщения. Используя идею шифроблокнотов, шифровальщик при личной встрече получает

шифроблокнот, каждая из страниц которого содержит ключ, такой же блокнот есть и у принимающей стороны, использованные страницы уничтожаются.

Проанализировав все области и условия применения шифра Вернама , мы выявили следующие существующие проблемы при использовании данной системы:

1) проблема непригодность псевдослучайных последовательностей;
2) проблема тайной передачи последовательности;
3) проблема надежного уничтожения использованных страниц шифроблокнота;
4) возможность восстановления ключа, при перехвате сообщения посторонними лицами;
5) проблема чувствительности системы к малейшему нарушению процесса шифрования.

Дело в том, что для работы шифра Вермана необходима истинно случайная последовательность нулей и единиц, однако по определению последовательность полученная с использованием любого алгоритма, является псевдослучайной, а, следовательно, необходимо использовать неалгоритмические методы получения ключа. Выход из данной ситуации достаточно прост, необходимо попросить помощи у физической составляющей процесса, предмету исследований квантовой криптографии, которая в отличии от традиционной криптографии использует не математические методы обеспечения секретности информации, а рассматривает процесс передачи информации с помощью объектов квантовой механики, ведь процесс передачи и приема информации всегда выполняется физическими средствами, такими как электроны в электрическом токе или фотоны в линиях оптоволоконной связи. Более того использование квантовой криптографии позволит нам так же избавиться от проблем пункта 2 и 4, приведенных выше.

Одной из основ квантовой криптографии является принцип неопределенности Гейзенберга, который гласит, что для любой квантовой системы невозможно одновременно получить координаты и импульс частицы, невозможно измерить один параметр фотона не исказив другой, а, следовательно, используя явления квантовой механики, возможно создать некую схему связи, которая всегда может обнаружить прослушку. Это обуславливается тем, что при каждой попытке измерения взаимосвязанных параметров внутри квантовой системы будет вноситься нарушение, разрушающее исходные сигналы, и по уровню шума в канале легитимные пользователи всегда смогут узнать о наличии третьей стороны и распознать степень активности перехватчика.

Рассмотрим простейший пример генерации секретного ключа. Отправляющая сторона (Алиса), используя случайный базис, передает принимающей стороне (Боб) некую последовательность фотонных импульсов, каждый из которых случайным образом поляризован в одном из четырех направлений, фотоны могут посылаться один за другим или все вместе, главное чтобы Алиса и Боб смогли однозначно установить взаимное соответствие между принятым и отправленным фотоном. В это же время Боб производит измерение принимаемых фотонов в одном из двух произвольно выбранных базисах. При этом в случае использования одинаковых базисов Алиса и Боб получат абсолютно коррелированные результаты, но в случае использования различных базисов результат будет противоположным. В итоге мы получим строку с 25% ошибок, которая называется «первичным ключом». Далее Боб при помощи открытых каналов связи сообщает Алисе о использованном базисе для каждого из фотонов, не оглашая результат , после чего Алиса передает в каких случаях базисы совпали. Если базисы совпали – бит оставляют, если нет – его попросту игнорируют. В таком случае примерно 50% данных выбрасывается, а

оставшийся набор бит образует новый «просеянный» ключ (табл. 1). В том случае если в канале не было шумов и прослушки обе стороны получают одинаковый набор случайных бит, который в дальнейшем и будут использовать для применения шифра Вернама, в противном случае полученные биты уничтожаются, в канале данных устраняются места утечки информации и процесс повторяется снова. Канал не прослушивается с вероятностью:

$1 - 2^{-k}$, где k – число сравненных битов.

Таблица 1. Передача и анализ истинно случайного ключа

Последовательность фотонов Алисы	|	/	/	–	\	|	|	–	–
Последовательность анализаторов Боба	+	X	+	+	X	X	X	+	+
«Первичный» ключ	0	0	1	1	1	0	1	1	0
Верные анализаторы	+	+		+	+			+	
Ключ	0	0		1	1			1	

Таким образом, мы можем исключить проблемы истинно случайных значений, тайной передачи последовательности и ее конфиденциальность. На настоящий момент не существует канала передачи данных, в которых исключена возможность перехвата данных, в противном случае криптография утратила бы свой смысл, зачастую частными предприятиями осуществляются передачи ключа системы Вернама с помощью других алгоритмов шифрования, таких как RSA, DES, но в таком случае мы получаем настолько же защищенный шифр на сколько защищены эти алгоритмы, что как мы уже выяснили не достаточно надежно. Проблема надежного уничтожения использованных страниц шифроблокнотов, а также других реализованных физических носителей информации является чисто организационной проблемой и может быть устранена лишь ужесточением контроля за уничтожением столь ценных данных.

Одно из основных достоинств шифра Вернама, также является и его главным недостатком – это чувствительность к любому нарушению процедур шифрования. В истории известны случаи, когда из перехваченной агентами АНБ США в 40-х годах прошлого века, были обнаружены сообщения, которые дважды закрыли при помощи одной и той же гаммы. И хотя период этот длился не долго (об успехах американских криптоаналитиков в спецслужбах СССР довольно быстро узнали о серьезных проблемах с надежностью в своей шифрпереписке), такие сообщения были расшифрованы в рамках секретного проекта «Venona», документы которого были не так давно рассекречены и выложены на всеобщее обозрение на сайте АНБ.

В данной работе мы проанализировали проблемы практического применения шифра Вернама, а также попытались предложить возможные пути их устранения, что в последующем приведет к развитию криптографии в целом. Несмотря на все недостатки и сложности в использовании шифра Вернама, эта схема одноразового блокнота является единственной системой с доказанной абсолютной криптографической стойкостью. А исходя из этого перед специалистами по защите информации стоит непростой выбор, между системами отличающимися простотой, доступностью, вероятной стойкостью и системой, стойкость (а значит и надежность) которой не вызывает сомнений.

Литература

1. Квантовая криптография: идеи и практика / под ред. С.Я. Килина, Д.Б. Хорошко, А.П. Низовцева. – Мн., 2008.

2. Синельников А. Шифры советской разведки.

3. Дональд Э. Кнут Случайные числа.

4. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. М. : Научный мир, 2004.

УДК 004.057.4

ПРОТИВОДЕЙСТВИЕ DDOS-АТАКАМ

Гиллунг А.И.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Научный руководитель – доц. Гирик А.В.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

DDoS – атака (от англ. Distributed Denial of Service, распределенная атака типа «отказ в обслуживании») – атака на вычислительную систему, выполняемая с большого количества компьютеров, с целью довести ее до отказа. То есть создать такие условия, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверам), либо этот доступ затруднен.

Изначально, DDoS – атаки использовались для проверки пропускной способности канала, однако, со временем киберпреступники осознали все вредоносные возможности этой технологии и приняли ее на свое «вооружение». Теперь DDOS-атаки используются киберпреступниками в самых различных целях: давление на пользователей; блокировка ключевых узлов сети Интернет; нарушение работоспособности интернет – сервисов компаний, бизнес которых основан на web-сервисах; в конкурентной борьбе; в политической конкуренции и т.д. Соответственно, прибыльность такого бизнеса достаточно высока. Последствия DDoS – атак могут привести к потере ключевых ресурсов сети, приложений и систем ведения бизнеса, репутационной потере, финансовым потерям и т.п. Так же DDoS – атаки могут использоваться для отвлечения внимания при запуске других вредоносных программ, например, для похищения конфиденциальных данных.

Целями таких атак является – создание условий, при которых правомерные пользователи лишаются возможности доступа к предоставляемым системой ресурсам (либо этот доступ оказывается затруднен). Сама по себе DDoS – атака выглядит как резко увеличивающееся количество трафика на атакуемом узле сети.

Существует несколько вариантов классификаций DDoS – атак по типам. Условно выделяется несколько методик, наиболее часто использующихся киберпреступниками:

1) Разрушающие – атаки, производимые таким способом, приводят к тому, что узел сети становится полностью недоступным: зависает, уничтожается операционная система, конфигурация устройства и т.п. Такие атаки производятся посредством уязвимостей, находящихся в программном обеспечении.

2) Атаки на ресурсы системы – при такой атаке формируется большое количество бессмысленных или сформированных в неправильном формате запросов к узлам сети или приложениям, что приводит к значительному снижению производительности компьютерной системы или сетевому оборудованию. Целью такой атаки является отказ работы системы из-за исчерпания ее ресурсов. Делятся на несколько видов:

– HTTP GET – целенаправленная, скоординированная отправка на web-сервер жертвы большого количества запросов с «зомби» - сети.

– DNS – flood (англ. flood – наводнение, затопление) – целенаправленная, специализированная отправка большого количества DNS запросов на DNS – сервер, при этом DNS – сервер становится не доступен для большого круга пользователей, т.к. его ресурсы заняты обработкой этих запросов.

– TCP SYN – flood – при этом типе атаки на атакуемый узел сети посылается большое количество запросов на открытие соединения. При этом атакуемому объекту приходится расходовать все свои ресурсы на отслеживание всех этих частично открытых соединений, что приводит к исчерпанию количества сокетов и устройство перестает отвечать.

– UDP – flood – этот тип атаки направлен на канал связи. На адрес атакуемой системы посылаются UDP запросы большого размера, при этом происходит быстрое исчерпание полосы пропускания канала связи, ведущего к атакуемой системе, и устройство, работающее по протоколу TCP, перестает отвечать.

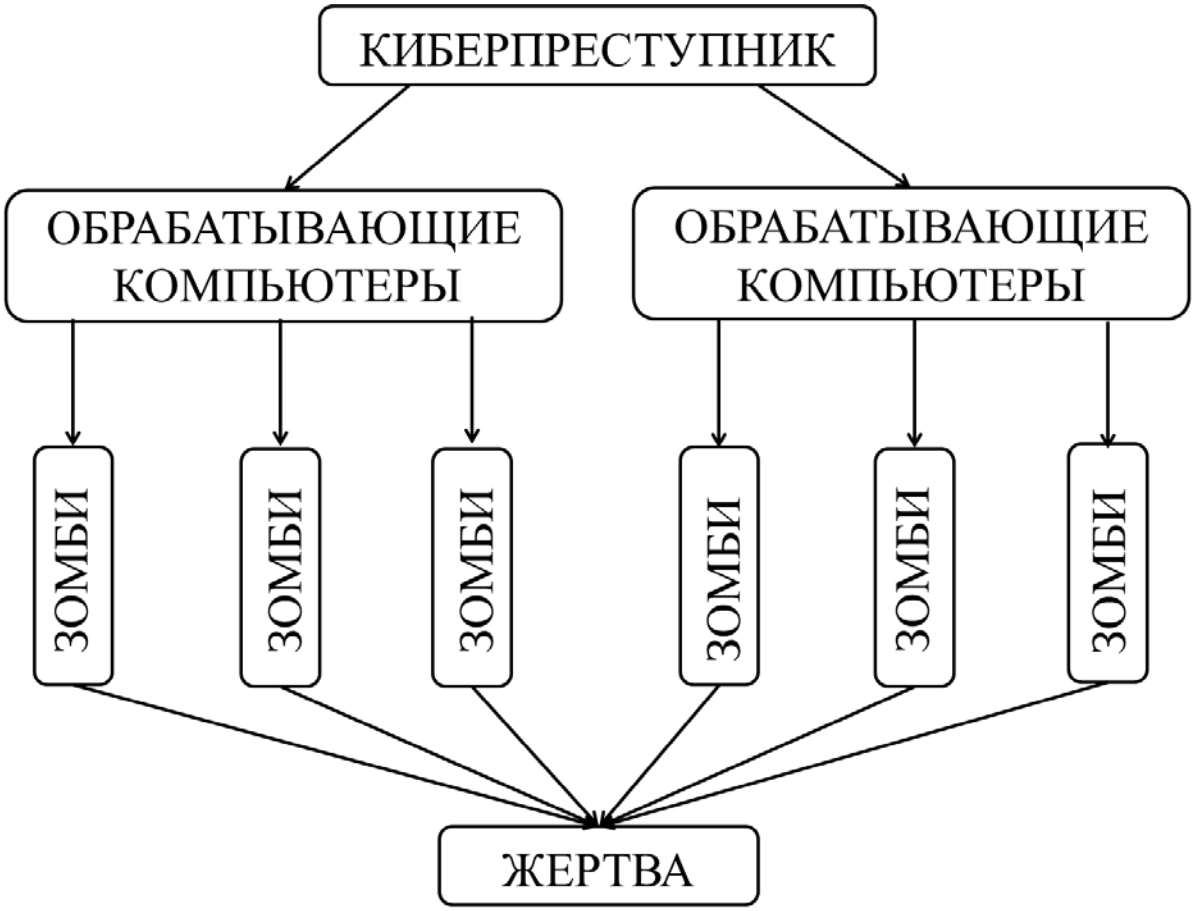
Чаще всего, при проведении DDoS – атаки используется несколько типов атак, что, в значительной степени осложняет противодействие DDoS – атакам.

В большинстве случаев, сеть, из которой производится DDoS – атака, имеет трех уровневую организацию. Такая сеть называется «кластер DDoS». Вверху кластера находятся один или несколько компьютеров, с которых начинается и координируется атака. На втором уровне – главные (обрабатывающие) компьютеры, которые непосредственно предают сигнал о начале атаки на следующий уровень. Третий уровень – заранее организованная ботнет сеть. Ботнет сеть – это сеть «компьютеров – зомби», попавших под управление киберпреступников после заражения их вредоносным кодом, обычно использующихся для неодобряемой или нелегальной деятельности – рассылка спам-писем, подборка паролей на удаленных компьютерах и сервисах, использование при проведении DDoS – атак. При достаточно большой степени изученности процесса образования ботнет сетей, противостояние киберпреступникам оказывается достаточно сложной задачей.

Дело в том, что обратный путь от жертвы к киберпреступнику проследить достаточно сложно, поэтому чаще всего они остаются не раскрытыми. Из-за этого обстоятельства и появился вид криминального бизнеса в сети Интеренет – создание ботнет сетей и последующая передача или сдача их в аренду заказчику для проведения DDoS – атак и рассылки спам – писем.

Практически во всех странах мира DDoS – атаки являются уголовным преступлением, но за решеткой их организаторы оказываются чрезвычайно редко. В наши дни организацией DDoS – атак занимаются не одиночки, а организованные преступные группы. Их разветвленность, организационная и географическая, позволяет успешно противостоять действиям правоохранительных органов. В российском законодательстве за преступления в компьютерной сфере предусмотрено 3 статьи уголовного кодекса РФ: выявление незаконного проникновения в

компьютерную сеть (ст. 272 УК РФ); борьба с распространителями вредоносных программ (ст. 273 УК РФ); выявление нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ).



Считается, что нет необходимости в специальных средствах обнаружения DDoS – атак, т.к. сам факт атаки не заметить невозможно, однако, достаточно часто отмечаются атаки, результат которых виден только через некоторое время.

Методы обнаружения DDoS – атак разделяются на несколько групп:

- сигнатурные – основанные на качественном анализе трафика;
- статистические – основанные на количественном анализе трафика;
- гибридные – сочетают в себе достоинства двух предыдущих методов.

Традиционные технические средства защиты (например, межсетевые экраны и системы обнаружения вторжений(IDS)) не противодействуют DDoS – атакам, т.к. они позволяют лишь либо запретить, либо разрешить прохождение сетевого трафика на основании анализа различных полей сетевых пакетов. Однако, атака может быть успешно реализована и в рамках разрешенных полей сетевых пакетов. Также практически невозможно отличить корректно-сформированный трафик от вредоносного, поскольку это те же самые запросы, что и от обычных пользователей, только генерируемые в несоизмеримо большем количестве. Киберпреступники используют еще одну технологию, называемую IP-spoofing (от англ. spoof – мистификация). Этот метод заключается в проставлении в поле обратного адреса IP-пакета неверного адреса и применяется для сокрытия истинного адреса атакующего, с целью вызвать ответный пакет на нужный адрес и с иными целями. Некоторые провайдеры используют технологию «Black-hole routing». Эта технология позволяет обнаруживать атаки на клиента или диапазон IP адресов и запрещает вход в

сеть некоторым IP адресам. Атака прекращается, но для клиента это выглядит как полное отключение от сети. Очевидно, что с крупными клиентами или важными данными так поступить невозможно, кроме того, атакующий может подставлять некоторые важные адреса(например, адреса корневых DNS).

Самым эффективным способом обнаружения DDoS – атак является использование специально разработанных для подавления DDoS – атак решений. Принцип их работы основан на обучении устройства тому, что может быть распознано как корректно-сформированный траффик и последующим выявлении аномалий. При выявлении аномалий включаются механизмы защиты разного уровня.

Одним из средств борьбы с DDoS-атаками является комплексное решение Cisco Clean Pipes. Особенностями данного комплекса является быстрое реагирование на проведение DDoS-атаки, легкая масштабируемость, высокая надежность и быстродействие. Комплекс Cisco Clean Pipes использует модули Cisco Anomaly Detector и Cisco Guard, а также системы статистического анализа сетевого трафика, получаемых с маршрутизаторов по протоколу Cisco Netflow.

В данном решении реализуется три уровня проверок:

1) фильтрация спуфинга;
2) выявление «зомби-компьютеров»;
3) блокирование траффика с атакующего адреса.

Anomaly Detector, как следует из названия, предназначен для обнаружения аномалий. Его задача – обучение, а затем обнаружение аномалий. Это пассивный элемент и через него траффик не проходит.

Cisco Guard (фильтр) – разбирает трафик на вредоносную и легитимную составляющие. Если детектор обнаруживает аномалии, то необходимо связать факт аномалии с DDoS-атакой. Для этого необходимо вмешаться в трафик и начать его анализировать. При этом детектор передает команду фильтру на контроль определенной зоны в сети и весь трафик зоны идет через него, таким образом на фильтр попадает только траффик содержащий атаку. Все остальное проходит мимо.

Такая схема позволяет уменьшить процент ложных срабатываний, экономия средств и увеличивается производительность фильтра.

Литература

1. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ред. от 21.07.2011)
2. Крис Касперски. Компьютерные вирусы изнутри и снаружи – Питер. – СПб : Питер, 2006. – С. 527. – ISBN 5-469-00982-3.
3. http://old.cio-world.ru/products/infrastructure/411180/
4. http://www.nestor.minsk.by/sr/2008/10/sr81004.html
5. http://www.outsourcing.ru/content/rus/277/2778-article.asp

ДЕЗИНФОРМАЦИЯ КАК ИНСТРУМЕНТ ПРОПАГАНДЫ НАСЕЛЕНИЯ

Гончаров А.Д., Гончаров С.А.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Сегодня мы живем в мире, где информация играет все более возрастающую роль в жизни людей, чему способствует стремительное развитие информационных технологий. Информация, наравне с материальными ресурсами, становится «лакомым кусочком» для отдельных индивидуумов, общественных организаций, а иногда и целых стран. Однако не вся информация одинаково «полезна». Издревле люди использовали заведомо ложные данные для введения в заблуждение своих оппонентов, извлекая тем самым пользу и выгоду для себя. В наше время масштабы дезинформации (от лат. des и informatio – ложная информация) достигли огромных размеров – ее целью становятся целые народы, государства и континенты.

В современном толковом словаре издательства «Большая Советская Энциклопедия» понятие «дезинформация» разъясняется как распространение искаженных или заведомо ложных сведений для достижения пропагандистских или других целей.

В военном деле дезинформация широко используется как один из способов политической агитации с целью обмануть население своей страны и оправдать милитаристские планы, направленные на развязывание боевых действий. Общечеловеческие и этические нормы поведения в данной ситуации уже не играют никакой роли.

Рассмотрим эту тему на примере весьма интересных и красноречивых фактов, взятых из новейшей истории, повествующих о том, как США готовили общественное мнение своей страны к началу вторжения в Ирак в 1991 году.

Факт 1: Ирак напал на независимое государство Кувейт.

На самом деле: Кувейт был на протяжении веков частью Ирака. И только Британские милитаристы оторвали его силой в 20-х годах 20 века, следуя политике «разделяй и властвуй». К тому же, ни одна страна Ближнего Востока не признала этого отделения.

Факт 2: Саддам Хусейн производит ядерное оружие и собирается применить его против Америки.

На самом деле: Планы производства ядерного оружия находились в зачаточном состоянии. Под таким предлогом можно бомбить большинство стран мира только за то, что они добились ощутимых результатов в исследовании ядерных реакций. Следовательно, намерения Хусейна напасть на США выглядят, конечно, чистой выдумкой.

Факт 3: Ирак не желает начинать мирные переговоры с Кувейтом и выводить свои войска.

На самом деле: Когда войска НАТО атаковали Кувейт, мирные переговоры уже шли полным ходом, а иракская армия покидала страну.

Рисунок 1. Саддам Хусейн

Факт 4: Чудовищные зверства, проводимые иракской армией в Кувейте.

На самом деле: Самые страшные зверства, типа кадров с убийством младенцев, были весьма умело выдуманы американской пропагандой. Хусейн был не настолько глуп, чтобы учинять бессмысленное кровопролитие народа, которым собирался впоследствии управлять.

Факт 5: Применение оружия массового уничтожения иракской армией.

На самом деле: США сами же, вплоть до 1991 года, поставляли Хусейну это оружие для войны с Ираном, Кувейтом и для подавления народных волнений внутри своей страны.

Огромную роль в формировании общественного мнения в самих США, поддерживающих 1-ую войну против Ирака, сыграли телекадры, где 15-летняя девочка, которую представляли как кувейтскую беженку, рассказывала, что она видела своими глазами, как иракские солдаты вытащили 312 младенцев-кувейтцев из роддома, и положили их на бетонный пол умирать с целью забрать инкубаторы, где находились эти младенцы. Интервью с этой девочкой крутили по американскому ТВ перед войной сотни раз. Надо признать, что она исполнила свою роль мастерски, даже заплакала. При этом у многих, кто это видел, тоже стояли слезы на глазах. Имя этого ребенка скрывали, потому что у нее, якобы, осталась семья в Кувейте, которая может пострадать от солдат Хусейна. Для того чтобы понять, каким важным фактором был этот ролик, добавим, что президент Джордж Буш-старший использовал рассказ о мертвых младенцах десять раз за сорок дней предвоенной пропагандистской кампании. К интервью неоднократно апеллировали члены американского Сената при решении вопроса, посылать ли войска в Залив.

Рисунок 2. Джордж Буш-старший

Впоследствии, однако, было доказано, что показанная по ТВ девочка - никакая не беженка, а дочь посла Кувейта в США, которая проживала на территории Соединенных Штатов и потому

никак не могла быть очевидцем оккупации Кувейта. Более того, она – член королевской фамилии, управляющей Кувейтом. Все ее родственники имеют огромные состояния, поместья за границей и проживают преимущественно в США и странах Запада, так что ее семья не могла пострадать, даже если бы девочка выступала под своим именем.

Весь этот пиар-трюк был заказан американским правительством фирме «Хилл энд Ноултон», которая занимается производством рекламы. Фирма проанализировала и выяснила, что американская общественность больше всего ненавидит людей, совершающих насилие над детьми. Поэтому именно такой сюжет был выдуман для раскручивания войны с Ираком. Впоследствии обман выплыл из-за того, что некоторые дотошные журналисты не поленились поехать в тот самый роддом и попытались поговорить с работниками и начальством. Оказалось, что ни о каком убийстве младенцев там и не слышали. Иракцы хотя и заглянули во время войны в это здание, но ограничились воровством стульев. Специальные «инкубаторы» для младенцев, которые они по сообщению девочки увезли с собой, до сих пор стоят на месте и служат своей цели.

Перед нами фальсификация, которая сознательно была выполнена телевизионщиками по заказу сторонников войны из администрации президента. Разумеется, сам президент Буш-старший не мог этого не знать. Выходит, что он сознательно манипулировал мнением миллионов простых американцев ради достижения своих политических целей.

Уже во время самой войны в Персидском Заливе ненависть к Ираку нагнетали также душераздирающими кадрами, где добровольцы из числа «зеленых» обмывают мылом бедных птиц, попавших в нефтяное пятно, разлитое жестокими иракцами. Однако вскоре после этого публикуется сообщение, что это кадры из репортажа, снятого на Аляске, где на скалы сел танкер, разливший 70 тыс. тонн нефти. То есть громогласно заявляется, что ведущие телеканалы всего мира сознательно фальсифицировали информацию. И что? Никакого эффекта. Ни слушаний в парламентах, ни обращений в суды, ни резолюций ООН...

При этом в Америке все чаще перекрывают доступ к независимой информации об Ираке (т.е. к очищенной от американской пропаганды). В самом же Ираке употребляются все более жесткие методы борьбы со свободой слова. Когда 2 корреспондента «Рейтер» посмели заснять горящий американский вертолет, по ним просто открыли огонь, а потом арестовали. При этом представитель американских военных заявил, что «корреспонденты «Рейтер» стреляли по ним из пулеметов и ручных гранатометов...»

Таким образом, на примере выше перечисленного, мы видим, что умело отработанная дезинформация побуждает общественность поддерживать конкретную линию политики страны, распространяющей эти данные. Главное – как люди воспринимают такого рода «информацию».

Из всего этого вытекает главный вывод, что человеческий фактор является основным как в процессе создания ложной информации, ее осмыслении, так и в принятии по этой информации последующих, далеко идущих решений.

Рисунок 3. Горящие нефтяные скважины

Литература

1. Доронин А. статья «Дезинформация или война в королевстве кривых зеркал», 2007.
2. Почепцов Г.Г. статья «Информация и дезинформация», 2004.
3. Российская социологическая энциклопедия.
4. Толковый словарь издательства «Большая Советская Энциклопедия».
5. Цубрикова Н.Н. «Политика дезинформации посредством сети Интернет» // Межвузовский сборник научно-технических статей. – СПб, 2010.
6. «Агрессия против Ирака» . http://panteon-istorii.narod.ru/sob/irak.htm

УДК 004.7

АНАЛИЗ СРЕДСТВ ОТЧЕТНОСТИ И МОНИТОРИНГА ДОСТУПА В ИНТЕРНЕТ

Ендовский А.С.
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Научный руководитель – доц. Хромов И.Н.
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Для целей безопасного использования ресурсов сети Интернет, а так же возможности мониторинга посещенных ресурсов используются прокси-сервера. В данной работе будет проведен сравнительный анализ трех наиболее широко используемых прокси-серверов: Squid, Traffic Inspector и Microsoft Forefront Threat Management Gateway 2010.

Прокси-сервер – служба, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс, расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кэша

ресурсов (если таковой имеется). В некоторых случаях запрос клиента или ответ сервера может быть изменен прокси-сервером в определенных целях. Также прокси-сервер позволяет защищать клиентский компьютер от некоторых сетевых атак и помогает сохранять анонимность клиента. Общий принцип работы прокси-сервера изображен на рис. 1.

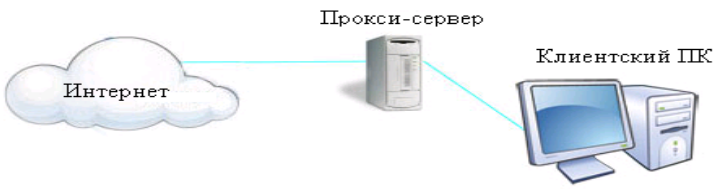


Рисунок 1. Общий принцип работы прокси-сервера

Squid

Программный пакет, реализующий функцию кэширующего прокси-сервера для протоколов HTTP и HTTPS. Разработан сообществом как программа с открытым исходным кодом (распространяется в соответствии с лицензией GNU GPL). Все запросы выполняет как один неблокируемый процесс ввода/вывода.

Используется в UNIX-like системах и в ОС семейства Windows NT. Имеет возможность взаимодействия с Active Directory Windows Server путем аутентификации через LDAP, что позволяет использовать разграничения доступа к интернет ресурсам пользователей, которые имеют учетные записи на Windows Server.

Внешний вид и средства администрирования

Squid не имеет пользовательского интерфейса, настраивается напрямую из командной строки FreeBSD. Конфигурирование происходит средствами командной строки, вводом в конфигурационные файлы необходимых команд (рис. 2).

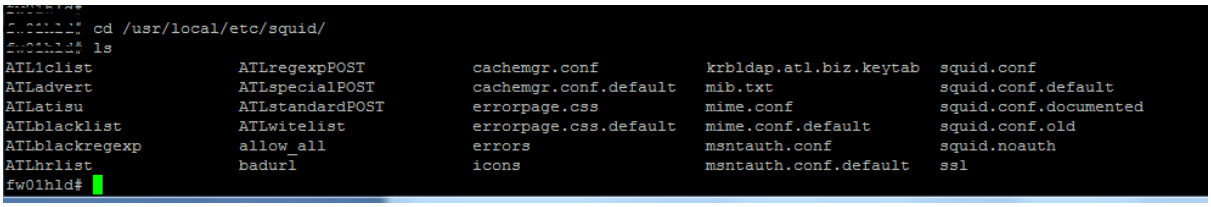


Рисунок 2. Командная строка Squid в FreeBSD

Возможности

Организация контроля доступа в интернет по спискам. Ограничение доступа к ресурсам сети Интернет так же происходит по спискам (ACL).

Отчетность

Squid не имеет встроенных средств отчетности. Для генерирования отчетности используются настройки, управляемые так же из командной строки. Просмотр возможен только через браузер, градация по отчетам за день, неделю и месяц. Сортировка по умолчанию производится по количеству трафика. Пример отчета – рис. 3.

www.gtkvostok.ru	10.08M	4.83%	0.09%	99.91%	00:00:30	30.461	0.16%	
urs.microsoft.com:443	9.18M	4.40%	2.07%	97.93%	01:28:21	5.301.417	27.30%	
www.ushurika.ru	8.15M	3.91%	0.06%	99.94%	00:00:47	47.460	0.24%	
yandex.st	5.98M	2.87%	78.92%	21.08%	00:00:34	34.836	0.18%	
api-maps.yandex.ru	5.97M	2.87%	75.78%	24.22%	00:00:46	46.228	0.24%	
yandex.ru	4.83M	2.32%	1.56%	98.44%	00:02:34	154.062	0.79%	
samara24.ru	4.46M	2.14%	12.52%	87.48%	00:00:31	31.142	0.16%	
www.yandex.ru	4.36M	2.09%	0.00%	100.00%	00:00:26	26.627	0.14%	
www.razgulyay-samara.ru	4.02M	1.93%	11.29%	88.71%	00:02:44	164.002	0.84%	
www.kupikupon.ru	3.74M	1.80%	0.54%	99.46%	00:00:59	59.026	0.30%	DENIED
brand-bag5.ru	3.73M	1.79%	0.21%	99.79%	00:01:17	77.491	0.40%	
crocus-elite.ru	3.64M	1.75%	0.12%	99.88%	00:01:07	67.597	0.35%	
i.kuponator.ru	3.60M	1.73%	74.32%	25.68%	00:00:52	52.443	0.27%	
boo.plusmedia.ru	3.58M	1.72%	19.38%	80.62%	00:03:27	207.572	1.07%	
gmstar.ru	3.50M	1.68%	64.94%	35.06%	00:00:35	35.809	0.18%	
vec01.maps.yandex.net	3.44M	1.65%	36.02%	63.98%	00:00:34	34.042	0.18%	
vec03.maps.yandex.net	3.44M	1.65%	36.10%	63.90%	00:00:36	36.000	0.19%	
vec02.maps.yandex.net	3.04M	1.46%	36.75%	63.25%	00:01:13	73.423	0.38%	
vec04.maps.yandex.net	3.02M	1.45%	38.94%	61.06%	00:00:36	36.078	0.19%	
an.yandex.ru	2.89M	1.39%	23.37%	76.63%	00:01:30	90.401	0.47%	
www.rutector.ru	2.83M	1.36%	0.00%	100.00%	00:00:24	24.054	0.12%	
tarif.riccom.ru	2.49M	1.19%	0.00%	100.00%	00:00:42	42.447	0.22%	
mc.yandex.ru	2.36M	1.13%	79.56%	20.44%	00:03:52	232.973	1.20%	DENIED
www.metaprom.ru	2.13M	1.02%	4.52%	95.48%	00:03:55	235.924	1.21%	
www.jam-club.org	2.12M	1.02%	0.43%	99.57%	00:00:42	42.154	0.22%	
pagead2.googlesyndication.com	1.99M	0.96%	54.66%	45.34%	00:00:30	30.413	0.16%	
googleads.g.doubleclick.net	1.87M	0.90%	3.27%	96.73%	00:03:11	191.747	0.99%	
www.restoranchik.ru	1.85M	0.89%	0.22%	99.78%	00:00:20	20.040	0.10%	DENIED
dosug.samara24.ru	1.79M	0.86%	1.29%	98.71%	00:00:22	22.183	0.11%	
maps.gstatic.com	1.70M	0.82%	13.04%	86.96%	00:00:18	18.548	0.10%	
www.postroy63.ru	1.66M	0.80%	33.83%	66.17%	00:02:43	163.444	0.84%	

Рисунок 3. Пример отчета Squid

Наличие поддержки

Squid является свободным ПО и не имеет технической поддержки ни в РФ, ни за ее пределами. Существуют технические форумы, где пользователи делятся опытом работы.

Стоимость

Бесплатно.

Traffic Inspector

Прокси-сервер для операционной системы Microsoft Windows. Основные задачи программы – организация доступа в Интернет, надежная сетевая защита, экономия трафика и рабочего времени, сертифицированный биллинг. Данный программный продукт имеет следующие сертификаты:

- ФСТЭК РФ;
- сертификат соответствия № 2407;
- сертификат соответствия Минсвязи. [2]

Внешний вид и средства администрирования

Имеет обширную панель управления на базе консоли управления Microsoft, позволяющей наглядно и удобно изменять конфигурацию прокси-сервера (рис. 4).

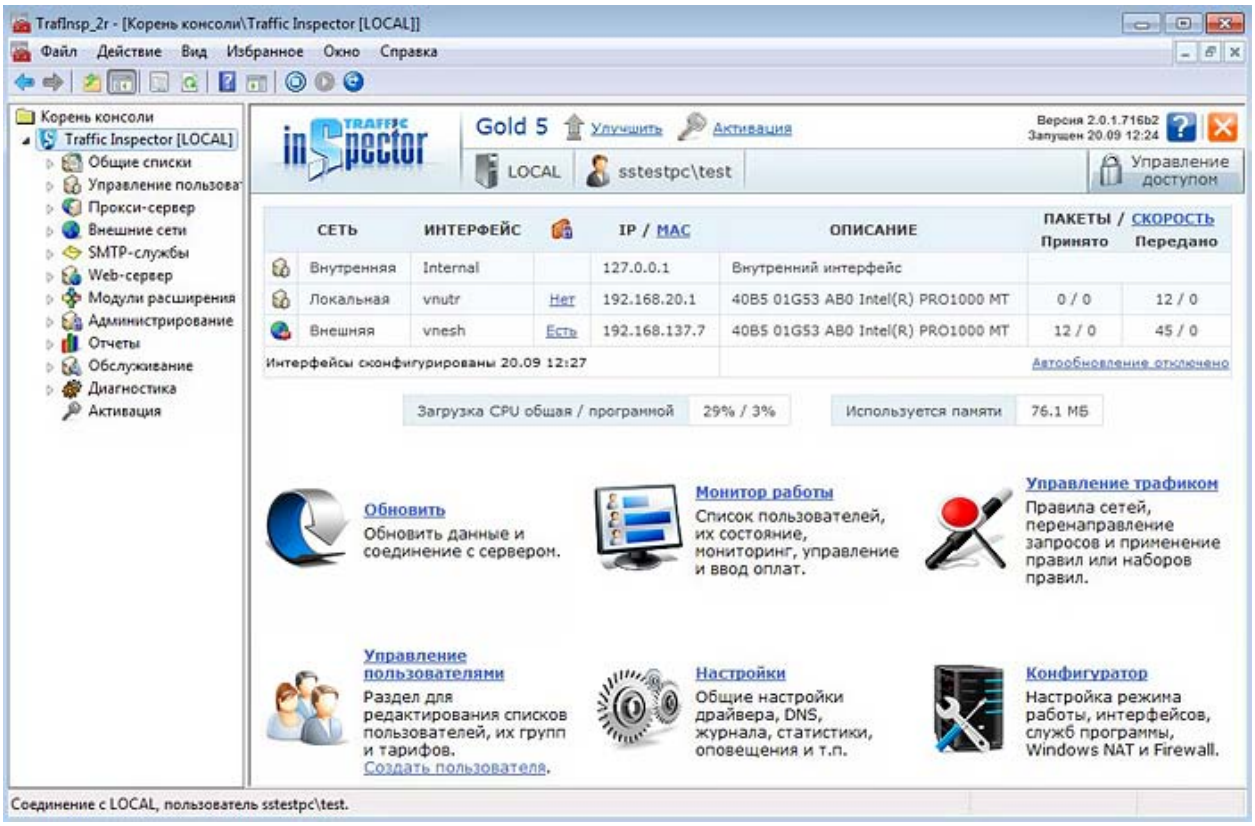


Рисунок 4. Панель управления Traffic Inspector

Возможности:

- индивидуальная/групповая тарификация;
- межсетевой экран;
- динамическое управление шириной канала;
- гибкая система фильтров;
- двойная антивирусная защита;
- фильтрация спама;
- использование различных каналов доступа;
- мониторинг сетевой активности;
- поддержка IP-телефонии;
- поддержка VPN;
- биллинг;
- управляемое кэширование;
- маршрутизация;
- клиентский агент.

Отчетность

Traffic Inspector предоставляет широкие возможности биллинга и отчетности. **Учет трафика** четко разделяется на «внешний» и «внутренний». Внешний – это трафик, полученный от провайдера, внутренний – отданный пользователям. Внешний трафик может быть детально разделен по подключениям, провайдерам, серверам, сетям и протоколам. Есть возможность составления отчетов по каждому пользователю, по любому периоду времени, по текущим соединениям и др. Все отчеты наглядны и имеют понятный интерфейс настройки (рис. 5).

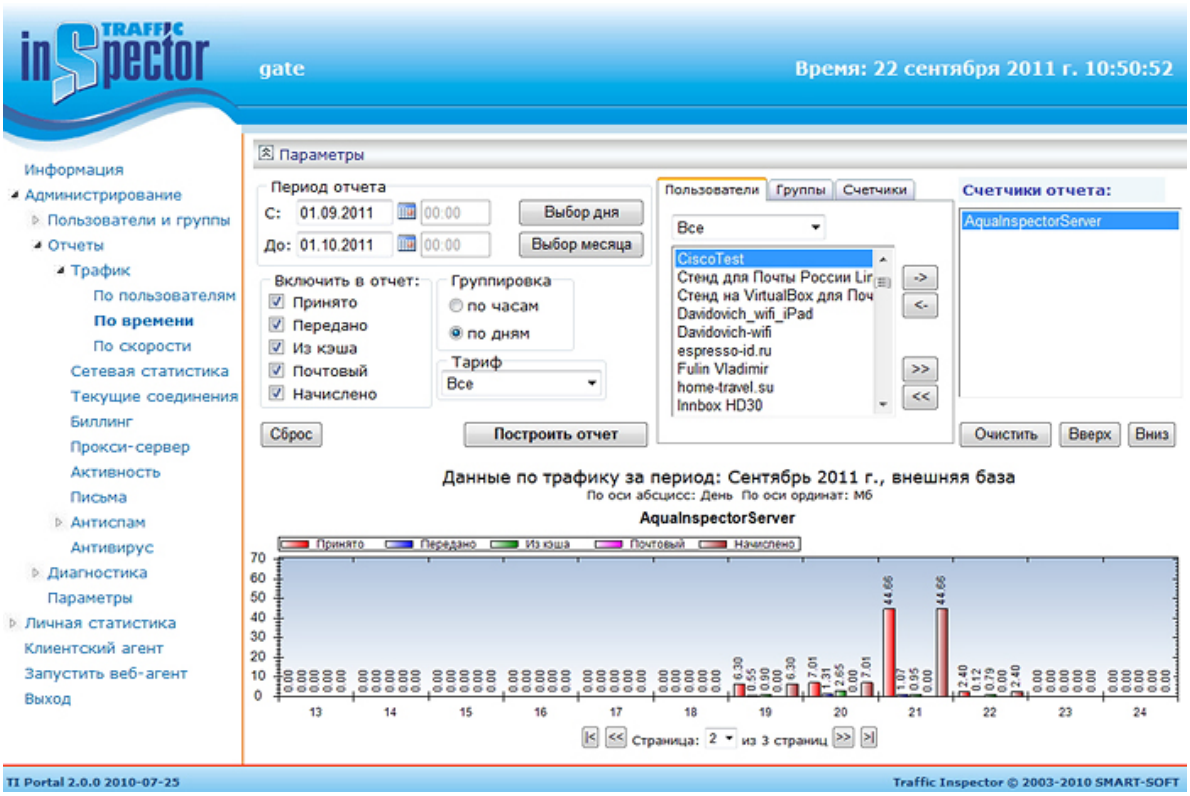


Рисунок 5. Отчеты Traffic Inspector

Наличие поддержки

Traffic Inspector имеет сертифицированную техническую поддержку в РФ по телефону или электронной почте в рабочее время, а так же собственный ресурс «базы знаний» и форум технических специалистов на русском языке.

Стоимость

Цена зависит от количества учетных записей, с которыми будет работать ПО, в стоимость так же входит доступ к технической поддержке (расширенная в течение года).

Учетных записей	Цена, руб.
5	3800
20	11200
100	30000
Без лимита	52900

Microsoft Forefront Threat Management Gateway

Прокси-сервер для защиты сети от атак извне, а также контроля интернет-трафика. Пришел на смену прокси-серверу Microsoft Internet Security and Acceleration Server (ISA Server) Позволяет организовать защиту локальной сети от вмешательств из сети Интернет и безопасно публиковать различные виды серверов, дает возможность распределять доступ пользователей локальной сети к ресурсам Интернет. Оснащен средствами для анализа посещаемых ресурсов, учета трафика, а также защиты против атак из сети Интернет. [1]

Внешний вид и средства администрирования

Microsoft Threat Management Gateway (TMG) управляется средствами консоли управления Microsoft (рис. 6).

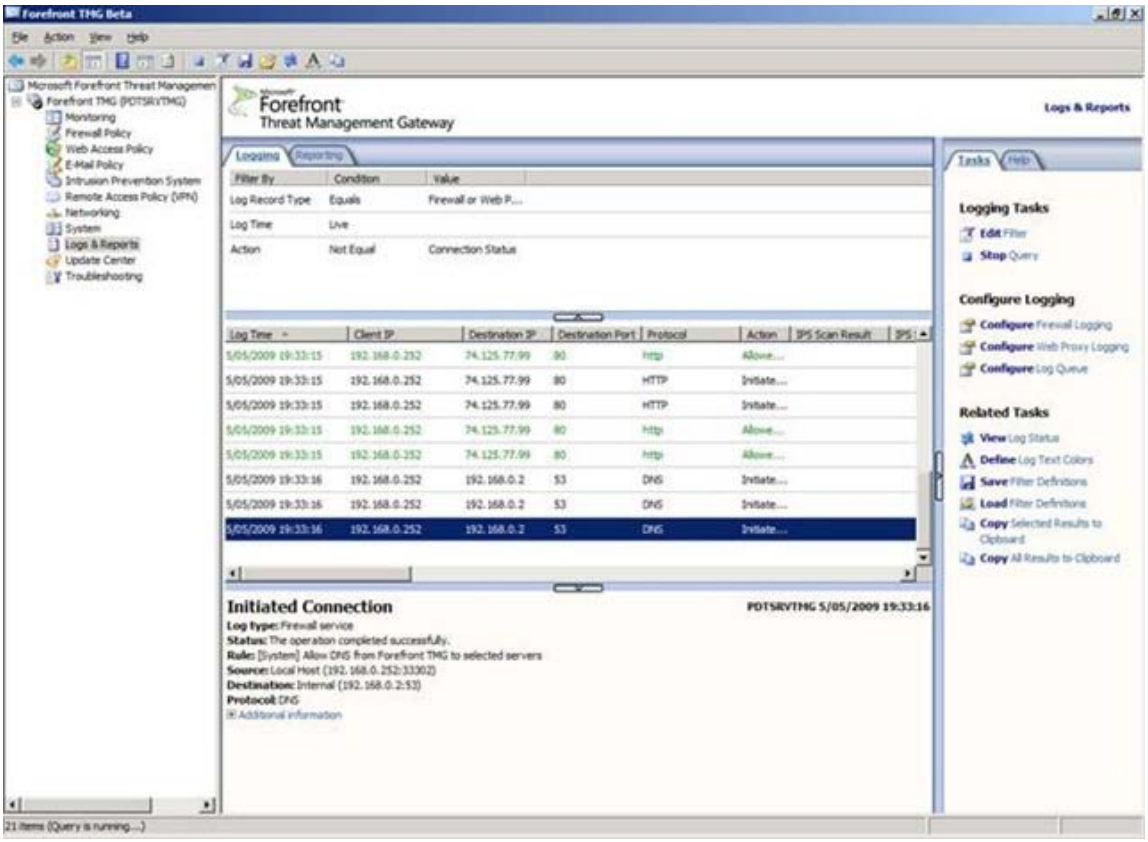


Рисунок 6. Оснастка TMG для консоли управления Microsoft

Возможности

- фильтрация адресов;
- расширенное преобразование сетевых адресов (NAT);
- защита от вредоносных интернет-программ.

Отчетность

TMG содержит развитую систему отчетности (рис. 7).

Наличие поддержки

Техническая поддержка по электронной почте.

Стоимость

Единовременная покупка (Open License) – 40441 руб.

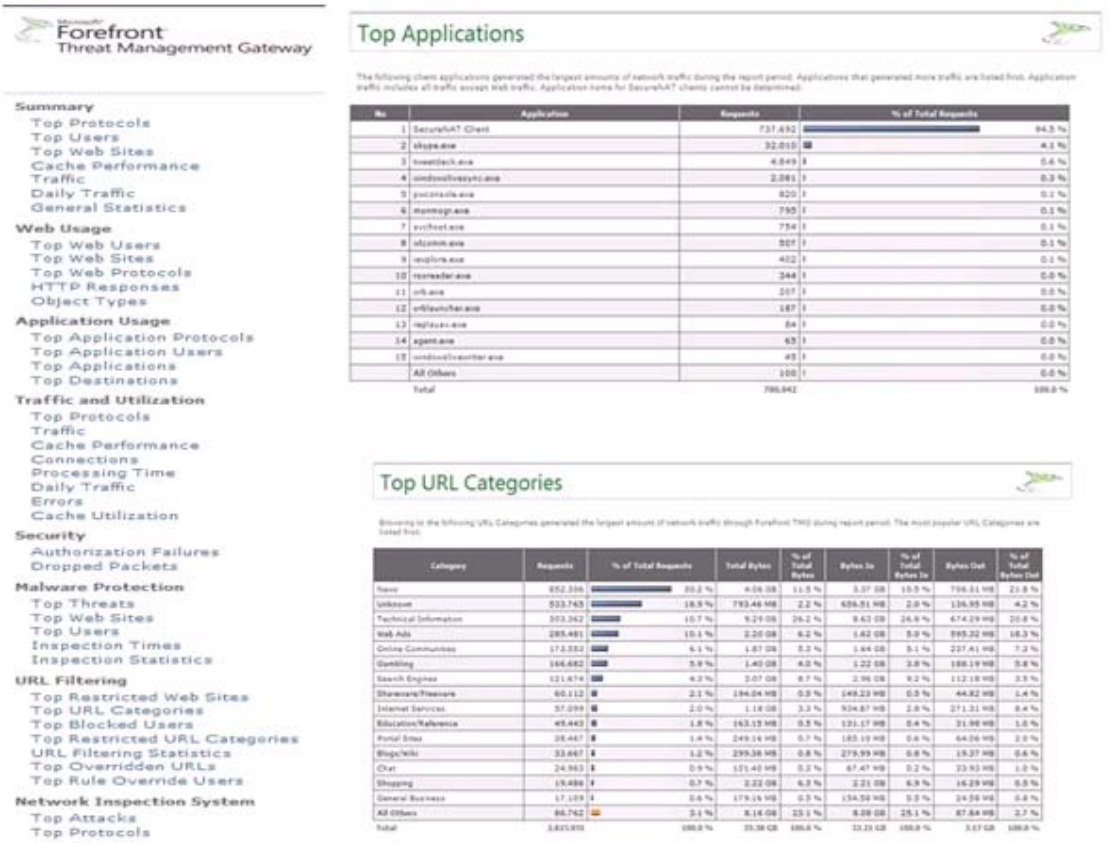


Рисунок 7. Отчетность TMG

Сводная таблица возможностей сравниваемых прокси-серверов

ПО/Опция	Squid	Traffic Inspecotr	TMG
Интерфейс GUI	–	+	+
Система отчетности	–	+	*
Возможность тарификации	–	+	–
Встроенный Firewall	–	+	+
NAT	–	+	+
Встроенный антивирус	–	+	+
Техническая поддержка	–	+	*
Цена (руб)	0	52900	40441

Не смотря на стабильность работы Squid, данное ПО очень ограничено в функционале и простоте настроек, просмотра отчетности. TMG в свою очередь значительно выше по классу, чем Squid, но в целях обеспечения корректного разграничения доступа к ресурсам сети Интернет, расширения функционала контроля трафика (таких как реализации возможности биллинга, создания отчетов и тонкой настройки) лучше всего использовать программный прокси-сервер Traffic Inspector. Помимо вышеперечисленного, с данным ПО предоставляется полноценная техническая поддержка, которая очень важна, в особенности для организаций с небольшим штатом специалистов в области информационных технологий.

Литература

1. http://microsoft.com/en-us/server-cloud/forefront/threat-management-gateway.aspx
2. http://smart-soft.ru
3. http://squid.opennet.ru

УДК 51-7

МОДЕЛИРОВАНИЕ РАБОТЫ ПРОФЕССОРСКО-ПРЕПОДАВАТЕЛЬСКОГО СОСТАВА УНИВЕРСИТЕТА

Казакова Д.С.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Научный руководитель – к.т.н., доц. Жигулин Г.П.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В работе рассмотрена деятельность профессорско-преподавательского состава университета, моделирование которой важно для правильной организации научного процесса, особенно когда идет речь об университете, имеющем статус «национальный исследовательский университет». Систематизированы материалы для разработки теоретической части модели, содержащей данные о должностных и функциональных обязанностях, принципах их распределения в профессорско-преподавательском коллективе. Проведена классификация факторов, характеризующих личность преподавателя. Показана актуальность разработки модели для грамотного планирования рабочего времени преподавателей в высшем учебном заведении.

На основе анализа деятельности профессорско-преподавательского коллектива была составлена модель личности работника университета, в которой подробно проанализированы психолого-личностные характеристики, уровень квалификации, функциональные обязанности при работе, как в стране, так и за рубежом. Для удобного использования модели была разработана база данных. Она позволяет хранить, консолидировать и использовать имеющуюся информацию о коллективе.

Для моделирования использовался аддитивный метод расчета весовых коэффициентов для оценки каждого из сотрудников. Рассчитываются параметры, показывающие: личностные характеристики, соответствие занимаемой должности, первоначальное положение человека и его достижения, возможность повышения. Так же важным показателем является коэффициент предпочтений, учитывая который мы сможем избежать обременительных обязанностей.

Для понимания и закрепления теоретических знаний разработан набор ситуационных задач, которые могут возникнуть. Это кадровые вопросы, возникающие при различных ситуациях на определенной кафедре или в университете. Приведены их решения с помощью модели.

Созданная модель может быть внедрена в любой профессорско-преподавательский коллектив, на любой кафедре высшего учебного заведения. Можно легко дополнять и

редактировать составляющие, как базы данных, так и постановку кадрового вопроса в зависимости от специфики кафедры и решаемых вопросов, что придает модели определенную эластичность. Использование этой модели позволяет легко найти и опробовать решения кадровых вопросов, не нанося неудобств работе профессорско-преподавательскому составу университета, что повышает эффективность учебного процесса.

Использование разработанной модели в учебном процессе позволяет сэкономить время при распределении должностных обязанностей, снизить риск принятия неверного решения и способствует повышению качества образования.

Литература

1. Базаров Т.Ю., Еремин Б.Л. Управление персоналом. – М., 1998.
2. Богатырь Б.Н. Система образования России как объект информатизации // Материалы школы-семинара «Создание единого информационного пространства системы образования» (г. Москва) 3–5 ноября 2006 г. – М., 2007.
3. Богдан Н.Н., Могилевкин Е.А. «Кадровый менеджмент в вузе». – ВГУЭС, 2008.
4. Веснин В.Р. Практический менеджмент персонала. – М., 1998.
5. Жигулин Г.П. Прогнозирование устойчивости субъекта информационного взаимодействия. – СПб : СПб ГУ ИТМО, 2006.
6. Ниссинен Й., Воутилайнен Э., «Время руководителя: эффективность использования». – М. : Экономика, 1998.
7. Сальникова Л.Н. Управление персоналом: учебное пособие. – Ярославль : Ярославский государственный ун-т, 1999.
8. Спивак В.А. Организационное поведение и управление персоналом. – СПб: «Питер», 2000.
9. Официальные интернет порталы: http://ru.wikipedia.org.

УДК 623.004

О ВОЗМОЖНОСТИ ПРИМЕНЕНИИ МЕТОДИКИ МАТЕМАТИЧЕСКОГО АНАЛИЗА ВЕРОЯТНОСТНЫХ ХАРАКТЕРИСТИК ЭЛЕМЕНТОВ СИСТЕМЫ ЗАЩИТЫ СЕТЕВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Кириленко Д.А., Круглов А.А.
46 ЦНИИ Минобороны

В настоящее время во всем мире резко повысилось внимание к проблеме информационной безопасности. Это обусловлено повсеместным использованием информационных технологий в различных сферах человеческой деятельности. К значительной части информации предъявляются требования по обеспечению определенной степени конфиденциальности. Особенно актуальны эти требования для сетевых информационных систем (СИС) специального назначения, поскольку они предназначены, как правило, для передачи конфиденциальной информации. Функции обработки информации в таких системах реализуются на объектах информатизации (ОИ).

Отличительной особенностью таких ОИ, как элементов СИС, является комплексное использование на них информационных и телекоммуникационных технологий, что вызывает необходимость применения более широкого спектра механизмов защиты информации, чем на обособленных автоматизированных рабочих местах. Вместе с тем, анализ существующей литературы в области защиты информации, описывающей в основном механизмы обеспечения компьютерной безопасности, позволяет сделать вывод о явной недостаточности теоретической проработки проблемы для ОИ СИС. Требования к уровню защиты СИС определяются видом воздействия противника, его глубиной и интенсивностью, то есть степенью угрозы сообщению. В задачу систем защиты информационных ресурсов входит анализ уровня вредоносного воздействия со стороны противника и принятие адекватного решения – противодействия вторжению по результатам анализа. Следовательно, *разработка вопроса обеспечения информационной безопасности СИС является особенно актуальной в современных условиях.*

В этой связи возникает необходимость разработки и применения методики математического анализа, позволяющей оценить по известным характеристикам возмущающих факторов (ВФ), в том числе интенсивности атак на шифр, на входе элементов системы защиты (СЗ) и заданным параметрам элементов СЗ характеристики ВФ, прошедших через элемент СЗ, что позволит качественно оценить уровень защищенности СИС.

Для исследования основных процессов, протекающих в элементах СЗ на основе имитации свойств технических средств защиты и внешних воздействий, необходимо математически описать свойства элементов СЗ и внешних воздействий, то есть построить математические модели, описывающие эволюцию состояний элемента СЗ и появление внешних воздействий. Следовательно, *объектом исследования является постановка и решение основной задачи определения характеристик потока воздействий ВФ, прошедших через элемент СЗ*.

В ряде работ приведены модели функционирования элементов СЗ и рассмотрены процессы их эволюции для различных условий функционирования.

Так, при постановке *задачи расчета распределения момента первого пропуска ВФ в явном виде*, эволюция элемента СЗ может быть описана некоторым случайным процессом с некоторым фазовым пространством. Моменты появления ВФ образуют некоторый процесс однородных событий. Задача исследования такой модели состоит в том, чтобы исследовать поток моментов появления возмущающих воздействий, попавших в систему защиты тогда, когда элемент системы находился в состоянии неработоспособности. Предполагается, что когда элемент СЗ работоспособен в момент поступления ВФ, то это воздействие теряется, а в противном случае ВФ проходит элемент защиты. При конкретной постановке задачи предполагается, что эволюция состояний элемента СЗ описывается полумарковским процессом с конечным множеством состояний и полумарковской матрицей. Относительно моментов появления ВФ, считается, что они образуют пуассоновский поток с некоторым параметром. Такое предположение делается в силу того, что процесс ВФ можно представить в виде суммы большого числа независимых редких потоков, образующих в конечном итоге поток ВФ. В таком случае суммарный предельный поток ВФ на основании предельной теоремы Григелиониса является пуассоновским потоком. Множество состояний процесса эволюции СЗ включает подмножества состояний работоспособности и неработоспособности. Так, если воздействие поступает в момент, когда элемент СЗ находится в состоянии работоспособности, то воздействие не проходит, а если в состоянии неработоспособности, то защита не срабатывает.

Описанная выше схема укладывается в общую модель полумарковского процесса с «катастрофами». Подобные задачи рассматривались специалистами в постановке для регенерирующих процессов [1].

Кроме вышесказанного, в литературе приводится модель функционирования элементов СЗ для случаев, когда необходимо решить задачу *выбора оптимального управления, максимизирующего ожидание времени до первого пропуска ВФ.* Такие модели описывают решение оптимизационной задачи при условии, что полумарковский процесс, описывающий эволюцию элемента СЗ, является управляемым, что так и есть на практике.

Так как для марковского случая момент первого пропуска ВФ происходит в марковский момент, то поток моментов пропуска ВФ образует процесс восстановлений с запаздыванием. Его вероятностные характеристики важны для описания модели и исследованы в ряде работ [2,3].

По формуле полной вероятности, учитывая, что смена состояний полумарковского процесса осуществляется в марковские моменты времени, получают систему интегральных уравнений, которую решают методом Лапласа, так как в нее входят интегральные свертки. В этом случае основная трудность заключается в обращении преобразования Лапласа для получения решения.

Ряд работ посвящен *вопросу исследования математического ожидания времени до* **первого** *пропуска ВФ*. При рассмотрении таких моделей эксплуатации значительно упрощается решение задачи расчета искомых величин в явном виде. По формуле полного математического ожидания выписывают систему линейных алгебраических уравнений, при решении которой получают ответ в замкнутом виде.

На практике может представлять интерес *распределение момента первого пропуска внешнего воздействия в стационарном случае*, то есть когда попытка НСД не повторяется, либо повторится через значительный интервал времени. Тогда эволюция состояний элемента СЗ описывается альтернирующим процессом восстановления и полумарковский процесс имеет два состояния. Такая модель рассмотрена [2, 3, 6] и позволяет получить в явном виде значения вероятностей отказов и восстановлений, а также соответствующие распределения и математические ожидания, что на практике позволяет спрогнозировать время отказа СЗ при определенном наборе и интенсивности ВФ.

Так как моменты пропуска ВФ являются марковскими, поток этих моментов является потоком восстановления с запаздыванием, у которого распределение первого интервала определяется в зависимости от начального распределения вероятностей отказов и восстановлений, а распределение последующих интервалов определяется исходя из условия работоспособности СЗ.

Рассмотренные выше модели функционирования рассчитаны на стационарные случаи и не позволяют оценивать распределения моментов пропуска ВФ и их математические ожидания в динамических системах, то есть в случаях, когда первый пропуск ВФ не является летальным для всей СЗ СИС. В связи с этим, для учета возможности повторяющегося воздействия ВФ и восстановления элемента СЗ, **предлагается** *решение оптимизационной задачи для поиска распределения момента первого пропуска внешнего воздействия*.

Пусть элемент СЗ имеет время безотказной работы ξ. Когда элемент работоспособен, назначаем проведение плановой предупредительной профилактики через время η. Если $\xi > \eta$, то

в моментη начинается плановая предупредительная профилактика, которая длится случайное время γ_1, и которая обновляет элемент. Если $\xi \leq \eta$, то в момент ξ начинается «аварийное» восстановление работоспособности, которое длится случайное время γ_2, и которое также полностью обновляет элемент или всю СЗ в целом.

В момент окончания любого восстановления, когда по определению элемент СЗ работоспособен, весь процесс повторяется независимо от прошлого.

Полумарковский процесс $\xi(t)$ принимает три состояния $\mathrm{E} = \{0,1,2\}$. Марковские моменты – это моменты начала и окончания восстановления работоспособности элемента СЗ. Положим $\xi(t) = 0$, если в момент t элемент работоспособен; $\xi(t) = 1$, если в момент t проводится плановая предупредительная профилактика; $\xi(t) = 2$, если в момент t проводится «аварийное» восстановление работоспособности элемента СЗ.

Полагаем $\mathrm{E}_0 = \{1,2\}, \mathrm{E}_1 = \{0\}$, то есть ВФ могут пройти через элемент, если в элементе СЗ проводится какое-либо восстановление, и не проходит, если элемент СЗ работоспособен.

Для получения решения данной оптимизационной задачи предлагается строить полумарковскую матрицу, элементы которой подставляются в систему алгебраических уравнений, которую можно решать относительно возможных состояний полумарковского процесса. Решение выражается дробно-линейным функционалом относительно распределения вероятностей возникновения указанных состояний элемента СЗ. В результате ряда расчетов получим значение интенсивности отказов в явном, числовом виде:

$$\frac{1-\int_0^{\infty} \mathrm{e}^{-\gamma * \mathrm{x}} \mathrm{dF}_1(\mathrm{x})}{\int_0^{\infty} \mathrm{e}^{-\gamma * \mathrm{x}} \mathrm{d}\left(\mathrm{F}_1(\mathrm{x})-\mathrm{F}_2(\mathrm{x})\right)} = \gamma(z) * \int_0^{\mathrm{t}} \overline{\mathrm{F}}(\mathrm{x})\mathrm{dx} - \mathrm{F}(\mathrm{t}), \qquad (1)$$

где $\gamma(x) = \frac{F'(x)}{\overline{F}(x)}$ – *интенсивность отказов*,

$\mathrm{F}(x), F'(x)$ – *распределения альтернирующего процесса восстановления*.

Корень t_0 уравнения (1), для которого достигается абсолютный максимум определяет детерминированное значение периода, через который следует назначать проведение плановых предупредительных профилактик элемента СЗ. В этом случае будет максимизировано значение математического ожидания времени до первого пропуска ВФ. Само значение математического ожидания также можно получить, но практического интереса в данном случае оно не имеет.

Предлагаемое решение позволяет в явном виде получить значение величины интенсивности отказов, которое дает возможность критериальной оценки СЗ поэлементно в составе сложных СИС. Кроме того, решение предлагаемой оптимизационной задачи в числовом виде определяет период, через который следует назначать проведение плановых предупредительных профилактик элемента СЗ.

Использование предложенного метода дает возможность поэлементно анализировать процесс функционирования сложных по своей структуре СЗ. Полученные результаты могут быть использованы при анализе и выработке решений на применение средств защиты от НСД, реализации комплекса мероприятий по оптимизации СЗ, а также на статистической основе определения оптимального времени между плановыми регламентными работами.

Предложенный вариант использования методики носит достаточно общий характер и может быть использован для анализа работоспособности и надежности любого элемента СИС, независимо от его функционального назначения.

Литература

1. Гихман И., Скороход А. Ведение в теорию случайных процессов – М. : «Наука», 1965.
2. Семкин А. и др. Основы организации обеспечения информационной безопасности объектов информатизации – М. : «Гелиос АРВ», 2005.
3. Климов С. Методы и модели противодействия компьютерным атакам – М., 2008 г.
4. Вентцель Е., Овчаров Л. Теория случайных процессов и ее инженерные приложения – М. : «Высшая школа», 2000.
5. Смирнов В. Курс высшей математики в 3 томах – М., 1958.
6. Малинецкий Г. Математические основы синергетики – М., 2009.

УДК 65.012.8

ОБЗОР МЕТОДИК ОЦЕНКИ ЭФФЕКТИВНОСТИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

Королева О.Ю., Несвит М.М.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Защищенность является одним из основных критериев эффективности функционирования информационной системы, наряду с производительностью, надежностью и отказоустойчивостью (под защищенностью системы будем понимать степень адекватности реализованных в ней механизмов защиты информации существующим в данной среде функционирования рискам). Вопросы оценки эффективности тесно связаны с вопросами проектирования системы защиты.

Целями оценки эффективности защищенности информации являются (помимо непосредственного получения сведений о текущем уровне защищенности информационной системы):

– анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов информационной системы;

– локализация узких мест в системе защиты информационной системы;

– оценка соответствия информационной системы существующим стандартам в области информационной безопасности;

– выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности информационной системы и другие.

– В данной работе рассмотрены четыре методики оценки эффективности защищенности информации и представлен метод выбора оптимальной системы защиты.

Примеры методик оценки эффективности защищенности информации

Оценка по моделям DREAD и STRIDE

Данная методика предполагает анализ эффективности системы безопасности с использованием классификации угроз по модели STRIDE и методике оценки риска DREAD. Этот подход был разработан компанией Microsoft и успешно применяется для определения опасностей, грозящих информационным системам. [2]

Для классификации угроз безопасности (первый этап) используется классификация, называемая STRIDE, по первым буквам английских названий категорий:

- Spoofing identity (Подмена сетевых объектов);
- Tampering with data (Модификация данных);
- Repudiation (Отказ от авторства);
- Information disclosure (Разглашение информации);
- Denial of service (Отказ в обслуживании);
- Elevation of privilege (Превышение привилегий).

На втором этапе следует определить методы защиты от угроз безопасности. Для выбора метода защиты желательно выполнить количественную оценку риска опасности для конкретной вычислительной системы. Для этой цели предлагается модель DREAD.

Способ оценки риска DREAD, названый по первым буквам английских названий описанных далее категорий:

- Damage potential (Потенциальный ущерб) – мера ущерба от успешной атаки;
- Reproducibility (Воспроизводимость) – мера возможности реализации угрозы;
- Exploitability (Подверженность взлому) – мера усилий и квалификации необходимых для атаки;
- Affected users (Круг пользователей, попадающих под удар) – доля пользователей, работа которых нарушается из-за успешной атаки;
- Discoverability (Открытость) – вероятность реализации данного способа нанесения ущерба;
- Суммарная DREAD-оценка равна арифметическому среднему всех оценок.

Также возможно включение в методику DREAD еще одного показателя – **з**атрат на устранение последствий успешной атаки, условно названный X (eXpense).

Далее на основании оценки проводится выбор конкретной технологии защиты.

Данная модель позволяет эффективно сформулировать требования к системе безопасности на этапе ее проектирования и рассчитать необходимый уровень защищенности на этапе эксплуатации. Она подходит для применения при отсутствии достоверной статистики по интенсивности угроз, однако с этим связан и весьма значительный ее недостаток – невозможность проанализировать только в рамках данной модели экономическую целесообразность внедрения того или иного механизма защиты.

Количественная оценка защищенности с точки зрения риска

Будем оценивать защищенность системы (Z) количественно в зависимости от стоимости защищаемой информации, вероятности взлома, стоимости самой системы защиты, производительности системы:

$$Z = f(C_{инф}, p_{взл}, Ц_{сзи}, П),$$

где $C_{инф}$ – стоимость защищаемой информации;

$p_{взл}$ – вероятность взлома;

$Ц_{сзи}$ – стоимость системы защиты информации;

П – производительность системы. [1]

С учетом введенного понятия защищенности системы оптимизационная задача состоит в обеспечении максимального уровня защищенности (как функции стоимости защищаемой информации и вероятности взлома) при минимальной стоимости системы защиты и минимальном влиянии ее на производительность системы:

$$Z_{opt} = \max(Z(C_{инф}, p_{взл}, Ц_{сзи}, П)).$$

С учетом сказанного может быть сделан вывод о многокритериальном характере задачи оценки эффективности системы защиты. Для сведения ее к однокритериальной введем дополнительные параметры:

- D – коэффициент защищенности;
- R – мультипликативный критерий риска ($R_{защ}$ – риск в защищенной системе, $R_{нез}$ – риск в незащищенной системе).

Рассмотрим защищенность системы с точки зрения риска:

$$R(p) = C_{инф} \cdot p_{взл}.$$

С другой стороны, можно рассматривать риск как потери в единицу времени:

$$R(\lambda) = C_{инф} \cdot \lambda_{взл},$$

где $\lambda_{взл}$ – интенсивность потока взломов. Эти две формулы связаны следующим соотношением:

$$p_{взл} = \lambda_{взл} / L,$$

где L – общая интенсивность потока несанкционированных попыток доступа злоумышленниками к информации.

В качестве основного критерия защищенности будем использовать коэффициент защищенности (D), показывающий относительное уменьшение риска в защищенной системе по сравнению с незащищенной.

$$D\% = (1 - R_{защ} / R_{нез}) \cdot 100\%.$$

Таким образом, в данном случае задача оптимизации выглядит следующим образом:

$$\begin{cases} D(C_{инф}, p_{взл}) \to \max \\ Ц_{сзи} \to \min \\ П_{сзи} \to \max \end{cases}$$

Для решения этой задачи сведем ее к однокритериальной посредством введения ограничений. В результате получим:

$$\begin{cases} D(C_{инф}, p_{взл}) \to \max \\ Ц_{сзи} \le Ц_{зад} \\ П_{сзи} \ge П_{зад} \end{cases}$$

где $Ц_{зад}$ и $П_{зад}$ – заданные ограничения на стоимость системы защиты и производительность системы.

Такой принцип сведения задачи к однокритериальной целесообразен, так как в любом техническом задании на разработку системы защиты указывается, в какой мере система защиты должна оказывать влияние на производительность системы. Кроме того, обычно вводится ограничение на стоимость системы защиты.

Теперь выразим коэффициент защищенности через параметры угроз. В общем случае в системе присутствует множество видов угроз. В этих условиях зададим следующие величины:

- w – количество видов угроз, воздействующих на систему;
- $C_i (i = 1,..., w)$ – потери от взлома i-того вида;
- $\lambda_i (i = 1,..., w)$ – интенсивность потока взломов i-того вида, соответственно;
- $Q_i (i = 1,..., w)$ – вероятность появления угроз i-того вида в общем потоке попыток несанкционированного доступа к информации, причем $Q_i = \lambda_i / L$;
- $p_i (i = 1,..., w)$ – вероятность отражения угроз i-того вида системой защиты.

Соответственно, для коэффициента потерь от взломов системы защиты имеем:

$$R(p) = \sum_1^w R_i(p) = \sum_1^w C_i \cdot p_{взлi},$$

где $R(p)$ – коэффициент потерь от взлома i-того типа.

Для незащищенной системы $p_{угрi} = Q_i$, для защищенной системы $p_{угрi} = Q_i \cdot (1 - p_i)$.

Соответственно, для коэффициента потерь от взломов системы защиты в единицу времени имеем:

$$R(\lambda) = \sum_1^w R_i(\lambda) = \sum_1^w C_i \cdot \lambda_{угрi},$$

где $R(\lambda)$ – коэффициент потерь от взломов i-того типа в единицу времени.

Для незащищенной системы $\lambda_{угрi} = \lambda_i$, для защищенной системы $\lambda_{угрi} = \lambda_i \cdot (1 - p_i)$.

Соответственно

$$D = 1 - \frac{\sum_1^w C_i \cdot Q_i \cdot (1 - p_i)}{\sum_1^w C_i \cdot Q_i} = 1 - \frac{\sum_1^w C_i \cdot \lambda_i \cdot (1 - p_i)}{\sum_1^w C_i \cdot \lambda_i}.$$

Данный метод позволяет с высокой точностью рассчитать коэффициент защищенности системы, однако для его применения необходима полная и достоверная информация о

статистике угроз и потерях от реализации угроз, получение которой бывает затруднительно, так как желательно сходство не только в структуре защищаемой и являющийся объектом статистических исследований системам, но и в специфике деятельности предприятий.

Количественная оценка защищенности с использованием графовой модели

В основе данной модели лежит описание системы защиты информации, построенное на взаимодействии «области угроз», «области защищаемых объектов» и «области механизмов безопасности». Отношения между их элементами и описывает систему защиты.

Для того, чтобы математически точно определить уровень защищенности информации, рассмотрим формальную модель системы защиты информационной системы. Ее основой будем считать модель системы защиты с полным перекрытием, в которой рассматривается взаимодействие «области угроз», «защищаемой области» (ресурсов системы) и «системы защиты» (механизмов безопасности системы). [3]

Таким образом, имеем три множества:

- $T = \{t_i\}$ – множество угроз безопасности,
- $O = \{o_j\}$ – множество объектов (ресурсов) защищенной системы,
- $M = \{m_k\}$ – множество механизмов безопасности.

Элементы этих множеств находятся между собой в определенных отношениях, собственно и описывающих систему защиты.

Развитие этой модели предполагает введение еще двух элементов:

- $V = \{v_r\}$ – набор уязвимых мест, определяемый подмножеством декартова произведения $T \cdot O$: $v_r = \langle t_i, o_j \rangle$. Таким образом, под уязвимостью системы защиты будем понимать возможность осуществления угрозы t в отношении объекта o;
- $B = \{b_l\}$ – набор барьеров, определяемый декартовым произведением $V \cdot M$: $b_l = \langle t_i, o_j, m_k \rangle$, представляющих собой пути осуществления угроз безопасности, перекрытые средствами защиты.

Для описания системы защиты используем графовую модель, представленную на рис. 1. В результате получаем систему, состоящую из пяти элементов: $\langle T, O, M, V, B \rangle$, описывающую систему защиты с учетом наличия в ней уязвимостей.

Защищенность информационной системы от угроз безопасности определяется количеством уязвимостей, для которых в системе не создано барьеров, перекрывающих эти уязвимости, а также прочностью существующих барьеров.

В идеале каждый механизм защиты должен исключать соответствующий путь реализации угрозы $\langle t_i, o_j \rangle$. В действительности же механизмы защиты обеспечивают лишь некоторую степень сопротивляемости угрозам безопасности. В связи с этим в качестве характеристик элемента набора барьеров $b_l = \langle t_i, o_j, m_k \rangle$, может рассматриваться набор $\langle P_l, L_l, R_l \rangle$, где

- P_l - вероятность появления угрозы;

– L_l - величина ущерба при удачном осуществлении угрозы (уровень серьезности угрозы);
– R_l - степень сопротивляемости механизма защиты m_k.

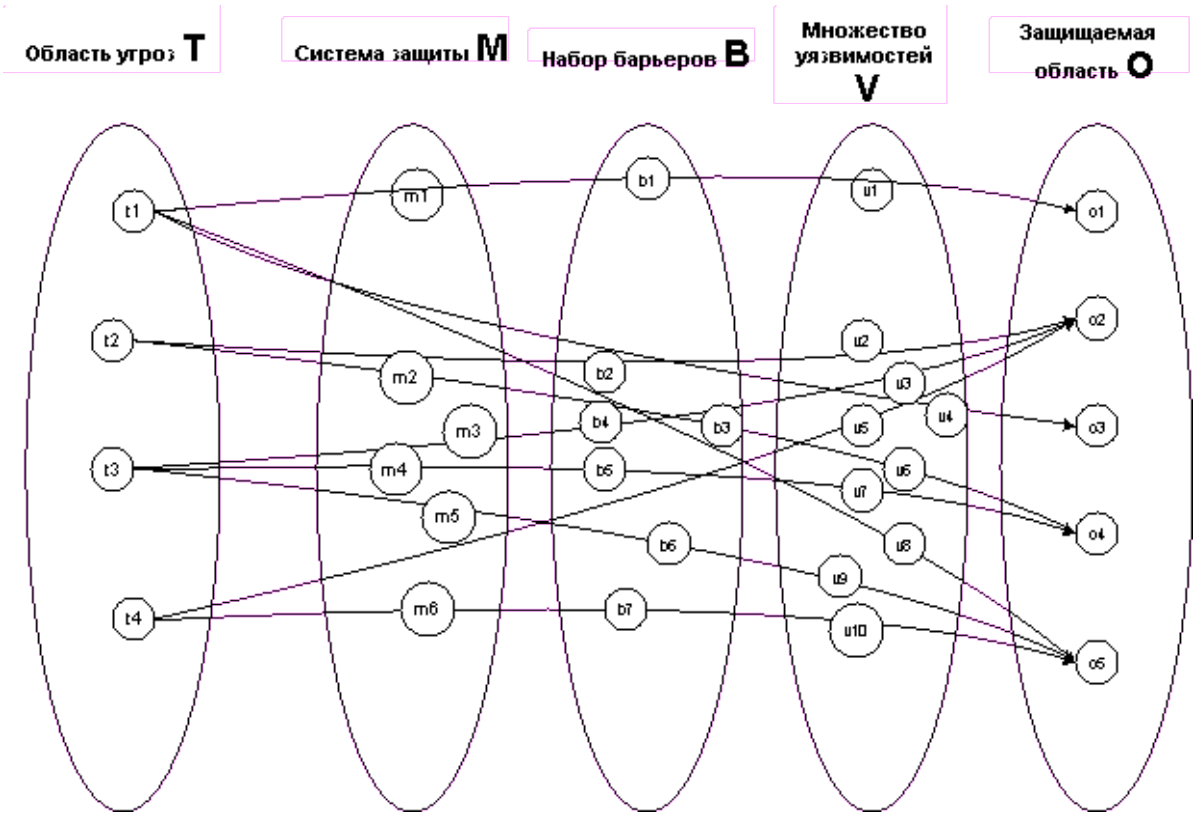


Рисунок 1. Описание системы защиты информации с использованием графовой модели

Прочность барьера $b_l = \langle t_i, o_j, m_k \rangle$ характеризуется величиной остаточного риска $Risk_l$, связанного с возможностью осуществления угрозы безопасности t_i в отношении объекта информационной системы o_j, при использовании механизма защиты m_k. Эта величина определяется по формуле:

$$Risk_l = P_k \cdot L_k \cdot (1 - R_k).$$

Для определения величины защищенности S можно использовать следующую формулу:

$$S = 1 \Big/ \sum_{(\forall b_k \in B)} (P_k \cdot L_k \cdot (1 - R_k),$$

где $P_k, L_k \in (0,1)$, $R_k \in [0,1)$.

В этой формуле, знаменатель определяет суммарную величину остаточных рисков, связанных с возможностью осуществления угроз безопасности T в отношении объектов системы O, при использовании механизмов защиты M. Суммарная величина остаточных рисков характеризует «общую уязвимость» системы защиты, а защищенность системы определяется как величина, обратная ее «уязвимости». При отсутствии в системе барьеров b_k, перекрывающих определенные уязвимости, степень сопротивляемости механизма защиты R_k принимается равной нулю.

Для защиты информации экономического характера, допускающей оценку ущерба в результате осуществления угроз безопасности, разработаны стоимостные методы оценки

эффективности средств защиты. Набор характеристик барьера дополняется величиной C_l - затраты на построение средства защиты барьера b_l. Выбор оптимального набора средств защиты связан с минимизацией затрат $W = \{w_l\}$, состоящих из затрат $C = \{c_l\}$ на создание средств защиты и возможных затрат в результате успешного осуществления угроз $N = \{n_l\}$.

Так же, как и в предыдущем случае, модель позволяет с высокой точностью рассчитать коэффициент защищенности информационной системы, однако получение исходных параметров для нее может быть затруднительным.

Экспертная оценка

Рассматриваемая методика предполагает экспертную оценку, включающую оценку угроз и оценку уязвимостей. Рассмотрим пример реализации подобного подхода, используемого в методе CRAMM (CCTA Risk Analysis and Managment Method) был разработан Агентством по компьютерам и телекоммуникациям Великобритании по заданию Британского правительства и взят на вооружение в качестве государственного стандарта):

Для оценки угроз выбраны следующие косвенные факторы:

- статистика по зарегистрированным инцидентам;
- тенденции в статистке по подобным нарушениям;
- наличие в системе информации, представляющей интерес для потенциальных внутренних или внешних нарушителей;
- возможность извлечь выгоду из изменения обрабатываемой в системе информации;
- наличие альтернативных способов доступа к информации;
- статистика по подобным нарушениям в других информационных системах организации.

Для оценки уязвимостей выбраны следующие косвенные факторы:

- количество рабочих мест (пользователей) в системе;
- осведомленность руководства о действиях сотрудников;
- характер используемого на рабочих местах оборудования и ПО;
- полномочия пользователей.

По косвенным факторам предложены вопросы и несколько фиксированных вариантов ответов, которые «стоят» определенное количество баллов. Итоговая оценка угрозы и уязвимости данного класса определяется суммированием баллов.

Проводится поочередный опрос экспертов, при этом необходимо определить условные значений квалификации каждого из них. Исходя из заданной квалификации экспертов рассчитывается вес в группе, затем итоговые оценки угрозы и уязвимости получаются суммированием с учетом весов экспертов. Расчет коэффициента защищенности проводится по приведенным выше формулам. После получения общей оценки всей группы рассматривается согласованность ответов, которая может использоваться для оценки достоверности результатов. [3]

Достоинство данного подхода – возможность учета множества косвенных факторов (и не только технических). Методика проста и дает владельцу информационных ресурсов ясное представление, каким образом получается итоговая оценка и что надо изменить, чтобы улучшить показатели. Однако косвенные факторы и их веса зависят от сферы деятельности организации, а

также от ряда иных обстоятельств. Таким образом, методика всегда требует подстройки под конкретный объект. При этом доказательство полноты выбранных косвенных факторов и правильности их весовых коэффициентов (задача малоформализованная и сложная) на практике решается экспертными методами (проверка соответствия полученных по методике результатов, ожидаемых для тестовых ситуаций). Подобные методики, как правило, разрабатываются для организаций определенного профиля (ведомств), апробируются и затем используются в качестве ведомственного стандарта.

Выбор оптимальной системы защиты информации

Безопасность должна быть в первую очередь экономически оправданной. Уже на этапе проектирования приходится выбирать допустимый уровень риска для снижения стоимости системы защиты и повышения производительности системы в целом. При этом на протяжении всего жизненного цикла системы необходима модификация системы защиты, основанная на анализе текущего состояния. Эта модификация предполагает выявление новых угроз и анализ их отражения механизмами защиты, присутствующими в системе на данный момент. При необходимости их следует модифицировать или заменить на новые. Кроме того их замена может быть целесообразной в связи с разработкой новых более эффективных технических решений. [1]

В данной работе в качестве метода выбора оптимальной системы защиты информации будет рассмотрен метод последовательного выбора уступок.

Зависимость изменения основных параметров, характеризующих систему защиты информации, от ее сложности (используемого набора механизмов защиты), представлена на рис. 2.

Стоимость системы защиты возрастает неограниченно, а производительность снижается в пределе до нуля. При этом коэффициент защищенности стремиться к предельному значению – единице и в некоторый момент достигает насыщения. При дальнейшем нарастании сложности (и, соответственно, увеличении цены и снижении производительности) защищенность возрастает незначительно.

Следовательно, при проектировании системы защиты, параметры защищенности которой расположены в области насыщения, целесообразно проанализировать параметры альтернативных вариантов. То есть целесообразно исследовать возможность использования менее сложных систем защиты и, задав некоторый промежуток снижения коэффициента защищенности (dD), выбрать систему, уровень защищенности которой удовлетворяет полученному (D – dD) (конечно, если таковые имеются). При этом может быть получен ощутимый выигрыш в цене и производительности.

Данный метод помогает добиться разумного компромисса и обеспечить максимальную защищенность при необходимом уровне цены и производительности системы.

В настоящее время, видимо, не существует каких-либо стандартизированных методик анализа защищенности информационных систем. Весьма точные результаты дает количественная оценка, однако для ее применения необходимо определить значения исходных параметров, получение которых бывает крайне затруднительно, а в некоторых случаях практически невозможно (например, при оценке ущерба от несанкционированного доступа к информации политического или военного характера). Экспертная оценка позволяет учесть множество

косвенных факторов, но она требует подстройки под объект и, желательно, опыта экспертов в работе с объектами со схожей спецификой деятельности.

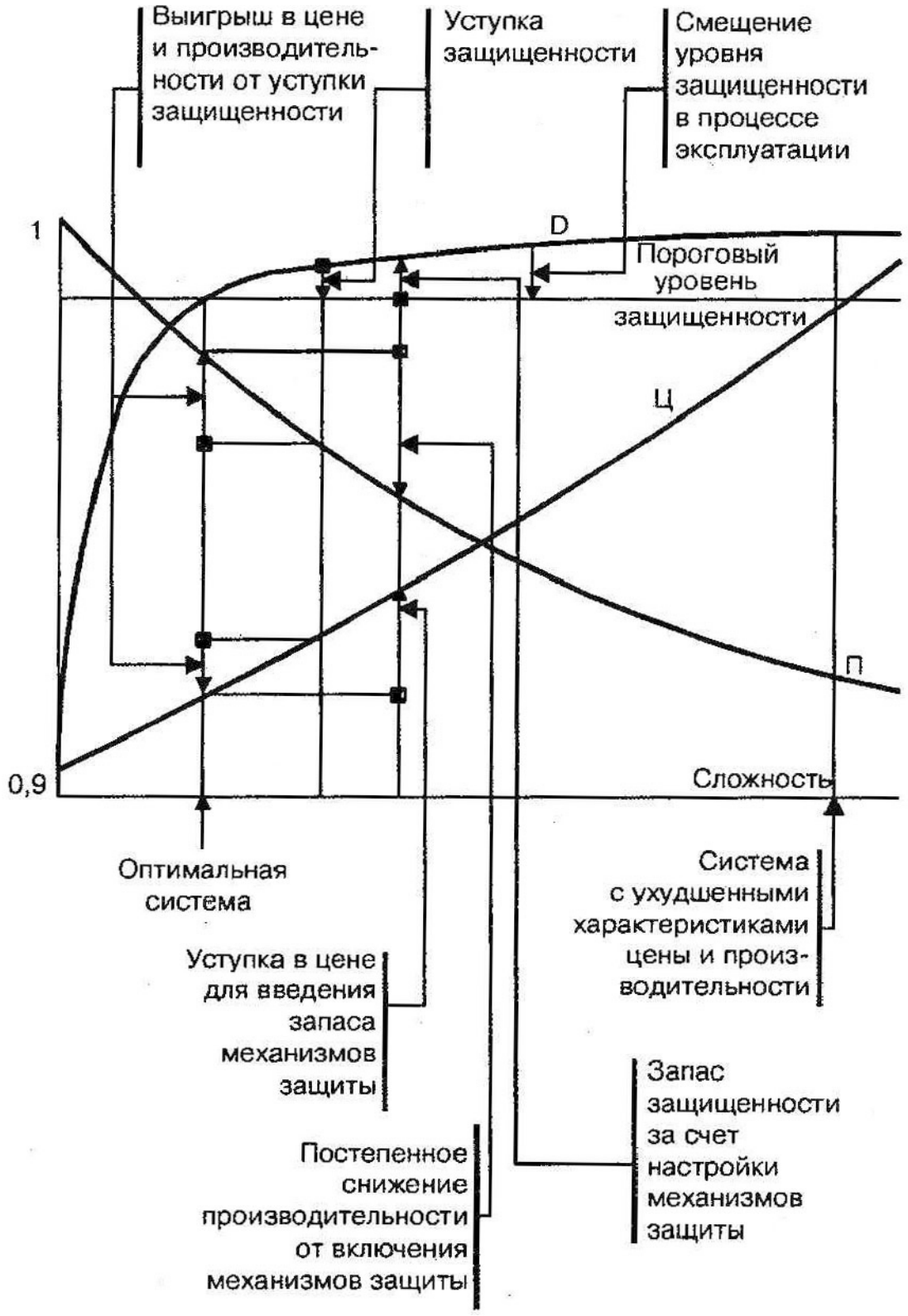


Рисунок 2. Зависимость изменения основных параметров, характеризующих систему защиты информации, от ее сложности

Проектирование системы защиты на основе оценки защищенности системы осуществляется с учетом данных об уже существующих угрозах и средствах защиты информации, однако в

процессе функционирования системы положение дел в этой области может значительно измениться. Поэтому проектирование системы защиты – процедура, предполагающая не только создание исходного варианта, но и постоянный анализ защищенности в процессе эксплуатации с доработкой «узких мест» – настройкой, заменой или дополнением отдельных механизмов защиты и добавлением новых по мере необходимости. Кроме того на всех этапах неизбежна модификация системы защиты информации, связанная с ее экономической оправданностью, – она не должна значительно снижать производительность информационной системы в целом и превышать ограничения по стоимости, что неизбежно вызывает снижение уровня защищенности.

Литература

1. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа – СПб : «Наука и техника», 2004.

2. Ховард М., Лебланк Д. Защищенный код – «Русская редакция», 2005.

3. Сайт «Защита информации, управление информационной безопасностью и рисками», iso27000.ru

УДК 696.6

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СТРУКТУРИРОВАННЫХ КАБЕЛЬНЫХ СИСТЕМАХ

Кремляков П.А.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Сегодня ни одна современная организация не обходится без использования локальных вычислительных сетей, телефонных сетей, систем видеонаблюдения и других слаботочных устройств и систем. Важную роль играют телефонные и локальные вычислительные сети, так как они задействованы не только в управлении и координировании действий персонала, но и в самих производственных процессах.

Для создания вышеупомянутых слаботочных систем необходимо провести монтаж структурированной кабельной системы.

Структурированная кабельная система в отличие от хаотично и спонтанно проложенных кабелей имеет возможность расширения, универсальность, удобством пользования и администрирования и прочие преимущества. К этим преимуществам относится обеспечение доступности, целостности и конфиденциальности информации, насколько это может обеспечить кабельная система.

Основной стандарт для структурированных кабельных систем – ISO/IEC 18801.

Существует множество фирм профессионально занимающихся монтажом структурированных кабельных систем, но, практика показывает, что не все работы проводятся в соответствии с этим стандартом. Это может происходить по разным причинам, от халатности монтажников, до нежелания руководства грамотно организовать работу. Это может привести к

нарушению работы локальной вычислительной сети, телефонии и прочего, что в большинстве случаев приведет к убыткам.

Безусловно, построенная в соответствии со всеми стандартами структурированная кабельная система не дает абсолютной информационной безопасности – для этого нужен комплекс мер; но грамотно построенная структурированная кабельная система создает основу для остальных мер и методов обеспечения информационной безопасности.

УДК 004.7

ОЦЕНКА УЯЗВИМОСТЕЙ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ УДАЛЕННОГО НАБЛЮДЕНИЯ

Люберт А.С.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Научный руководитель – доц. Хромов И.Н.

Система удаленного видеонаблюдения (УВН) – программно-аппаратный комплекс, предназначенный для организации видеоконтроля на территориально удаленных объектах посредством взаимодействия с удаленным устройством управления.

В настоящее время системы удаленного видеонаблюдения становятся более распространенными среди частных лиц и небольших компаний вследствие относительно небольших цен на оборудование и доступ в сеть и желания обеспечить приемлемый уровень информационной безопасности.

Система удаленного видеонаблюдения может применяться в различных областях деятельности при отсутствии непосредственной возможности нахождения на объекте наблюдения. Область применения системы практически не ограничена и может быть использована как для периодического наблюдения за жилыии помещениями, так и для построения системы безопасности коммерческих объектов.

Основная цель системы – информирование пользователя в кратчайшие сроки о проникновении на территорию объекта, а также ведение записи видеоматериалов для последующего анализа.

Компоненты системы УВН

- устройства формирования видеоизображения (видеокамеры, IP-камеры, web-камеры и т.п.);
- устройство управления системой УВН (сервер управления, web-сервер и т.п.);
- дополнительные датчики и исполнительные устройства (датчик движения, температуры, задымления и т.п.; сирена, световая сигнализация и т.п.).

Задачи систем УВН в рамках мониторинга ИБ

Передача видеопотока с устройств формирования видеоизображения

Предоставление пользователю возможности получения видеопотока или отдельных видеокадров с видеокамер в реальном времени.

Реагирование на внештатные ситуации

Реагирование на сигналы детектора движения видеокамер и прочих датчиков, уведомление пользователя о внештатной ситуации, активация исполнительных устройств.

Ведение журнала событий

Запись в журнал данных о произошедших внештатных ситуациях, ведение архива видеоматериалов для последующего анализа.

Одна из основных функций системы – сохранение видеопотока для последующего анализа происходящих событий, а также возможного получения доказательств каких-либо фактов противозаконной деятельности. В совокупности с предыдущими задачами, позволяет в кратчайшие сроки удаленно получить документальное подтверждение произошедших на объекте наблюдения событий.

Варианты реализации УВН

Реализации подключения устройств:

– одна IP-камера, совмещающая в себе устройство формирования видеоизображения и устройство управления;
– одна или несколько IP-камер и выделенное устройство управления, объединенные в локальную сеть.

Реализации подключения устройств системы к сети:

– с использованием прямого подключения к сети;
– с использованием GSM-модема.

Программное обеспечение

Специализированное ПО системы подразделяется на две независимые части:

1) ядро системы – запись видеопотоков в архив, получение сигналов от датчиков, ведение журнала событий, уведомление пользователя (язык программирования – Python);
2) web-интерфейс – доступ к видеоинформации, контроль, управление ядром системы с клиентского ПО (язык программирования – PHP).

В качестве клинетского ПО выступает браузер пользователя, которое в случае необходимости возможно заменить на специализированное клиентское ПО.

Методы исследования

В качестве методов исследования будут произведены действия, направленные на тестирование аппаратной и программной частей системы:

1) удаленное получение видеопотока с объекта с анализом качества полученных материалов;
2) проникновение в контролируемую зону с целью получения уведомления о событии доступа;

3) анализ видеоархива на предмет наличия всех запланированных событий и видеоматериалов;

4) общее тестирование всех компонентов системы.

Так как система по большей части функционирует удаленно без постоянного присмотра и обслуживания, необходимо тщательно рассмотреть вопросы безопасности.

Основной недостаток системы – это хранение всех видеоматериалов на самом объекте наблюдения, так как при угрозах на сам объект (пожар, кража) могут быть потеряны все накопленные материалы. Может быть решен периодической отправкой видеоархива на определенный узел сети Internet, но при использовании дорогостоящего соединения с сетью может быть экономически не выгодным.

Уязвимости существующих УВН

Конфиденциальность

1) Несанкционированный удаленный доступ к системе – удаленное подключение и запрос видеопотока нелегитимным пользователем.

Метод устранения: защита на подключение к системе паролем или сертификатом.

2) Несанкционированный доступ к системе в обход устройства управления – физическое подключение к локальной сети системы.

Метод устранения: физическое ограничение на доступ к устройствам сети, запрет на добавление устройств в сеть.

Целостность

1) Нарушение физической целостности устройств получения видеоинормации – выход из строя, уничтожение камер наблюдения злоумышленником.

Метод устранения: усиленный корпус уличных камер, скрытая установка, уведомление пользователя о выходе камеры из строя.

2) Нарушение физической целостности устройства управления – выход из строя сетевого оборудования, ЭВМ, в том числе отключение электропитания.

Метод устранения: использование качественных комплектующих аппаратного обеспечения, использование источников бесперебойного питания.

3) Нарушение физической целостности исполнительных устройств – выход из строя, уничтожение исполнительных устройств злоумышленником.

Метод устранения: использование качественных комплектующих исполнительных устройств, уведомление пользователя о выходе исполнительных устройств из строя.

4) Удаление или модификация видеоархива – частичное или полное уничножение данных архива видеоматериалов.

Метод устранения: создание и хранение резервных копий архива, защита на доступ к системе паролем или сертификатом, видеонаблюдение в области расположения аппаратных компонентов системы.

Доступность

1) Недоступность канала передачи данных – отсутствие соединения с сетью.

Метод устранения: наличие резервного канала связи, анализ качества приема сигнала в момент установки системы.

Литература

1. http://www.tss-security.ru/Zaschita-Informatsii.html
2. http://www.rossisec.ru/
3. http://www.alt-1c.ru/pages.html?id=5

УДК 004

ИСПОЛЬЗОВАНИЕ ОБЩЕДОСТУПНЫХ ИНТЕРНЕТ-РЕСУРСОВ О ДЕЯТЕЛЬНОСТИ КОМПАНИЙ ДЛЯ СОСТАВЛЕНИЯ И СРАВНЕНИЯ ПРОГНОЗОВ

Мандрик П.И.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

За последние 5 лет количество цифровой информации увеличилось десятикратно. Таким образом для составления прогнозов с каждым годом приходится анализировать больший ее объем. При составлении и проверке экономических и политических прогнозов большую помощь могут оказать следующие общедоступные ресурсы.

Annual report – полный ежегодный отчет компании своим акционерам о проделанной деятельности и планах на будущее. Он в обязательно порядке содержит в себе описание основных факторов риска, перечень совершенных обществом в отчетном году сделок, положение общества в отрасли.

Google Finance – провайдер финансовой информации принадлежащий компании Google Inc. Сервис предоставляет доступ к финансовой информации о большинстве транснациональных компаний. Доступна информация по котировкам и рейтинги ценных бумаг, пресс-релизы и финансовые отчеты компаний, исторические данные доступны в виде графиков.

Yahoo! Finance – провайдер финансовой информации принадлежащий Yahoo! Один из главных поставщиков подобной информации в США. Предоставляет новости и справочную информацию по темам, связанным с бизнесом, финансами и экономикой. Справочная информация включает в себя котировки и рейтинги ценных бумаг, пресс-релизы и финансовые отчеты компаний. В России не представлен.

Настоящий доклад посвящен варианту получения и использования статистических данных для прогнозирования, сравнения и проверки уже готовых прогнозов на примере фирмы BP для определения ее конкурентных преимуществ.

УДК 004.056

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОСУЩЕСТВЛЕНИИ МЕЖДУНАРОДНОГО НАУЧНО-ТЕХНИЧЕСКОГО СОТРУДНИЧЕСТВА

Митин И.И., Яковлев А.М.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Развития производства высокотехнологичных инновационных товаров, услуг и технологий, обеспечение опережающего развития конкурентоспособных отраслей и производств рынка наукоемкой продукции является одной из приоритетных задач государства в области обеспечения национальной безопасности.

В условиях коммерциализации рынка образовательных услуг и высоких технологий, обучение иностранных граждан и проведение прикладных исследований в их интересах должно рассматриваться не только как источник дополнительных финансовых поступлений, но и как важный фактор государственной научно-технической политики и осуществляться с учетом оценки рисков, связанных с получением ими знаний в ущерб национальной безопасности РФ. К таким рискам относится:

– предоставление сотрудниками ВУЗа иностранным гражданам образовательных услуг в различных формах, как на территории РФ, так и за границей;
– выполнение сотрудниками ВУЗа научно-исследовательских, опытно-конструкторских, технологических и иных работ в интересах иностранных заказчиков;
– научная и учебная деятельность сотрудников и учащихся ВУЗа за границей РФ (в иностранных научных, учебных заведениях, промышленных компаниях и т.п.);
– прием иностранных граждан в ВУЗе;
– внешнеторговые сделки по продаже (купле) товаров;
– экспонирование товаров и технологий на международных выставках, как на территории РФ, так и за границей.

Оценка показателя эффективности информационной безопасности (далее – ИБ) Российской Федерации при передаче «чувствительных» технологий иностранным гражданам в «осязаемой» и «неосязаемой» формах выстраивается на значениях «потенциалов» – числовых эквивалентов источников угроз, получаемых путем статистического анализа показателей.

Для каждого «потенциала» определяется вес путем количественной оценки угроз безопасности. Расчет «потенциалов» осуществляется путем экспертной оценки.

Необходимым условиям, подтверждения факта максимальной эффективной ИБ является стремление показателя эффективной ИБ к максимальному значению.

Применение предлагаемой методики позволяет учесть все важные факторы при построении системы ИБ субъектов инновационной деятельности.

УДК 004.056

ВОПРОСЫ ОБЕСПЕЧЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТИ В СВЕТЕ РЕАЛИЗАЦИИ ФЦП «ЭЛЕКТРОННАЯ РОССИЯ»

Нибилица А.Ю.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Научный руководитель – доц. Хромов И.Н.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В данной статье приведен анализ угроз системе безопасности электронного правительства, представлена альтернативная классификация угроз и превентивные меры для противодействия несанкционированному доступу к данным.

Ключевые слова: угрозы, безопасность, электронное правительство.

Современное общество и в особенности крупные города уже не мыслят себя без Internet’а. Миллионы людей каждый день пользуются услугами Internet–магазинов и электронной почты, общаются в социальных сетях и передают информацию через файлообменники – Internet позволил значительно облегчить процесс коммуникации между людьми, и теперь используется для взаимосвязи рядовых граждан и правительства.

Ведущие европейские страны и США уже в 2000–2001 годах разработали и внедрили свои системы электронного правительства для оказания качественных государственных услуг гражданам, а в нашей стране практическая реализация ФЦП «Электронная Россия» осуществляется только сейчас. И теперь перед нами особенно остро стоит вопрос об адекватности нашей системы электронного правительства нуждам граждан и организаций, в сочетании с выполнением условий конфиденциальности, целостности и доступности персональных данных в процессе реализации предоставляемых государством услуг.

1. Основные положения о системе электронного правительства

Электронное правительство представляет информационно–коммуникационную систему для оказания стандартного набора государственных услуг гражданам, организациям и представителям разных ветвей государственной власти с целью повышения эффективности работы государственного аппарата на этапах составления, передачи и обработки запросов в государственные учреждения.

Основными направлениями потоков информации в системе электронного правительства [1] являются взаимодействие между государством и гражданами (Government-to-Citizen), между государством и бизнесом (Government-to-Business), между различными ветвями государственной власти (Government-to-Government) и между государством и государственными служащими

(Government-to-Employees). Это означает, что система электронного правительства в качестве сервера должна надежно аутентифицировать пользователя-клиента и предоставить ему доступ к определенным данным и услугам в соответствие с предоставленными клиенту полномочиями.

Вопрос обеспечения безопасности информации к тому же осложняется тем, что в соответствие с Положением о системе межведомственного электронного документооборота для организации технико-технологической инфраструктуры используются каналы связи, арендуемые у операторов связи, а настройку технических средств и средств защиты осуществляют «организаторы межведомственного электронного документооборота», т.е. конкретные представители на местах.

В связи с этим возникает ряд угроз безопасности информации – как уже классифицированных и типизированных специалистами в области защиты информации, так и специфичных для данной ситуации.

2. Перечень угроз безопасности системы электронного правительства

Все существующие угрозы можно классифицировать по объекту атаки злоумышленника, целью которого может быть как получение несанкционированного доступа к конфиденциальной информации, так и временное или полное выведение системы из строя.

Классы угроз:

- аппаратные;
- программные;
- пользовательские,

где каждый класс затем делится на *внутренние* и *внешние* угрозы.

Вначале рассмотрим класс аппаратных угроз.

Аппаратные угрозы представляют собой отказы вычислительного оборудования (ПК, принтеров, роутеров, модемов и пр.) и их частей (жестких дисков, сетевых плат ПК и т.д.), намеренно провоцируемые злоумышленником для временного выведения системы из строя или уничтожения конфиденциальной информации. Аппаратные угрозы не так популярны у злоумышленников как программные, но они не менее эффективны и порой позволяют пробить брешь в хорошо настроенной системе безопасности.

Внешние аппаратные угрозы можно разделить на:

- *вандализм* – намеренная порча злоумышленником оборудования, расположенного вне режимной зоны организации, но связанного с оборудованием посредством каналов передачи (так, например, при выведении из строя электрических трансформаторов, резкий скачок напряжения в сети питания может уничтожить носители информации и, соответственно, саму информацию на подключенных к этой сети устройствах, что особенно опасно для банков данных и электронных архивов);
- *провокация* – намеренное осуществление злоумышленником определенных действий, ведущих к реализации жертвой предсказуемой реакции и использованию ее в целях доступа к защищаемой информации (так злоумышленник может получить доступ к маршрутизатору провайдера и отослать ложный сигнал о неисправности подключения к сети Internet, обслуживающий персонал либо заменит неисправный модуль, либо временно приостановит

работу, отправив «неисправное» оборудование на ремонт, где злоумышленник может поставить в устройство «закладку» и получить несанкционированный доступ к системе).

Внутренние аппаратные угрозы представляют собой *саботаж* – намеренная или непреднамеренная порча оборудования сотрудником организации, вследствие чего система может выйти из строя (например, сотрудницы могут непреднамеренно залить роутеры водой, поливая цветы).

Программные угрозы представляют собой математическое обеспечение для любого вида техники, позволяющее в силу внутренних ошибок либо преднамеренно встроенных функций осуществлять несанкционированный доступ к информации.

Внешние программные угрозы [2] представляют:

– *сниффер пакетов* – прикладная программа, которая перехватывает все сетевые пакеты, передающиеся через определенный домен. В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа трафика. Однако ввиду того, что некоторые сетевые приложения передают данные в текстовом формате (telnet, FTP, SMTP, POP3 и т.д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли). Это может представлять серьезную угрозу безопасности, учитывая то, что разные государственные структуры будут осуществлять обмен конфиденциальной информацией через Internet;

– *IP-спуфинг* – подмена собственного IP–адреса злоумышленником с целью получения доступа в корпоративную сеть. Особенно опасно, если аутентификация пользователей в сети основывается только на проверке IP–адреса. Атаки IP–спуфинга часто являются отправной точкой для прочих атак (например, DoS– атака начинается с чужого адреса, скрывающего истинную личность злоумышленника);

– *отказ в обслуживании (Denial of Service – DoS)* – зависание системы, вызванное переполнением канала связи запросами клиентов так, что сервер не имеет физической возможности обрабатывать новые запросы. Атака злоумышленника в этом случае делает сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения. В случае использования некоторых серверных приложений (таких как Web-сервер или FTP-сервер) атаки DoS могут заключаться в том, чтобы занять все соединения, доступные для этих приложений и держать их в занятом состоянии, не допуская обслуживания обычных пользователей;

– *парольные атаки* – использование злоумышленником логина и пароля зарегистрированного пользователя с целью проникновения в систему и получение доступа к конфиденциальной информации. Злоумышленник может проводить парольные атаки с помощью простого перебора (brute force attack), программы – троянского коня, IP-спуфинга и сниффинга пакетов. Хотя логин и пароль часто можно получить при помощи IP-спуфинга и снифинга пакетов, злоумышленники часто пытаются подобрать пароль и логин, используя для этого многочисленные попытки доступа – простой перебор (brute force attack). Часто для такой атаки используется специальная программа, которая пытается получить доступ к ресурсу общего пользования (например, к серверу);

– *атаки типа man-in-the-middle* – искажение или перехват исходящего трафика злоумышленником, при использовании промежуточных узлов при передаче информации по сети. Для атак этого типа часто используются снифферы пакетов, транспортные протоколы и протоколы

маршрутизации. Атаки проводятся с целью кражи информации, перехвата текущей сессии и получения доступа к частным сетевым ресурсам, для анализа трафика и получения информации о сети и ее пользователях, для проведения атак типа DoS, искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии (доступ ко всем пакетам, передаваемым от провайдера в любую другую сеть, может, к примеру, получить сотрудник этого провайдера);

– *атаки на уровне приложений* – характерны тем, что злоумышленник использует ошибки в работе приложений, позволяющие получить несанкционированный доступ к конфиденциальной информации. Сведения об атаках на уровне приложений широко публикуются, чтобы дать возможность администраторам исправить проблему с помощью коррекционных модулей (патчей);

– *сетевая разведка* – сбор информации о сети с помощью общедоступных данных и приложений, используемый для подготовки атаки против какой–либо сети. Сетевая разведка проводится в форме запросов DNS, эхо-тестирования (ping sweep) и сканирования портов. Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены. Эхо–тестирование (ping sweep) адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, злоумышленник использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами, и анализирует характеристики приложений, работающих на хостах. В результате добывается информация, которую можно использовать для взлома.

Внутренние программные угрозы [2] представляют:

– *злоупотребление доверием* – злонамеренное использование отношений доверия, существующих в сети (взлом одного из серверов в периферийной части корпоративной сети приводит к взлому и всех остальных серверов, поскольку все они принадлежат к одному и тому же сегменту и доверяют другим системам своей сети);

– *переадресация портов* – разновидность злоупотребления доверием, когда взломанный хост используется для передачи через межсетевой экран трафика, который в противном случае был бы обязательно отбракован (например, если используется межсетевой экран с тремя интерфейсами, к каждому из которых подключен определенный хост и этот хост будет взломан, то, несмотря на то, что внешний хост может подключаться к хосту общего доступа (DMZ), но не к хосту, установленному с внутренней стороны межсетевого экрана, а хост общего доступа может подключаться и к внутреннему, и к внешнему хосту, злоумышленник получает доступ и к внутреннему и к внешнему хостам);

– *несанкционированный доступ* – намеренное преодоление правил политики безопасности сотрудниками организации для получения доступа к конфиденциальной информации (например, если сотрудник-злоумышленник используя права авторизованного пользователя обходит систему безопасности);

– *вирусы и приложения типа* «*троянский конь*» – вредоносные программы, которые внедряются в другие программы либо маскируются под полезные приложения и выполняют определенные нежелательные функции на рабочей станции конечного пользователя (например, собирают логины и пароли и пересылают их злоумышленнику).

Пользовательские угрозы основываются на методе социальной инженерии [3], представляющие собой совокупность действий злоумышленника, направленных на эксплуатацию человеческих качеств сотрудников, как доверие, сочувствие, лень, некомпетентность и

невнимательность, приводящие к несоблюдению правил внутренней безопасности и утечке конфиденциальной информации.

Внешние пользовательские угрозы представляют:

– *звонки* «*сотрудников*» *обслуживающих организаций* – телефонные звонки злоумышленников, представляющихся сотрудниками служб обеспечения безопасности/техподдержки и пр. и предлагающие пользователям установить программы из Internet'а. Обычно злоумышленник заранее выкладывает зараженный файл с программой и объясняет пользователю откуда его нужно скачать;

– *звонки* «*сотрудников*» *организации* – звонки злоумышленника, представляющегося сотрудником организации с целью получить авторизованный доступ к сети организации (так представившись сотрудником организации злоумышленник может с помощью личного обаяния расположить к себе человека, отвечающего за организацию удаленного доступа к рабочим станциям, и получить авторизованный доступ к конфиденциальной информации);

– *фишинг* – электронные письма с поддельные уведомления от банков, провайдеров, платежных систем и других организаций с просьбой перейти по указанной ссылке, страница по которой полностью имитирует официальную страницу организации, и авторизоваться – ввести логин и пароль – или ввести номер банковской карты/страховки и т.д., после чего фальшивая страница пересылает конфиденциальные данные злоумышленнику;

– «*подставная утка*» – проникновение злоумышленника на территорию организации под видом сотрудника и реализация им противоправных действий с целью хищения конфиденциальной информации.

Внутренние пользовательские угрозы представляют:

– *подкуп/шантаж сотрудников* – действия определенного характера, в результате которых собственные сотрудники организации передают конфиденциальную информацию злоумышленнику;

– *некомпетентность сотрудников* – непреднамеренное раскрытие конфиденциальной информации злоумышленнику сотрудником, в силу личного расположения или недальновидности последнего.

Учитывая превалирующую компьютерную безграмотность государственных служащих на местах, следует предусмотреть при разработке ПО для организации соединения между гос. подразделениями максимально дружелюбный пользовательский интерфейс и предельную автоматизацию запроса данных.

Все перечисленные типы угроз и способы противодействия им систематизированы ниже в табл. 1.

Таблица 1. Классификация угроз безопасности

Класс	Подкласс	Тип	Описание	Противодействие
Аппаратные	Внешние	Вандализм	Намеренная порча злоумышленником оборудования (силовых установок), вне охраняемой зоны организации	Использование стабилизаторов и фильтров для всех входных каналов связи
		Провокация	Намеренное осуществление злоумышленником действий,	Использование специально разработанной для конкретной

			ведущих к реализации жертвой предсказуемой реакции и использованию ее в целях доступа к защищаемой информации	организации с учетом всех особенностей инструкция по внутренней безопасности
	Внутренние	Саботаж	Намеренная или непреднамеренная порча оборудования сотрудником организации	Планирование и расстановка оборудования в рабочем помещении таким образом, чтобы минимизировать вероятность доступа к соединительным элементам
Программные	Внешние	Снифферы Пакетов	Прикладная программа, которая перехватывает все сетевые пакеты, передающиеся через определенный домен	Использование систем аутентификации и криптографии и коммутируемую инфраструктуру
		IP-спуффинг	Подмена собственного IP-адреса злоумышленником с целью получения доступа в корпоративную сеть	Использование контроля доступа соединений (для обмена внутри сети).Передача по каналам связи только шифрованной информации
		Отказ в Обслуживание (Dos)	Зависание системы, вызванное переполнением канала связи запросами клиентов	Программное ограничение числа полуоткрытых каналов в любой момент времени и ограничение объема трафика
		Парольные Атаки	Использование злоумышленником логина и пароля зарегистрированного пользователя с целью проникновения в систему	Использование сложных паролей на основе персональных данных пользователей
		Атаки Типа Man-In-The-Middle	Искажение или перехват исходящего трафика злоумышленником при использовании промежуточных узлов	Использование мощной системы криптографии
		Атаки Приложений	Злоумышленник использует ошибки в работе приложений, позволяющие получить несанкционированный доступ к конфиденциальной информации	Обновлять систему и приложения при выходе новых патчей, использовать специальные приложения для анализа лог-файлов системы, использование системы IDS
		Сетевая Разведка	Сбор информации о сети с помощью общедоступных данных и приложений, используемый для подготовки атаки против какой–либо сети	Полностью избавиться от сетевой разведки невозможно, но можно использовать системы IDS для своевременного уведомления администратора о ведущейся сетевой разведке
	Внутренние	Злоупотребление Доверием	Злонамеренное использование отношений доверия, существующих в сети	Жесткий контроль уровня доверия в пределах сети
		Переадресация Портов	Разновидность злоупотребления доверием, когда взломанный хост	Использование надежной системы доверия

			используется для передачи трафика через межсетевой экран	
		Вирусы и Трояны	Вредоносные программы, которые выполняют определенные нежелательные функции на рабочей станции конечного пользователя	Использование антивирусов, обновление баз данных сигнатур и приложений
Пользовательские	Внешние	Звонки Сотрудников Техслужб	Телефонные звонки злоумышленников, представляющихся сотрудниками служб обеспечения безопасности/техподдержки и пр.	Подробный и доходчивый инструктаж сотрудников о возможных угрозах безопасности и способах противодействия им; систематические семинары и тренинги для сотрудников с целью повышения сознательности и сплоченности коллектива; разработка внутренних стандартов и правил поведения
		Звонки «Сотрудников»	Звонки злоумышленника, представляющегося сотрудником организации с целью получить авторизованный доступ к сети организации	
		Фишинг	Электронные письма с поддельные уведомления от банков, провайдеров, платежных систем и других организаций	Повышение информационной грамотности сотрудников
		«Подставная Утка»	Проникновение злоумышленника на территорию организации под видом сотрудника	Создание системы внутреннего контроля, включая системы видеонаблюдения и пропускную систему на входе
	Внутренние	Подкуп/ Шантаж	Действия определенного характера, в результате которых собственные сотрудники организации передают конфиденциальную информацию злоумышленнику	Обеспечение надежной системы безопасности, направленной на противодействие как внешним атакам, так и внутренним со строгой политикой приоритетов и прав доступа
		Некомпетентность	Непреднамеренное раскрытие конфиденциальной информации злоумышленнику сотрудником	Проведение тренингов, направленных на повышение мотивации работы и сознательности сотрудников

3. Способы противодействия угрозам системе безопасности

Как уже было отражено в табл. 1, для противодействия угрозам безопасности необходимо реализовывать комплексный подход.

Для исключения угроз безопасности посредствам ПО следует использовать сертифицированные программные продукты проверенных производителей. Также на рабочих станциях необходимо настроить грамотную политику приоритетов и прав доступа. В качестве межсетевого экрана использовать компьютер под управлением ОС, отличной от ОС рабочих станций, так для ПК работающих под Windoows целесообразно использовать прокси-сервер для соединения с Internet под управлением ОС Linix – что существенно затруднит взлом системы

безопасности злоумышленнику. В числе превентивных мер обязательно следует включить своевременное обновление драйверов и установку патчей для приложений.

Для исключения негативного влияния человеческого фактора необходимо проводить коллективные тренинги для повышения информационной грамотности сотрудников и соблюдения правил внутренней безопасности.

Из всего вышеизложенного следует, что наряду со специализированными программными продуктами, такими как антивирусы и IDS, необходимо применять специально разработанную для конкретной организации с учетом особенностей ее деятельности и дислокации политику безопасности в совокупности с правилами внутреннего распорядка.

Для обеспечения безопасности информации – персональных данных пользователей и внутренней документации отдельного органа власти, необходимо использовать комплекс превентивных мер, таких как контроль за программным и аппаратным обеспечением, а также повышать информационную грамотность персонала.

Литература

1. Wikipedia.org [Электронный ресурс]/ Wikimedia Foundation, 2010. – Режим доступа: http://ru.wikipedia.org/wiki /Электронное_правительство.htm/, свободный. – Статья. – яз. рус.

2. Сетевые атаки [Электронный ресурс] / Материалы с сайта lagman–join.narod.ru; Режим доступа: http://lagman–join.narod.ru/spy/CNEWS/cisco_attacks.html/, свободный. – Статья. – яз. рус.

3. Wikipedia.org [Электронный ресурс]/ Wikimedia Foundation, 2010. – Режим доступа: http://ru.wikipedia.org/wiki /Социальная_инженерия.htm /, свободный. – Статья. – яз. рус.

УДК 004.62

МЕТОДИКА ПРЕДВАРИТЕЛЬНОЙ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

Нибилица А.Ю.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Научный руководитель – доц. Хромов И.Н.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Не так давно информационные технологии стали неотъемлемой частью человеческой жизни, но уже прочно укрепили свои позиции, привнеся с собой множество удобных решение и не меньше специфических проблем. С каждым годом компьютеров становится все больше и больше, они объединяются в сети, обмениваются информацией, накапливают важные для людей данные.

Компьютеры, как аппаратное, так и программное обеспечение, создавались людьми и, соответственно, получили от своих создателей разного рода ошибки, несовершенства и недостатки. Опасность распространения конфиденциальной информации посредством

использования уязвимых мест компьютерных систем ставит первостепенную задачу защиты информации.

Для того чтобы сформировать эффективную систему защиты необходимо четко представлять потенциально опасные состояния системы, а для этого нужна качественная система оценки уязвимостей.

1. Общие сведения о методах оценки защищенности

В мае 2000 года представители четырнадцати развитых стран (Канада, Франция, Германия, Великобритания, США, Нидерланды, Италия, Греция, Испания, Швеция, Норвегия, Финляндия, Австралия и Новая Зеландия) подписали основное на данный момент в этой сфере соглашение CCRA (Arrangement of the Recognition of Common Criteria Certificates in the field of Information Technology Security). Соглашение CCRA позволяет значительно расширить возможность присоединения новых стран-участниц, и в 2001 году к соглашению CCRA присоединился Израиль, в 2002 году – Австрия, в 2003 году – Турция, Венгрия и Япония.

Согласно CCRA признание сертификатов общих критериев оценки должно базироваться на уверенности в том, что оценка безопасности компьютерных систем проводилась с использованием принятых методов оценки безопасности информационных технологий. В соглашении CCRA в качестве документа по методам оценки определена общая методология оценки.

В России основным стандартом по проведению оценки защищенности компьютерных систем является руководящий документ (РД) «Общая методология оценки безопасности информационных технологий», принятый коллегией Гостехкомиссии РФ в 2004 г. Но в действующем РД в п. 9.5 « Оценка стойкости функций безопасности» содержится только перечень общих рекомендаций для оценщика без ссылки на конкретные методики оценки. В связи с этим в данной работе представлена методика предварительной оценки защищенности информации.

2. Методика предварительной оценки защищенности информации

Чтобы обеспечить защищенность системы, необходимо нейтрализовать действие возможных для данной системы угроз. Все угрозы можно разделить на три группы: аппаратные, программные и пользовательские.

Рассмотрим принцип действия методики на примере аппаратных угроз, среди которых можно выделить следующие.

Вандализм – намеренная порча злоумышленником оборудования (силовых установок), вне охраняемой зоны организации.

Противодействие: использование стабилизаторов и фильтров для всех входных каналов связи.

Провокация – намеренное осуществление злоумышленником действий, ведущих к реализации жертвой предсказуемой реакции и использованию ее в целях доступа к защищаемой информации.

Противодействие: использование специально разработанной для конкретной организации с учетом всех особенностей инструкция по внутренней безопасности и систем наружного и внутреннего наблюдения.

Саботаж – намеренная или непреднамеренная порча оборудования сотрудником организации.

Противодействие: планирование и расстановка оборудования в рабочем помещении таким образом, чтобы минимизировать вероятность доступа к соединительным элементам.

Сведем представленные угрозы и способы противодействия в таблицу, рабочее поле которой представляет собой пересечение строк – угроз и столбцов – противодействий. Заполним поле значениями от 0 до 5, определяющими степень защищенности системы при использовании определенного способа противодействия. Степень защищенности определяется методом экспертной оценки и имеет следующую интерпретацию: 5 – полностью нейтрализует угрозу, 4 – почти полностью нейтрализует угрозу, 3 – в достаточной степени нейтрализует угрозу, 2 – плохо нейтрализует угрозу, 1 – почти не нейтрализует угрозу, 0 – не нейтрализует угрозу.

ПУ	План внутренней безопасности	Использование источников бесперебойного питания	Использование систем наблюдения
Вандализм	1	4	3
Провокация	5	0	1
Саботаж	4	0	2

Используя приведенные в таблице данные можно рассчитать эффективность использование конкретного способа противодействия или совокупности нескольких способов по формуле:

$$SL = \frac{\sum_{i=1}^{s} \tilde{N}_i}{Max_{SL}} \cdot 100\%$$

где SL – уровень защищенности, C_i – степень защищенности при выборе i-го способа, Max_{SL} – максимально возможная степень защищенности, s – количество угроз.

Правило определения уровня защищенности: необходимо сложить степени защищенности относительно каждой из угроз и полученную сумму разделить на максимальную степень защиты, а затем результат умножить на сто процентов.

$$SL = \frac{4+5+4}{15} \cdot 100\% = 86{,}6\% .$$

При использование данных средств противодействия уровень защищенности аппаратных средств системы составляет 86,6%.

3. Особенности методики предварительной оценки защищенности информации

В основе данной методики лежит принцип экспертной оценки состояния защищенности, из чего следует необходимость профессиональных знаний и навыков у лиц, использующих данный метод. Но для получения адекватного результата оценки, вполне достаточно базовых знаний системного администратора и навыков пользования информационными ресурсами всемирной сети, а именно, бальную оценку по приведенной шкале можно устанавливать оперирую лингвистическими переменными.

Соответствие степени защищенности системы усилиям злоумышленника, затраченным на преодоление системы защиты.

5	полностью нейтрализует угрозу	злоумышленник не сможет преодолеть защиту, даже если потратит много времени/сил/ресурсов системы
4	почти полностью нейтрализует угрозу	злоумышленник потратит много времени/сил/ресурсов системы для преодоления системы защиты
3	в достаточной степени нейтрализует угрозу	злоумышленник потратит достаточно много времени/сил/ресурсов системы для преодоления системы защиты, чтобы его можно было вовремя обнаружить
2	плохо нейтрализует угрозу	злоумышленник потратит немного времени/сил/ресурсов системы для преодоления системы защиты
1	почти не нейтрализует угрозу	злоумышленник почти не затратит времени/сил/ресурсов на преодоление защиты

Например: угрозу парольной атаки можно снизить, используя сложные пароли на основе персональных данных пользователей. Следует задать вопрос: «Такая мера усложнит работу злоумышленника?» – откуда следует ответ: «Да, серьезно усложнит» – а значит, данному способу противодействия соответствует степень защищенности системы 4.

Также следует учесть, что заданная формула вычисления для достижения физической интерпретации налагает определенные ограничения на свои аргументы:

1) Максимально возможная степень защищенности *MaxSL* ограничена сверху:

$$Max_{SL} < 5 \times У,$$

где *У* – количество угроз.

2) Максимальная сумма коэффициентов в строке не должна превышать пяти:

$$\sum_{i=1}^{s} C_i \le 5,$$

где *s* – число способов противодействия угрозе.

Чтобы получить адекватную оценку степени противодействия угрозе совокупности способов, необходимо учитывать взаимную корреляцию (дублирующие функции) выбранных способов.

Уровень защищенности системы в процентах имеет определенный физический смысл, а именно:

- *SL* > 90% – очень высокий уровень защищенности;
- *SL* > 70% – высокий уровень защищенности;
- *SL* > 50% – средний уровень защищенности;
- *SL* > 30% – низкий уровень защищенности;
- *SL* < 30% – практически незащищенная система.

Используя приведенную систему соответствия можно без привлечения сторонних организаций провести экспресс-оценку защищенности предприятия, определить слабые места

системы безопасности и сформировать перечень требований по повышению уровня защищенности системы.

Для обеспечения эффективной системы безопасности на предприятии необходимо как можно более полное представление о потенциальных уязвимостях системы, которое можно получить, использую качественной системе оценки защищенности.

На данный момент не существует четко прописанного стандарта оценки защищенности с перечнем рекомендуемых методик оценки, что приводит к неопределенности в данной области и простору для процветания различного рода мошенничества.

В настоящее время на рынке информационных услуг представлен широкий выбор разнообразных фирм, предлагающих услуги оценки защищенности предприятий с использованием громоздких методик оценки.

Представленная методика позволяет провести экспресс-оценку защищенности предприятия, определить слабые места системы безопасности и сформировать перечень требований по повышению уровня защищенности системы.

Литература

1. Руководящий документ, Безопасность информационных технологий, «Общая методология оценки безопасности информационных технологий», ФСТЭК, 2004. – 184 с.

2. Методология оценки безопасности информационных технологий по общим критериям [Электронный ресурс] / Материалы с сайта http://www.itzashita.ru/. – Режим доступа:http://www.itzashita.ru/theory/metodologiya-ocenki-bezopasnosti-informacionnyx-texnologij-po-obshhim-kriteriyam-2.htm/, свободный. – Статья. – яз. рус.

УДК 004.056.57

ОСНОВНЫЕ АСПЕКТЫ ДЕЯТЕЛЬНОСТИ СИСТЕМНОГО АДМИНИСТРАТОРА ПРИ ОБНАРУЖЕНИИ И ПРОТИВОДЕЙСТВИИ ВТОРЖЕНИЯМ

Нибилица А.Ю.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Научный руководитель – доц. Хромов И.Н.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В наши дни обязательной частью любой сферы человеческой деятельности стали компьютеры: настольные ПК и ноутбуки дома и в офисе, терминалы для оплаты услуг и банкоматы на улицах и в метро, компьютерные клубы и интернет-кафе – все это прочно закрепилось в современном городе и постепенно распространяется в провинции. И какой бы не была упомянутая динамика, важно то, что человечество жизни без компьютеров уже не представляет.

Сколько можно было бы не перечислять достоинства личного пользования ПК, но людям все равно будет мало – и тогда на сцену информационных технологий выходят сети. Объединение нескольких ЭВМ в сеть с общими данными и устройствами позволило добиться не только серьезного прироста эффективности при работе с распределенными ресурсами, но и связать пользователей, сидящих за мониторами своих ПК.

Теперь стоит упомянуть, что если с управлением отдельным компьютером мог справиться всего один человек, обладающий знаниями продвинутого пользователя, то для настройки и поддержки корректного функционирования целой сети (пусть даже не превышающей десяти ПК) уже понадобился квалифицированный специалист – системный администратор, в обязанности которого входит не только техническая поддержка рядовых пользователей, но и обнаружение и противодействие вторжениям.

Обязанности системного администратора

Сейчас только крупные и обеспеченные организации могут позволить себе содержать одновременно системного администратора, т.е. человека, занимающегося технической поддержкой пользователей, и специалиста по защите информации, в обязанности которого напрямую входит обнаружение и противодействие вторжениям, в любом виде способным к несанкционированному доступу к информации.

Поэтому в малых и средних, в большинстве своем, частных, фирмах широко используется практика совмещения обязанностей системного администратора и специалиста по защите информации, почему следует отдельно остановиться на типовом перечне обязанностей системного администратора.

Основные обязанности системного администратора:

– добавление и удаление пользователей (процесс управления записями можно автоматизировать, но ряд решений, связанных с включением в систему нового пользователя (где следует разместить его начальный каталог, на каком компьютере будет создана учетная запись и т.д.), должен принимать администратор);

– подключение и удаление аппаратных средств (в случае приобретения новых аппаратных средств или подключения уже имеющихся устройств к другой машине, систему нужно переконфигурировать таким образом, чтобы она распознала и активизировала эти устройства);

– резервное копирование (процесс можно автоматизировать или поручить подчиненным, но все равно системный администратор обязан убедиться в том, что резервное копирование выполнено правильно и по графику);

– инсталляция новых программ (после приобретения нового программного обеспечения его нужно инсталлировать и протестировать, если программы работают нормально, пользователям необходимо сообщить об их наличии и местонахождении);

– мониторинг системы (проверка правильности функционирования электронной почты и телеконференций; просмотр регистрационных файлов на предмет наличия ранних признаков неисправностей; контроль за подключением локальных сетей; контроль наличия системных ресурсов и пр.);

– поиск неисправностей (обязательная задача администратора – диагностировать сбои в системе и в случае необходимости вызывать специалистов);

– ведение локальной документации (системный администратор должен документировать все инсталлируемые программные средства, не входящие в стандартный комплект поставки, документировать разводку кабелей, вести записи по обслуживанию всех аппаратных средств, регистрировать состояние резервных копий, документировать локальные процедуры и правила работы с системой);

– слежение за безопасностью системы (системный администратор отвечает за реализацию стратегии защиты и должен периодически проверять, не нарушена ли защита системы);

– оказание помощи пользователям (системный администратор обязан своевременно реагировать на любые неисправности в системе, сигнализируемые пользователями; это требует большого количества времени и коммуникабельности; «помощь пользователям» является наиболее трудоемким пунктом работы системного администратора).

Как можно видеть среди вышеперечисленного, задачи системного администратора объемны и трудоемки даже при возможности некоторой автоматизации процессов, это приводит к возрастанию рисков не обнаружения критических ситуаций вследствие усталости из–за высокой загруженности и монотонности работы.

Поэтому выделим базовый набор признаков, позволяющий максимально достоверно выявить факт вторжения в систему.

Основные признаки вторжения

Прежде всего, нас будут интересовать признаки вторжений в систему не с точки зрения пользователя, а с позиции системы безопасности, т.е. *компьютерной программы*. Конечно, для системного администратора будет важной информация, исходящая от пользователя, с примерным содержанием: «Мой компьютер не выходит в сеть» – или: «Компьютер издает странные звуки/изменяет обои/просит отправить sms с кодом на номер…» – но в данной статье сконцентрируем основное внимание на событиях системы, выдающих факт вторжения и доступных автоматизированному анализу.

Если системный администратор решит использовать программу, допустим, собственноручно написанную, для обнаружения аномалий в поведении системы, демаскирующих вторжение, ему необходимо учесть следующие пункты.

1) **Изменение списка автозагрузки**

При установке программного обеспечения на ПК регламентируются программы, запускающиеся при входе в систему. В большинстве случаев этот список на офисных ПК никогда не меняется. Если создать общий для всей организации перечень разрешенных программ, то при автоматическом анализе всех рабочих станций в сети можно выявить несоответствия и потенциальные угрозы, что позволит избежать потенциально возможного НСД к данным и повысить эффективность работы сотрудников на местах.

2) **Анализ запущенных процессов**

Также, как и с программами автозагрузки, можно выделить типовой список процессов, характерной для организации, несовпадение с которым может вызвать подозрение на организацию вторжения.

3) **Анализ журнала событий**

Благодаря встроенной во все современные операционные системы возможности непрерывного протоколирования событий, можно без больших усилий выявить факт заражения системы. Обнаружить заражение можно сравнив списки запускавшихся приложений/обращений к ресурсам за последний месяц и списком приложений последних дней, особое внимание стоит уделить системным событиям, соответствующим неудачам при запуске служб или инициализации драйверов, попытки повышения прав до уровня администратора. Грамотно сформулированные правила отбора при анализе журнала позволят выявить нежелательное вторжение или же вовремя предупредить его.

4) **Удаленные файлы**

При наличии в списке удаления системных файлов или файлов, принадлежащих определенной программе, можно обнаружить следы НСД в систему.

5) **Анализ периодов включения/выключения межсетевых экранов, брандмауэров, антивируса**

Естественно, что ответственного системного администратора должен привлечь сам факт отключения межсетевого экрана или брандмауэра, но не менее важны для анализа и выявления причин время и длительность периода неактивности.

6) **Анализ активности рабочей станции в сети**

При наличии статистики взаимодействия между несколькими рабочими станциями в сети, можно выявить аномальное поведение – например, активность ПК или сервера, давно неиспользуемого в работе организации, или запрос доступа в Internet от рабочей станции, по должностным обязанностям не нуждающейся в доступе к глобальной сети.

Каждый из этих пунктов не гарантирует 100% вероятности обнаружения вторжения, но при известной совокупности подозрительных сочетаний параметров, можно вынести однозначное заключение о возможности вторжения в локальную сеть организации.

Способы противодействия вторжениям

Уже давно сформулированы различные правила по противодействию вторжениям вредоносных программ или злоумышленников в частные сети отдельных пользователей или предприятий, но с каждым днем появляются все новые и новые обходные пути, позволяющие совершить НСД к защищенным файлам и данным. Отчасти это вызвано некорректной настройкой политики безопасности в сети, отчасти ошибками в работе прикладных программ, но тем не менее следует придерживаться основных правил и следующих рекомендаций для формирования качественной системы безопасности.

1) **Использование межсетевых экранов, брандмауэров, антивирусов, специализированных программ обнаружения и противодействия вторжениям**

Признаки типичных сценариев вторжений известны и вполне доступны для анализа существующим системам обнаружения вторжений; несмотря на то, что эти программы, какими бы хорошими и мощными они не были, не могут противодействовать абсолютно всем вторжениям, их использование значительно усложнит злоумышленнику задачу и позволит системному

администратору, если не окончательно предотвратить вторжение, то как минимум выиграть время.

2) **Блокирование и анализ входящих и исходящих сетевых пакетов**

Какой бы не была замечательной идея дождаться полного формирования массива данных, разбитого по пакетам и переданного через сеть, и дальнейшего его скрупулезного анализа, такая стратегия значительно увеличивает нагрузку на пропускную способность сети и требует значительных затрат, поэтому системным администраторам остается только надеяться на системы обнаружения вторжений со встроенной функцией анализа входящего трафика.

3) **Систематический анализ сети по перечисленным выше признакам обнаружения вторжений**

При возможности автоматизации процесса анализа работы сети можно выбрать время, когда в сети организации появляются «зеленые зоны», периоды наименьшей загрузки средств корпоративной сети, и в эти промежутки проводить автоматизированный анализ, что позволит избежать перегрузки сети и одновременно контролировать ситуацию на предмет вторжения.

4) **Регистрация событий и оповещение ответственных лиц**

Обязательным результатом любого анализа должен быть отчет о просмотренных данных и событиях с возможностью формирования выборки по разным критериям и средствами сигнализации системному администратору о наличие подозрительных ситуаций.

Из вышеперечисленного можно сделать вывод, что использование автоматизированных систем обнаружения вторжений значительно сократит нагрузку на системного администратора по обеспечению безопасности сети, но не исключает полностью участие человека.

Обязанности современных системных администраторов в большинстве случаев включают в себя пункты по обеспечению безопасности корпоративной сети. При анализе этих пунктов можно выделить действия, поддающиеся полной или частичной автоматизации, для сокращения нагрузки на системных администраторов и повышения качества их работы.

В данной статье были рассмотрены основные способы противодействия вторжениям, доступные для автоматизации и основывающиеся на приведенных выше признаках вторжения в корпоративную сеть организаций.

Но, не смотря на возможность переложить часть обязанностей с плеч системного администратора на специализированную программу, полностью исключить участие человека и человеческого фактора в процессе обеспечения безопасности в корпоративной сети пока не представляется возможным.

Литература

1. Wikipedia.org[Электронный ресурс]/ Wikimedia Foundation, 2010. – Режим доступа: http://ru.wikipedia.org/wiki /Системный_администратор.htm/, свободный. – Статья. – яз. рус.

2. Сетевые атаки [Электронный ресурс] / Материалы с сайта lagman–join.narod.ru; Режим доступа: http://lagman–join.narod.ru/spy/CNEWS/cisco_attacks.html/, свободный. – Статья. – яз. рус.

3. Уральский центр систем безопасности [Электронный ресурс]/ Материалы с сайта www.ussc.ru; Режим доступа: http://www.ussc.ru/list.php?ttop=150106&id=110026 /, свободный. – Статья. – яз. рус.

УДК 004.93

ПОСТРОЕНИЕ МОДЕЛИ СИСТЕМЫ БЕЗОПАСНОСТИ НА ОСНОВЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Нибилица А.Ю.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Научный руководитель – доц. Хромов И.Н.

Санкт–Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Современные потребности человека ставят перед вычислительной техникой все более сложные и трудоемкие задачи, требующие применения нелинейного подхода и нечеткой логики, практически нереализуемые на традиционном аппаратном обеспечении с линейными алгоритмами. Все чаще исследователи в различных областях науки и техники сталкиваются с необходимостью использовать параллельные вычисления, алгоритмы без строгой формализации параметров и способные к самообучению системы.

Для решения технических, экономических, статистических задач такого рода используются искусственные нейронные сети, позволяющие за сравнительно короткие сроки проанализировать большие объемы данных и вывести наиболее вероятный на данной выборке результат.

1. Общие сведения об искусственных нейронных сетях

Искусственные нейронные сети (ИНС) представляют собой программно-аппаратный аналог биологических нейронных сетей, позволяющих вести параллельную высокопродуктивную обработку информации. По примеру биологических прототипов основой ИНС являются нейроны – специализированные структуры, настроенные на анализ данных, отвечающих заданным параметрам. Нейроны, воспринимающие информацию в качестве цельного образа – как определенную совокупность параметров – связываются между собой послойно и неравноценно, т.е. каждый новый слой связан с предыдущим и эти связи имеют различные настраиваемые веса.

Основными минусами технологии ИНС является их ресурсоемкость и высокая стоимость программно-аппаратной реализации, но при немалых затратах на создание ИНС демонстрируют высокие показатели самоокупаемости. Еще одним существенным недостатком можно считать, что традиционные ИНС неспособны объяснить, каким образом они решают задачу – так как процесс обучения, за исключением простейших случаев, зависит от большого числа взаимосвязанных между собой факторов, что значительно усложняет анализ и проверку полученных результатов. Также нельзя забывать о том, что созданные по образу и подобию человека ИНС склонны к

ошибкам, в силу искусственного ограничения числа входных параметров и оправданного примитивизма используемой модели.

Преимущества нейросетевого подхода заключаются в использовании параллелизма при обработке информации, позволяющем ускорить процесс анализа входных данных; едином и эффективном принципе обучения, обеспечивающем обоснованный качественный результат; надежности функционирования благодаря возможности самонастраиваться и самообучаться; способности решать неформализованные задачи на основе полученных знаний и накопленного опыта.

Области применения ИНС весьма разнообразны – это распознавание текста и речи, семантический поиск, экспертные системы и системы поддержки принятия решений, предсказание курсов акций, системы безопасности, анализ текстов. В военной сфере в качестве примера можно привести ИНС для управления автопилотируемым гиперзвуковым самолетом–разведчиком LoFLYTE (Low–Observable Flight Test Experiment), разработанная фирмой Accurate Automation Corp, Chattanooga, TN по заказу NASA и Air Force, позволяющая автопилоту обучаться, копируя приемы пилотирования летчика; в сфере экономики и финансов – ИНС фирмы Neural Data для предварительной обработки транзакций на валютных биржах ряда стран, отслеживающая подозрительные сделки; в сфере здравоохранения – система объективной диагностики слуха у грудных детей компании «НейроПроект», способная с достоверностью эксперта по 200 наблюдениям вместо 2000 в течение нескольких минут определить уровень слуха без участия специалиста.

2. Построение модели системы безопасности на ИНС

В силу своей природы ИНС могут иметь более двух слоев нейронов, объединенных по принципу: каждый нейрон произвольного слоя связан со всеми нейронами предыдущего слоя, если произвольный слой первый – каждый его нейрон связан со всеми входами ИНС; каждая связь, объединяющая два нейрона в сети, имеет свой вес.

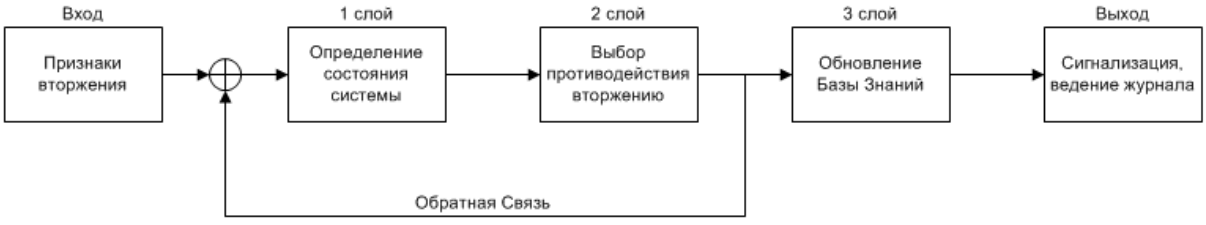


Рисунок 1. Функциональная схема модели противодействия вторжениям на базе ИНС

В предлагаемой модели, представленной на рис. 1, мы рассмотрим ИНС в три слоя. Первый слой будет включать в себя состояния системы (такие как «опасность», «тревога», «предупреждение», «игнорирование»), что позволит выбрать стратегию противодействия выявленной угрозе. На втором слое будет формироваться реакция системы (действия, которые следует предпринять для предотвращения вторжения: «отключение сетевого соединения», «блокирование процесса», «перенесение адреса в «черный список», «игнорирование»). На третьем слое пополняется База Знаний и с помощью обратной связи заново определяем состояние системы. На входе ИНС располагаются признаки вторжения («ошибка аутентификации»,

«запрос на права администратора», «попытка открытия чужого файла», «попытка установить неразрешенное соединение», «запуск неавторизованных программ»), используемые для обнаружения факта взлома системы, а на выходе заполняется Журнал Мониторинга Системы и принимается решение об оповещении ответственного за системную безопасность лица. Также следует отметить, что обратная связь между третьим и первым слоем влияет на определение весов межнейронных связей.

Построим математическую модель системы, представленной на рис. 2, где U – вектор входов, задающие входные параметры, X'' – вектор состояния нейронов первого слоя, определяющий состояние системы в плане безопасности, X' – вектор состояния нейронов второго слоя, определяющий реакцию системы, необходимые действия в сложившейся ситуации, X – вектор состояния нейронов третьего слоя, повторно определяющий состояния системы после выполнения действий по обеспечению безопасности, Y – вектор выходов системы, определяющий результат. Связи между векторами входа, состояний и выхода определим с помощью матриц B, A1, A2, C; обратную связь зададим с помощью матрицы L.

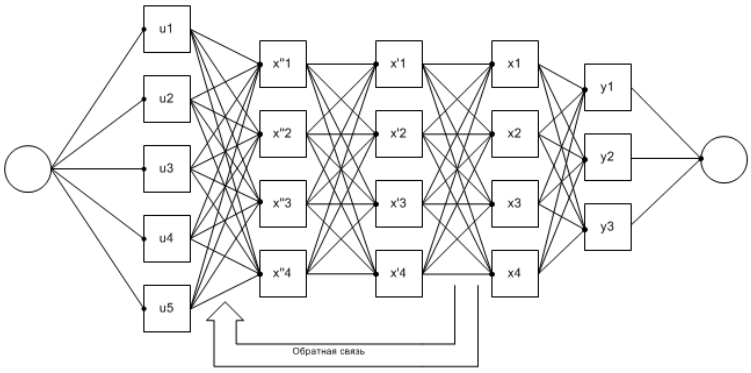


Рисунок 2. Структурная схема модели противодействия вторжениям на базе ИНС

Математическая модель для заданной системы имеет вид:

$$\begin{cases} x'' = Lx + Bu \\ x' = A2x'' \\ x = A1x' \\ y = Cx \end{cases} \Rightarrow \begin{cases} x = A1\ A2\ [I - L\ A1\ A2]^{-1}\ Bu \\ y = Cx \end{cases} \Rightarrow \begin{cases} x = Fu \\ y = Cx \end{cases}$$

Математическая модель системы приведена в форме *Вход-Состояние-Выход*, где *I* единичная матрица размерности 3x3; обратная связь в системе положительная, чтобы отобразить реально протекающие процессы: после принятия определенных действий во втором слое состояние системы обновляется.

Для большей прозрачности выполняемых действий разложим векторы на компоненты, присваивая значения лингвистического множества.

Вектор входных значений:

$$U = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \end{bmatrix} = \begin{bmatrix} \text{"ошибка аутентификации"} \\ \text{"запрос на права администратора"} \\ \text{"попытка открытия чужого файла"} \\ \text{"попытка установить неразрешенное соединение"} \\ \text{"запуск неавторизованных программ"} \end{bmatrix}$$

Вектор состояния системы:

$$X'' = \begin{bmatrix} x''_1 \\ x''_2 \\ x''_3 \\ x''_4 \end{bmatrix} = \begin{bmatrix} \text{"опасность"} \\ \text{"тревога"} \\ \text{"предупреждение"} \\ \text{"игнорирование"} \end{bmatrix}$$

Вектор реакции системы:

$$X' = \begin{bmatrix} x'_1 \\ x'_2 \\ x'_3 \\ x'_4 \end{bmatrix} = \begin{bmatrix} \text{"отключение сетевого соединения"} \\ \text{"блокировка процесса"} \\ \text{"перенесение адреса в "черный список"} \\ \text{"игнорирование"} \end{bmatrix}$$

Вектор измененных состояний системы:

$$X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} \text{"опасность"} \\ \text{"тревога"} \\ \text{"предупреждение"} \\ \text{"игнорирование"} \end{bmatrix}$$

Вектор выходных значений:

$$Y = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} \text{"отправка } sms \text{ администратору"} \\ \text{"вывод предупреждения на экран"} \\ \text{"игнорирование"} \end{bmatrix}$$

Отношения между компонентами задается с помощью экспертной оценки по 10ти бальной шкале, нормированной по основанию 10 и определяющей вклад каждого предыдущего компонента в последующий – их зависимости – по следующей формуле:

Состояние системы {«опасность»} равно 0,5х{«ошибка аутентификации»} плюс 0,6х{«запрос на права администратора»} плюс 0,6х{«попытка открытия чужого файла»} плюс 0,7х{«попытка установить неразрешенное соединение»} плюс 0,5х{«запуск неавторизованных программ»}.

Таким образом, получаем строку коэффициентов: [0,5 0,6 0,6 0,7 0,5]; аналогично заполняем все матрицы связей и получаем следующий набор.

Матрица, связывающая вход и состояния:

$$B = \begin{bmatrix} 0{,}5 & 0{,}6 & 0{,}6 & 0{,}7 & 0{,}5 \\ 0{,}5 & 0{,}3 & 0{,}3 & 0{,}4 & 0{,}4 \\ 0{,}5 & 0{,}2 & 0{,}2 & 0{,}3 & 0{,}2 \\ 0{,}5 & 0{,}1 & 0{,}1 & 0{,}2 & 0{,}1 \end{bmatrix}$$

Матрицы, определяющие отношение между состояниями системы:

$$A1 = \begin{bmatrix} 1 & 0{,}7 & 0{,}4 & 0{,}2 \\ 0{,}8 & 0{,}5 & 0{,}3 & 0{,}1 \\ 0{,}6 & 0{,}5 & 0{,}2 & 0{,}1 \\ 0{,}4 & 0{,}2 & 0{,}1 & 0{,}1 \end{bmatrix}$$

$$A2 = \begin{bmatrix} 0{,}1 & 0{,}3 & 0{,}6 & 0{,}8 \\ 0{,}2 & 0{,}4 & 0{,}7 & 0{,}9 \\ 0{,}4 & 0{,}5 & 0{,}8 & 0{,}9 \\ 0{,}5 & 0{,}6 & 0{,}8 & 0{,}9 \end{bmatrix}$$

Матрица обратных связей:

$$L = \begin{bmatrix} 0{,}1 & 0{,}1 & 0{,}1 & 0{,}0 \\ 0{,}2 & 0{,}1 & 0{,}1 & 0{,}0 \\ 0{,}2 & 0{,}2 & 0{,}1 & 0{,}0 \\ 0{,}3 & 0{,}1 & 0{,}1 & 0{,}0 \end{bmatrix}$$

Матрица выхода:

$$C = \begin{bmatrix} 1 & 0{,}7 & 0{,}4 & 0{,}1 \\ 0{,}8 & 0{,}5 & 0{,}3 & 0{,}1 \\ 0{,}3 & 0{,}2 & 0{,}1 & 0{,}1 \end{bmatrix}$$

Матрица преобразований:

$$F = \begin{bmatrix} 2{,}00 & 4{,}20 & 4{,}20 & 4{,}60 & 4{,}00 \\ -1{,}00 & 0{,}80 & 0{,}80 & 0{,}60 & 0{,}40 \\ -0{,}65 & -1{,}66 & -1{,}66 & -1{,}79 & 0{,}74 \\ 0{,}41 & -0{,}24 & -0{,}23 & -0{,}15 & 0{,}86 \end{bmatrix}$$

Знак «минус» в матрице преобразований F говорит о том, что данный входной компонент не влияет на формирования определенного состояния системы и его можно без существенных последствий обнулить. Тогда матрица преобразований примет вид:

$$F = \begin{bmatrix} 2{,}00 & 4{,}20 & 4{,}20 & 4{,}60 & 4{,}00 \\ 0{,}00 & 0{,}80 & 0{,}80 & 0{,}60 & 0{,}40 \\ 0{,}00 & 0{,}00 & 0{,}00 & 0{,}00 & 0{,}74 \\ 0{,}41 & 0{,}00 & 0{,}00 & 0{,}00 & 0{,}86 \end{bmatrix}$$

Так как моделирование подобной системы представляется затруднительным в обычных условиям, используя известные математические преобразования, приведенные выше, можно снизить число слоев в ИНС до одного, не теряя при этом общности рассуждений, и промоделировать систему в пакете Fuzzy Logic Toolbox прикладной программы Matlab.

3. Анализ полученных результатов

Используя пакет Fuzzy Logic Toolbox прикладной программы Matlab, можно получить наглядное представление о функционировании и основных характеристиках исследуемой модели.

В табл. 1 представлены три набора входных и выходных данным моделируемой системы с расшифровкой имеющихся значений.

Таблица 1

№ п/п	**Вход *U***		**Выход *Y***	
	Значение	*Расшифровка*	*Значение*	*Расшифровка*
1	u_1=1	была ошибка аутентификации	y_1=11,82	Отправка sms администратору
	u_2=1	был запрос на получение прав администратора	y_2=9,38	Вывод предупреждения на экран
	u_3=0	не было попытки открытия чужого файла	y_3=3,56	Игнорирование
	u_4=1	была попытка установить	*Примечание:*	

		неразрешенное соединение	в системе подразумевается, что при y_1>10 – отправка sms при y_2>5 – предупреждение на экран при y_3>1 – игнорирование Порядок приоритета: $y_1 > y_2 > y_3$	
	u_5=0	не было запуска неавторизованных программ		
2	u_1=0	не была ошибка аутентификации	y_1=4.76	Отправка sms администратору
	u_2=0	не было запроса на получение прав администратора	y_2=3.76	Вывод предупреждения на экран
	u_3=1	не было попытки открытия чужого файла	y_3=1.42	Игнорирование
	u_4=0	была попытка установить неразрешенное соединение		
	u_5=0	не было запуска неавторизованных программ		
3	u_1=1	была ошибка аутентификации	y_1=7,06	Отправка sms администратору
	u_2=0	не было запроса на получение прав администратора	y_2=5,62	Вывод предупреждения на экран
	u_3=0	не было попытки открытия чужого файла	y_3=2,14	Игнорирование
	u_4=1	была попытка установить неразрешенное соединение		
	u_5=0	не было запуска неавторизованных программ		

В табл. 1 цветом выделены действия, на выполнение которых будет запрограммирована система при выполнении определенных условий

В настоящее время ИНС являются важным расширением понятия вычисления. Они уже позволили справиться с рядом непростых проблем и обещают создание новых программ и устройств, способных решать задачи, которые пока под силу только человеку. Современные нейрокомпьютеры используются в основном в коммерческих целях, таких как прогнозирования курса акций, расчет финансовых рисков и моделирование рынка, и поэтому редко и не полностью задействуют свой потенциал «параллелизма».

Разработанная модель системы безопасности описана в векторно-матричной форме, что позволяет достаточно полно отобразить все необходимые характеристики системы в доступные параметры.

Представленная в данной статье модель построения системы безопасности на ИНС является достаточно общей и требует детальной проработки совместно с экспертами в области безопасности, но при этом демонстрирует неплохие качественные характеристики для заданного уровня детализации, хороший потенциал и высокое прикладное значение.

Литература

1. Яхъяева Г.Э. Нечеткие множества и нейронные сети: учебное пособие.– 2-е изд., испр. – М. : БИНОМ, 2008. – 316 с.: ил., табл.

2. Нейронные сети [Электронный ресурс] / Материалы с сайта www.statsoft.ru; Режим доступа: http://www.statsoft.ru/home/textbook/modules/stneunet.html/, свободный. – Статья. – яз. рус.

3. Нейронные сети [Электронный ресурс] / Материалы с сайта www.aiportal.ru; Режим доступа: http://www.aiportal.ru/articles/neural–networks/neural–networks.html/, свободный. – Статья. – яз. рус.

УДК 004

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ И ПРОГНОЗИРОВАНИЕ ЛЕСНЫХ ПОЖАРОВ

Никитин С.В.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Научный руководитель – к.т.н., доц. Жигулин Г.П.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Лесные пожары – бедствие, наносящее России с ее обширными лесными массивами, неисчислимые материальные, моральные и экологические потери. В 1999 г. было зафиксировано свыше 30 000 лесных пожаров общей площадью свыше 2 миллионов гектаров. Тревожит тот факт, что год от года их количество не уменьшается.

Природные пожары, особенно лесные и торфяные, иногда становятся для России настоящим бедствием. Сгорают гигантские площади лесных массивов, уничтожаются уникальные экосистемы.

С пожарами в атмосферу выбрасывается огромное количество дыма, содержащего такие опасные загрязнители как углекислый газ, угарный газ и окись азота. В отдельные годы этих выбросов столько же, сколько от сжигания всей перерабатываемой в России нефти. От задымления страдают жители городов и поселков. По оценкам медиков, задымление Москвы в результате лесных и торфяных пожаров летом 2002 г. могло привести к гибели более 100 человек. Особенно опасно задымление воздуха для детей первого года жизни и новорожденных. У них под воздействием дыма увеличивается частота врожденных пороков сердца и заболеваний органов дыхания.

На тушение лесных пожаров тратятся огромные, по масштабам современной России средства.

В самые «горячие» месяцы практически все организации лесной сферы России переключается на борьбу с пожарами и вынужденно оставляют все остальные дела.

Известно, что пожар лучше предотвратить, чем потом, рискуя жизнью его тушить, именно поэтому в борьбе с пожарами важную роль играет их раннее обнаружение и прогнозирование распространения огня.

Целью данного проекта является разработка модели для прогнозирования количества лесных пожаров на территории Российской Федерации.

Для достижения поставленной цели в работе необходимо решить следующие **задачи**:

1) изучение существующих подходов прогнозирования;
2) выявление общих закономерностей в существующих моделях;
3) разработка собственной модели прогнозирования.

Методы исследования: При разработке модели использовались математические методы расчетов.

Практическая ценность:

Реализация и внедрение результатов: Разработанное ПО моделирования и прогнозирования ЧС, внедрено в Санкт-Петербургском государственном университете информационных технологий, механики и оптики на кафедре мониторинга и прогнозирования информационных угроз при проведении практических занятий и самостоятельной работы студентов по дисциплине «Программное моделирование и прогнозирование состояний разнородных систем».

Некогда достаточно эффективная система борьбы с пожарами на природных территориях в нашей стране в последние годы находится в состоянии крайнего упадка. Даже в зоне активной защиты леса при нынешнем сокращении возможностей авиалесоохраны и системы наземного наблюдения крайне редко удается обнаружить пожар на ранней стадии. Именно поэтому общество испытывает насущную потребность в моделирующих системах и прогнозах, помогающих принимать решения по оценке складывающихся ситуаций, выработке стратегических направлений в развитии экономического и социального потенциала страны.

В современных условиях умение предвидеть и прогнозировать будущее а, следовательно, и влиять на социальные процессы становится также одним из самых ценных качеств молодого специалиста.

Прогнозирование и моделирование занимают здесь особо важное место как высокотехнологичные методы научного анализа и предвидения.

Математическое моделирование во многих случаях дает возможность оценить степень опасности того или иного процесса в природе и обществе, провести оперативные расчеты рекомендуемых средств по предотвращению надвигающихся чрезвычайных обстоятельств или снижению величины ущерба от неизбежных катаклизмов и дать соответствующие прогнозы.

УДК 004.387

НОВЫЕ МЕТОДИКИ И СРЕДСТВА ПОИСКА ЭЛЕКТРОННЫХ УСТРОЙСТВ «ПЕРЕХВАТА ИНФОРМАЦИИ»

Прожерин В.Г., Прожерин Д.В.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Информация заняла существенное место на рынке товаров и услуг, стоимость отдельных разработок исчисляется миллиардами долларов, своевременное выявление перспективных разработок у конкурентов снижает себестоимость собственных исследований и сокращает их срок. Соответственно рынок устройств перехвата информации неуклонно растет, совершенствуется, при их создании используются новейшие разработки в области IT технологий, оптико-электронных и электронных средств. Одновременно дальнейшее развитие получают средства и методики противодействия данным устройствам. Каковы же перспективы развития средств аппаратного противодействия?

Классификация средств перехвата акустической информации приведена во многих справочниках и учебных пособиях, в рамках этой статьи не будем подробно рассматривать данный вопрос. Не смотря на значительное количество устройств по снятию информации, все они обладают определенными демаскирующими признаками, и обнаружение электронных устройств перехвата информации (закладных устройств), также как и любых других объектов, производится в соответствии с этими признаками.

1) Наиболее информативными признаками проводной микрофонной системы являются:

– тонкий провод, неизвестного назначения, подключенный к малогабаритному микрофону (часто закамуфлированному и скрытно установленному), и выходящий в другое помещение;
– наличие в линии (проводе) неизвестного назначения постоянного (в несколько вольт) напряжения и низкочастотного информационного сигнала.

2) Демаскирующие признаки автономных некамуфлированных акустических закладок включают:

– признаки внешнего вида - малогабаритный предмет (часто в форме параллелепипеда) неизвестного назначения;
– одно или несколько отверстий малого диаметра в корпусе;
– наличие автономных источников питания (например, аккумуляторных батарей);
– наличие полупроводниковых элементов, выявляемых при облучении обследуемого устройства нелинейным радиолокатором;
– наличие в устройстве проводников или других деталей, определяемых при просвечивании его рентгеновскими лучами.

3) Камуфлированные акустические закладки по внешнему виду на первый взгляд не отличаются от объекта имитации, особенно если закладка устанавливается в корпус бытового

предмета без изменения его внешнего вида. Такие закладки можно выявить путем разборки предмета.

Закладки, устанавливаемые в малогабаритные предметы, ограничивают возможности последних. Эти ограничения могут служить косвенными признаками закладных устройств. Чтобы исключить возможность выявления закладки путем ее разборки, места соединения разбираемых частей склеивают.

Некоторые камуфлированные закладные устройства не отличаются от оригиналов даже при тщательном внешнем осмотре. Их можно обнаружить только при просвечивании предметов рентгеновскими лучами.

В ряде случаев закамуфлированное закладное устройство обнаруживается по наличию в обследуемом предмете не свойственных ему полупроводниковых элементов (выявляемых при облучении его нелинейным радиолокатором). Например, обнаружение полупроводниковых элементов в пепельнице или в папке для бумаг может указать на наличие в них закладных устройств.

Наличие портативных звукозаписывающих и видеозаписывающих устройств в момент записи можно обнаружить по наличию их побочных электромагнитных излучений (излучений генераторов подмагничивания и электродвигателей).

Дополнительные демаскирующие признаки акустических радиозакладок**:**

– радиоизлучения (как правило, источник излучения находится в ближней зоне) с модуляцией радиосигнала информационным сигналом;
– наличие (как правило) небольшого отрезка провода (антенны), выходящего из корпуса закладки.

Вследствие того, что при поиске радиозакладок последние находятся в ближней зоне излучения и уровень сигналов о них, как правило, превышает уровень сигналов от других РЭС, у большинства радиозакладок обнаруживаются побочные излучения и, в частности, излучения на второй и третьей гармониках, субгармониках и т.д.

Дополнительные демаскирующие признаки сетевых акустических закладок**:**

– наличие в линии электропитания высокочастотного сигнала (как правило, несущая частота от 40 до 600 кГц, но возможно наличие сигнала на частотах до 7 МГц), модулированного информационным низкочастотным сигналом;
– наличие тока утечки (от единиц до нескольких десятков мА) в линии электропитания при всех отключенных потребителях;
– отличие емкости линии электропитания от типовых значений при отключении линии от источника питания (на распределительном щитке электропитания) и отключении всех потребителей.

Дополнительные демаскирующие признаки акустических и телефонных закладок с передачей информации по телефонной линии на высокой частоте:

– наличие в линии высокочастотного сигнала (как правило, несущая частота до 7 МГц) с модуляцией его информационным сигналом.

Дополнительные демаскирующие признаки телефонных радиозакладок:

– радиоизлучения с модуляцией радиосигнала информационным сигналом, передаваемым по телефонной линии;

– отличие сопротивления телефонной линии от «∞» при отключении телефонного аппарата и отключении линии (отсоединении телефонных проводов) на распределительной коробке (щитке);

– отличие сопротивления телефонной линии от типового значения (для данной линии) при отключении телефонного аппарата, отключении и закорачивании линии на распределительной коробке (щитке);

– падение напряжения (от нескольких десятых до 1,5...2 В) в телефонной линии (по отношению к другим телефонным линиям, подключенным к данной распределительной коробке) при положенной и поднятой телефонной трубке;

– наличие тока утечки (от единиц до нескольких десятков мА) в телефонной линии при отключенном телефоне.

Дополнительные демаскирующие признаки акустических закладок типа «телефонного уха»:

– отличие сопротивления телефонной линии от " ∞ " при отключении телефонного аппарата и отключении линии (отсоединении телефонных проводов) на распределительной коробке (щитке);

– падение напряжения (от нескольких десятых до 1,5...2 В) в телефонной линии (по отношению к другим телефонным линиям, подключенным к данной распределительной коробке) при положенной телефонной трубке;

– наличие тока утечки (от единиц до нескольких десятков мА) в телефонной линии при отключенном телефоне;

– подавление (не прохождение) одного-двух вызывных звонков при наборе номера телефонного аппарата.

Дальнейшее развитие средств перехвата информации, инициирует развитие средств и методик противодействия.

Простейшими и наиболее дешевыми обнаружителями радиоизлучений закладных устройств являются индикаторы электромагнитного поля**,** которые световым или звуковым сигналом сигнализируют о наличии в точке расположения антенны электромагнитного поля с напряженностью выше пороговой (фоновой). Более сложные из них **-** частотомеры обеспечивают, кроме того, измерение несущей частоты наиболее "сильного" в точке приема сигнала.

Одним из новых промышленно выпускаемых устройств является Индикатор «**Радэкс ЭМИ 50**». При помощи данного прибора можно обнаружить и локализовать электромагнитные поля повышенной активности, устанавливать не только сам факт наличия электромагнитного поля, но и выявлять месторасположение источников электромагнитного излучения. Одной из особенностей данного прибора является наличие изотопной антенны. Индикатор электромагнитных полей «**Радэкс ЭМИ 50**» является достаточно компактным и простым в эксплуатации прибором. У данного прибора предусмотрена функция запоминания предыдущих измерений. Если электромагнитное поле в помещении выходит за рамки допустимых норм, то прибор подает оператору звуковые сигналы.

Наряду с использованием индикаторов электромагнитного поля для обнаружения радиоизлучений применяются радиочастотомеры. Наиболее характерным представителем данных устройств являются радиочастотомеры RFM-31, RFM-32**.** Данные устройства**,** выпускаемые в Польше по лицензии обладают малыми размерами, рабочей частотой до 3 ГГц, режимом захвата и удержания частоты, возможностью подключения к системе безопасности AR 8000/8200.

Дальнейшее развитие индикаторов электромагнитных полей, имеющих существенные недостатки в поиске закладок получили сканерные приемники и анализаторы спектра. Они имеют существенно лучшую чувствительность, и обеспечивают поиск в диапазоне частот, перекрывающем частоты почти всех применяемых радиозакладок – от десятков кГц до единиц ГГц. Лучшими возможностями по поиску радиозакладок обладают анализаторы спектра**.** Кроме перехвата излучений закладных устройств они позволяют анализировать и их характеристики, что немаловажно при обнаружении радиозакладок, использующих для передачи информации сложные виды сигналов.

Представителями данной группы устройств является серия цифровых анализаторов спектра **Anritsu (MS2663C- MS2663B)**. Они имеют следующие характеристики: диапазон частот 9 кГц – 8,1 ГГц, полоса пропускания 30 Гц – 3 МГц; уровень шума – 130 дБм; динамический диапазон больше 110 дБ; измерение: частоты, отношения мощности несущей к шуму, мощности соседнего канала, мощности шума; оценка занимаемой полосы частот; допусковый контроль; опционально трекинг-генератор; вес 13,5 кг.

Другие представители данных устройств это Анализаторы спектра типа R3465 от компании Advantest имеют следующие характеристики:

- диапазон частот 9 кГц – 8 ГГц;
- средний уровень собственных шумов при фильтре 1 кГц менее –115 во всем диапазоне рабочих частот;
- точка пересечения по интермодуляции третьего порядка +7 дБм;
- точка компрессии на 1 дБ по входу –5 дБм при аттенюаторе 0 дБ;
- разрешение полосы ПЧ от 300 Гц до 3 МГц с кратностью шага 1, 3, 10, плюс фильтр 5 МГц;
- уровень фазовых шумов на частоте 1 ГГц: –100 дБн/Гц на отстройке 10 кГц, –110 дБн/Гц на отстройке 100 кГц;
- неравномерность АЧХ менее ±1.00 дБ до 3 ГГц, менее ±1.50 дБ в диапазоне рабочих частот;
- наличие ЖИГ-фильтра в диапазоне 1,7 ГГц – 8 ГГц;
- ступенчатый аттенюатор 70 дБ с шагом 10 дБ;
- минимальное время развертки во временной области (режим нулевой полосы обзора) 50 мксек;
- наличие АМ и ЧМ демодуляторов;
- цветной дисплей с диагональю 16.25 см;
- наличие выходов 2-ой ПЧ 421,4 МГц и 3-ей ПЧ 21,4 МГц;
- наличие считывателя для карты-памяти флэш-типа, портов для подключения принтера и внешнего монитора;
- внешнее управление по интерфейсу GP-IB, RS-232.

Более совершенными анализаторами спектра на современном этапе являются приборы Rohde & Schwarz FSMS представляющие собой прецизионный анализатор спектра, позволяющие решать задачи исследования сигналов любого уровня сложности, а также, благодаря наличию трекинг-генератора, задачи тестирования четырехполюсников. Данный анализатор спектра имеет следующие характеристики:

- диапазон частот 100 Гц – 26,5 ГГц;
- средний уровень собственных шумов при фильтре 10 Гц менее –140 дБм на частоте 5 ГГц, менее –138 дБм на частоте 20 ГГц, менее –130 дБм на частоте 26,5 ГГц;
- точка пересечения по интермодуляции третьего порядка +15 дБм до 5 ГГц;
- разрешение полосы ПЧ от 6 Гц до 30 кГц и от 80 кГц до 3 МГц с шагом ~10%;
- низкий уровень фазовых шумов: –110 дБн/Гц на частоте 5 ГГц, –104 дБн/Гц на частоте 10 ГГц, –96 дБн/Гц на частоте 26 ГГц (отстройка 10 кГц);
- неравномерность АЧХ менее ±1.00 дБ дот 5 ГГц, менее ±2.50 дБ в диапазоне рабочих частот;
- возможность вывести на экран до3 графиков, возможность наблюдать сигнал в двух раздельных окнах;
- цветной дисплей с разрешением 1024x512;
- встроенный трекинг-генератор с диапазоном частот до 5 ГГц для измерения модуля коэффициента передачи и коэффициента отражения (с внешним направленным ответвителем) четырехполюсников;
- внешнее управление по интерфейсу GP-IB.

Многофункциональный комплекс OSCOR-5000.00. Прибор обнаружения средств негласного съема информации OSC-5000 предназначен для контроля различных каналов утечки информации. Способен в ручном и автоматическом режимах производить поиск и локализацию широкого спектра средств несанкционированного съема информации, таких как радиомикрофоны, телефонные передатчики, передатчики по электросети и проводным линиям, лазерного съема. Микропроцессорное управление позволяет быстро производить анализ полученных в сеансе работы данных, хранить их в памяти прибора и протоколировать их на встроенном плоттере. Новую версию прибора 5.0 отличает высокоскоростной USB-порт для соединения с ПК, более высокая скорость сканирования, дисплей с подсветкой, и улучшенная функциональность. Характеристики OSC-5000*:*

- 24 часовой автоматический и ручной контроль различных каналов утечки информации;
- спектральный анализ диапазона от 10кГц до 3ГГц (до 21ГГц с конвертером MDC-2100);
- сохранение в памяти прибора графических образов спектральных полос; их обработка и анализ;
- анализ сигнала по типу модуляции;
- быстрая локализация источника тревожного сигнала;
- контроль телефонных линий и проводных коммуникаций напряжением до 250В;
- анализ инфракрасного канала;
- пассивный коррелятор акустических сигналов с программируемыми режимами, позволяющий бесшумно обнаруживать подслушивающие устройства;
- предварительная загрузка параметров эфира (фона) и режим быстрого анализа;

– возможность создания баз данных сигналов с сохранением их параметров (времени обнаружения, типа демодулятора, уровня тревоги);

– программирование полос частот для обследования с различными режимами анализа;

– анализ видеосигналов систем PAL/SECAM/NTSC;

– удаленное управление прибором через модем;

– акустический локатор OTL-5000, позволяющий определять расстояние до активных радиомикрофонов;

– удобное функциональное меню, меняющееся в зависимости от режима работы;

– ленточный плоттер, позволяющий быстро протоколировать результаты работы;

– эргономичный дизайн и компактное размещение в прочном атташе-кейсе всего комплекта оборудования, включая комплект антенн и аксессуаров;

– коммуникационное программное обеспечение OPC-5000 поставляемое вместе с прибором, позволяет работать с OSCORом под управлением персонального компьютера.

Методы поиска с использованием нелинейных локаторов, обнаружителей пустот, металлоискателей и рентгеновских аппаратов. Наиболее распространенным в этой серии приборов является профессиональный нелинейный локатор NR-900 EK Коршун; **данный нелинейный локатор, реализует режим автоматической идентификации электронных объектов поиска на фоне коррозионных помех**.

Прибор применяется для обнаружения и локализации скрытно установленных электронных устройств негласного получения информации независимо от их функционального состояния: включено/выключено/ждущий режим. В процессе работы реализованы следующие принципы:

– специальный алгоритм обработки и представления сигналов, реализованные в приборе, позволяют упростить и повысить эффективность различия электронных устройств на фоне объектов со сложными свойствами.

– режим «ИДЕНТИФИКАЦИЯ» обеспечивает возможность повышения вероятности различения радиоэлектронных устройств и коррозийных полупроводников;

– расширенный диапазон регулировки мощности зондирующего сигнала позволяет точно дозировать энергию излученного сигнала при локализации обнаруженных электронных устройств;

– управление режимами работы прибора осуществляется с помощью пульта;

– индикация служебной информации на антенной системе удобна для визуального восприятия результатов поиска.

Развитием рентгеновских комплексов являются рентгено-телевизионные аппараты «Шмель-ТВ» и «Рона» В них теневое рентгеновское изображение преобразуется в телевизионное, проецируемое на экран удаленного от излучателя телевизионного монитора. Рентгеновский аппарат «Шмель-ТВ» обеспечивает возможность наблюдения объекта как на экране монитора, удаленного до 2 м от рентгеновской установки, так и экране просмотровой приставки комплекса «Шмель-90К». Размер экрана рентгено-телевизионного преобразователя – 360 × 480 мм или 240 × 180 мм. Блок управления комплекса позволяет запоминать до 1000 изображений, проводить контрастирование, увеличение масштаба (девять зон с двукратным увеличением), преобразование негатив/позитив и обеспечивает информационно-техническое сопряжение с ПЭВМ, что позволяет при наличие внешнего компьютера проводить дополнительную обработку изображений, распечатывать их на принтере и создавать базы данных для дальнейшего использования. Переносная рентгено-телевизионная установка «Рона» включает блок управления

и индикации, излучатель и рентгено-телевизионный преобразователь. Общая масса установки - 28 кг. Максимальный разнос блока управления от рентгено-телевизионного преобразователя и излучателя составляет 10 м. Комплекс позволяет получать рентгеновские изображения контролируемых предметов, находящихся за преградой из алюминия толщиной до 40 мм. Режим работы рентгеновского аппарата импульсный с длительностью. Размер рабочего поля преобразователя – 270 × 360 мм, а экрана монитора (диагональ) – 23 см. Разрешающая способность установки позволяет выявлять медные проволочки диаметром 0,25 мм за преградой из алюминия толщиной 1 см. После кратковременного включения рентгеновского излучателя поток излучения образует на рентгено-телевизионном экране преобразователя теневое оптическое изображение контролируемого предмета. Это изображение считывается телевизионной камерой и в цифровом виде записывается в блоке управления и индикации. Затем изображение внутреннего строения предмета выводится на монитор блока. Полученное изображение может быть представлено в позитивном или негативном виде. Возможно изменение контраста наблюдаемого изображения и его электронное масштабирование, которое позволяет увеличивать в 2 раза любую из 9 частей изображения.

В последние годы все большее распространение в передаче аналоговых и цифровых сигналов находят применение оптоволоконные системы. Обладая низкими потерями, оптоволоконная линия связи способна транслировать видеосигналы на расстояния до десятков километров без использования промежуточных усилителей. Как правило, частота передачи видеосигнала через оптоволоконные системы составляет более 10 миллиардов бит/с Одним из преимуществ, отличающих оптоволоконные системы, является абсолютная защищенность оптоволокна от электрических помех, наводок и полное отсутствие излучения во вне. Это объясняется тем, что в оптическом канале связи для передачи информации используется световой сигнал, никак не взаимодействующий с электромагнитными полями, а само оптоволокно является диэлектриком и по своей природе не может никак взаимодействовать с электрическими и магнитными полями. Несмотря на чрезвычайно малый диаметр, оптическое волокно может выпускаться в прочной внешней оболочке, выдерживающей большие механические нагрузки, а также гарантирующей длительную работу в сырых помещениях и агрессивных средах. Некоторые типы оптических кабелей допускают их прокладку непосредственно в земле, что резко удешевляет и ускоряет монтажные работы. Все оптоволоконные системы отличаются повышенным уровнем безопасности, так как передаваемый сигнал не излучается за пределы оптического волокна и к нему невозможно подключиться для несанкционированного перехвата. Излучение наружу при оптоволоконной передаче информации практически отсутствует. Эффективный захват информации возможен только путем непосредственного физического подключения к оптоволоконной линии. Но если ВОСПИ рассматривать как систему в целом, содержащую рабочие станции, интерфейсные карты, серверы, концентраторы и другие сетевые активные устройства, которые сами непосредственно являются источником излучений, то проблема утечки информации становятся актуальной. Наиболее эффективным способом перехвата информации с оптоволоконных кабельных систем является непосредственное подключение к ним. В последнее время создаются специальные дистанционно управляемые роботы, которые способны самостоятельно передвигаться по кабельным канализациям и производить подключение к оптоволоконному кабелю для последующей передачи данных, проходящих в ОКС. Для предотвращения подключения с использова-нием специальной техники, имеются разработки по использованию внутренних силовых металлических конструкций

оптоволоконных кабелей в качестве сигнальных проводов. Это предполагает невозможность подключения к оптоволокну без нарушения целостности силовых конструкций. При нарушении целостности металлических конструкций происходит срабатывание сигнализации в центре контроля за ОКС. Дополнительного оборудования для контроля над охранной системой практически не требуется. Кроме этого предлагается установка анализаторов спектра поступающего сигнала и по характеру смещения определяется как наличия посторонних устройств в канале, так и относительное место их установки.

Правовой базой работ по сертификации информационных технологий являются законы РФ «О сертификации продукции и услуг», «О стандартизации», «Об информатизации и защите информации», «О государственной тайне», «О защите прав потребителей», Указы президента РФ, постановления правительства РФ, а также ряд других подзаконных актов. Национальным органом по сертификации определен Госстандарт РФ. Процедура сертификации безопасности автоматизированных систем, входящая в состав более общей процедуры сертификации качества функционирования АС, должна опираться на государственные стандарты, определяющие систему функциональных показателей, оцениваемых при сертификации, регламентирующие управление проектированием и документирование программного обеспечения. Указом Президента РФ от 30.03.94г. № 614 функции межведомственной комиссии по защите гостайны были временно возложены на Гостехкомиссию при Президенте РФ. В целом же на Гостехкомиссию возложены обязанности по координации, организационно-методическому руководству, лицензированию деятельности предприятий и сертификации продукции в области защиты информации. В соответствии с Постановлением Правительства РФ от 26.06.95г. № 608 «О сертификации средств защиты информации» созданы системы сертификации Гостехкомиссии при Президенте РФ, Министерства обороны РФ, разработаны и введены в действие перечни средств защиты информации, подлежащих обязательной сертификации в этих системах. Центральным органом системы сертификации средств криптографической защиты информации является ФАПСИ.

Литература

1. Доктрина информационной безопасности Российской Федерации. 9 сентября 2000 г. № Пр-1895.

2. Закон РФ от 21 июля 1993 г. N 5485 «О государственной тайне».

3. А.П. Зайцев. Програмно-аппаратные средства обеспечения информационной безопасности. – Томск, 2004.

4. А.А. Хорев. Методы и средства поиска электронных устройств перехвата информации. – Москва, 2008.

5. Журнал «Information Security», № 2, 3, 2011.

УДК 004

КИБЕРВОЙНЫ – УГРОЗА XXI ВЕКА

Созинова Е.Н.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Научный руководитель – к.т.н., доц. Жигулин Г.П.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

«Подавить противника, не вступая в схватку с ним,
есть величайшая мудрость военного искусства»
Сунн Цзы.

Постановка проблемы. В современный период развития общества, происходит переход от индустриального общества к информационному. Информация становится более важным ресурсом, чем материальные и энергетические ресурсы. Предоставляя огромные возможности, информационные технологии несут большую опасность, создавая совершенно новую, мало изученную область для возможных угроз, реализация которых может привести к непредсказуемым и даже катастрофическим последствиям. В современном информационном противоборстве, осуществляемом при подготовке и в ходе ведения боевых действий, все более широко используются новые информационные технологии, что позволяет говорить о его переходе на новую, более высокую стадию информационной войны. «Горячие войны» постепенно вытесняются «холодными». Решающую роль в них играет информационное оружие. XXI век принес такие виды оружия, последствия от которых опасней атомной бомбы. Компьютерные технологии стали реальной силой. Кибервойна становится доминирующей разновидностью информационных войн. В отличие от обычного вооружения, кибероружие несопоставимо дешевле, а по эффективности, зачастую, превосходит его. Совершенствуясь, хакерские атаки превращаются в настоящее кибероружие.

Цель работы. Рассмотреть понятие «кибервойна» и «кибероружие»; проанализировать современное состояние данной проблемы в России и мире; дать прогноз о развитии данной ситуации, используя метод «экспертной оценки».

Базовые положения исследования. Стратегической целью кибервойны – является достижение духовной, политической и экономической власти. Можно выделить два направления развития кибервойн:

– развитие и распространение информационных технологий и информационного оружия в военной области;

– кибервойна, как элемент информационных войн, осуществляется посредством всемирной паутины и ПО.

В цифровую эру геополитика и дипломатия, основанные на границах государств и их защите, переживают серьезные проблемы. Информационно-технологическая революция внесла существенные коррективы в геополитику стран. Новейшая геополитика оперирует Большими пространствами многомерной сопряженности, включая виртуальное пространство Всемирной

Сети (киберпространство) и вооружена информационно-коммуникационными технологиями манипулирования сознанием (подсознанием) человека, позволяющими эффективно вести кибервойны.

Промежуточные результаты. В современном мире от компьютеров зависит многое: давление в нефтепроводах, функционирование энергосистем, движение воздушных судов, работа больниц и экстренных служб. Данные системы функционируют с использованием программного обеспечения и, соответственно, уязвимы для разнообразных атак и вредоносных программ, которые могут привести к катастрофическим последствиям, с нанесением экономического и физического ущерба, сопоставимого с воздействием обычных вооружений. Примеры проявления кибервойн и применения кибероружия: операция «Лунный лабиринт» (1998), операция «Титановый дождь» (2003), операция «Аврора» (2009), GhostNet (2009), Операция «Сад», Система Suter, глобальная система «Эшелон», червь Stuxnet (2010). Одним из самых значимых эпизодов кибервойны последнего времени стала публикация секретных материалов на сайте Wikileaks. Публикация данных материалов поставила под угрозу жизнь многих людей и нанесла существенный ущерб американской дипломатии и имиджу страны в целом. Банковский сектор не стал исключением. В конце лета 2011 в России появилась новый вид киберугрозы – троянец Ice IX, клон знаменитого ZeuS. Данная программа представляет серьезную угрозу для пользователей Интернет-банкинга. Объем компьютерной преступности в банковской отрасли, с развитием различных онлайн-сервисов и информационных технологий, сегодня достигает миллиарда долларов. Подобных примеров бесконечное множество.

Все больше стран мира признают наличие у себя подразделений, которые призваны защищать свое киберпространство и разрабатывать кибероружие. Многие государства включают аспекты кибервойны в свои доктрины национальной безопасности и создают специализированные подразделения по ведению кибервойн. Летом 2011 года Президент США подписал указ четко регламентирующий поведение американских военных при ведении кибератак. Международные организации при участии России и США ведут работу над созданием конвенции по ведению кибервойны.

Практические результаты. В данной работе определены цели и задачи кибервойн; определены направления их развития; приведены примеры использования кибероружия; обозначена актуальность проблематики; охарактеризована геополитическая проблема; обозначены угрозы информационной безопасности государства, организаций и структур (в том числе банковских и кредитно-финансовых). На основании анализа современного состояния данной проблемы – выделены основные моменты и даны рекомендации. Используя метод «экспертной оценки» сделан прогноз и сформулированы выводы.

Основной результат. Анализируя данную проблему, можно выделить основные моменты:

1) Рекомендации: предоставить военным и федеральным ведомствам соответствующие инструменты защиты их онлайновых систем; реорганизовать Интернет – ввести стандарты и лицензирование; четко проработать алгоритм действий и принять соответствующие законы; определить механизм классификации киберугроз по видам и степени важности; разработать четкие регламенты и определить зоны ответственности для сотрудников.

2) Кредитно-финансовым или банковским организациям для снижения рисков киберугроз можно посоветовать практиковать использование «временной виртуальной кредитной карты» с виртуальным счетом, которая делает покупки в интернете более безопасными.

3) Защита от кибератак и во время кибервойны – должна быть комплексной. Комплексность должна состоять из совокупности организационных, технических, программных и правовых мер.

4) Используя метод «экспертной оценки» можно спрогнозировать:

- велика вероятность кибератак, направленных на дестабилизацию финансовых рынков;
- в ближайшем будущем кибервойны будут следовать в фарватере традиционных конфликтов и являться их составной частью;
- велика вероятность того, что правительства будут использовать кибератаки как часть военной стратегии;
- кибервойна, в которой будут использоваться только компьютеры – маловероятна;
- наибольший эффект от кибератак достигается благодаря ошибкам персонала;
- рисуемая СМИ картина кибервойн будет существенно отличаться от действительности;
- наибольший вред может нанести организованная кибератака или же кибератака в совокупности с происшествием другого рода;
- проведение кибердиверсии в мирное время – маловероятно;
- страны, наиболее уязвимые для кибервторжения: США, Китай, Россия, Индия;
- с каждым годом количество зафиксированных случаев применения кибероружия и ведения кибервойны возрастает;
- для решения основных проблем, связанных с применением кибероружия – требуются не военные методы, а сотрудничество между правительством и частным сектором.

УДК 004.4

ПОСТРОЕНИЕ СИСТЕМ ПРЕДОТВРАЩЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ И ОБРАЗОВАНИЯ ДОКАЗАТЕЛЬНОЙ БАЗЫ ПРИ ИХ СОВЕРШЕНИИ

Федоров И.С.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Научный руководитель – к.т.н., доц. Жигулин Г.П.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В настоящее время огромное внимание в организациях уделяется вопросам информационной безопасности. Внедряются межсетевые экраны, средства антивирусной и антиспам защиты и многое другое. В основном все эти средства направлены на противодействие внешнему нарушителю, при этом нисколько не защищая от нарушителя внутреннего.

Стоит отметить, что на текущий момент защита от внутреннего нарушителя является одним из наиболее приоритетных направлений обеспечения ИБ организации.

Основные факты

– Внутренний нарушитель представляет собой легитимного сотрудника организации, который обладает определенными правами на доступ к информационным ресурсам. Вследствие умышленных или ошибочных действий внутренний нарушитель может принести ущерб организации.

– Внутренний нарушитель представляет собой легитимного сотрудника организации, который обладает определенными правами на доступ к информационным ресурсам. Вследствие умышленных или ошибочных действий внутренний нарушитель может принести ущерб организации.

– Все нарушения политики безопасности происходят вследствие недостаточного контроля за повседневной деятельностью пользователей.

– Сетевые системы обнаружения вторжений малоэффективны для обнаружения внутренних нарушений.

Возможные действия внутреннего нарушителя

– умышленные действия, связанные с работой вне рамок основной деятельности;

– умышленные действия, связанные с доступом к внутренней информации вне рамок основной деятельности;

– умышленные действия, связанные с попытками изменения информационного наполнения системы;

– неумышленные действия, связанные с недостаточным уровнем квалификации пользователя;

– умышленные действия, направленные на деструкцию системы.

Инструментальные средства

Для облегчения жизни администратора информационной безопасности существует ряд систем, позволяющих в автоматическом режиме следить и реагировать на действия пользователей. В политике безопасности организации должен быть закреплен принцип регистрации всех действий с конфиденциальной информацией, в т.ч. и в электронной форме. Именно записи в журналах регистрации позволяют определить круг лиц, через которых могла произойти утечка, и при успешном расследовании инцидента привлечь к ответственности нарушителя.

Различные системы фиксируют ряд действий пользователя и заносят их в журнал, но могут быть случаи, когда нарушение безопасности происходит по причине, не предусмотренной системой регистрации действия. Такой случай не будет явно зафиксирован в журнале и его обнаружение будет затруднено.

Для предотвращения такой ситуации необходимо дублировать систему регистрирующую абсолютно все действия пользователя (в том числе не предусмотренные службой безопасности). Наиболее удобной в использовании является система регистрации видео изображения на экране пользователя. Такая система наглядно покажет, что делал каждый сотрудник в определенные моменты времени.

Существующие на данный момент системы, реализующие этот принцип, имеют ряд недостатков:

– ведется запись отдельно взятых изображений, а не видео потока;

– данные передаются серверу, но в случаи разрыва сети работа компьютера не блокируется и сбор данных о действии сотрудника прекращается;

– программное обеспечение распространяется с закрытым кодом и может содержать угрозу для организации;

– отсутствие кроссплатформенности;

– при всех недостатках цена на данное программное обеспечение высока.

После устранения перечисленных недостатков с использованием данных, представляемых системой, у администраторов и руководства организации появляются неоспоримые доказательства несанкционированной деятельности пользователей, и только с использованием вышеупомянутых мер возможно оперативное исправление возникших проблем.

Литература

1. Жигулин Г.П., Николаев С.В., Яковлев А.Д. Теория и практика информационного противоборства и прогнозирования информационных угроз. – СПб : СПб ГУ ИТМО, 2008. – 286 с.

2. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М. : ДМК Пресс, 2008. – 544 с.

3. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

ИНФОРМАЦИОННАЯ ПОЛИТИКА РОССИЙСКОЙ ФЕДЕРАЦИИ И ПРОБЛЕМЫ ЕЕ РЕАЛИЗАЦИИ В НАЧАЛЕ XXI ВЕКА

Цепелев С.Д.

Современная Россия находится в состоянии активной трансформации и модернизации. Вслед за США, Японией и западноевропейскими странами, наша страна начинает движение в сторону новой формы цивилизации – информационного общества. Этот процесс сопровождается изменениями практически во всех сферах – социально-экономической, политической, культурной, и, хотя сами изменения являются очень многоплановыми и не всегда однозначными, общий вектор развития России неизбежен и очевиден. Сейчас уже ни у кого не остается сомнений в определяющей роли информационных технологий и процессов для формирования будущего как отдельных стран и регионов, так и человечества в целом.

Актуальность темы данной работы обусловлена рядом факторов:

– все возрастающие потребности общества в информационной сфере предъявляют новые требования к государственной информационной политике – как количественные, так и качественные;

– никогда еще не стоял так остро, как сейчас вопрос о защите общества от деструктивного информационно-психологического воздействия средств массовой информации и определенных сил, использующих СМИ (в т.ч. Интернет) в целях распространения информации экстремистского или иного содержания, оказывающей разрушительное действие на личность;

– формирование в России единого информационно-коммуникационного пространства является обязательным условием для сохранения социальной и политической стабильности и обеспечения территориальной целостности государства;

– формирование и поддержание позитивного имиджа современной России в мире невозможно без проведения качественной и эффективной государственной информационной политики.

Информационная политика государства не может существовать сама по себе, в отрыве от социальных, экономических, политических и культурных реалий. В связи с этим необходимо заметить, что проведение эффективной государственной информационной политики невозможно вне основного русла развития общества и государства, без определения ее содержания и без существования каналов обратной связи между ее объектами и субъектами. Не менее важным требованием к государственной информационной политике является ее комплексность и системность. Всего этого нельзя добиться без четкого взаимодействия и сотрудничества органов государственной власти всех уровней в области формирования и реализации информационной политики.

Содержание понятия государственной информационной политики, ее цели и задачи

Согласно Концепции государственной информационной политики России, государственная информационная политика представляет собой совокупность целей, отражающих национальные интересы России в информационной сфере, стратегических направлений их достижения (задач) и систему мер их реализующих.

Государственная информационная политика – комплекс политических, правовых, экономических, социально-культурных и организационных мероприятий государства, направленный на обеспечение конституционного права граждан на доступ к информации.

Также можно определить государственную информационную политику как особую сферу жизнедеятельности людей, связанную с воспроизводством и распространением информации, удовлетворяющей интересы государства и гражданского общества, и направленную на обеспечение творческого, конструктивного диалога между ними и их представителями.

На основе интересов РФ в информационной сфере, указанных в доктрине информационной безопасности выделим следующие цели и задачи государственной информационной политики:

– соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны;

– информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам;

– развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на

мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов;

– защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

В этих целях необходимо:

– обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, на защиту своей чести и своего доброго имени;

– развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации;

– усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала Российской Федерации;

– укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;

– гарантировать свободу массовой информации и запрет цензуры, укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;

– не допускать пропаганду и агитацию, способствующую разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;

– интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования;

– развивать производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, аппаратных и программных средств защиты информации, расширять участие России в международной кооперации производителей этих средств и систем;

– обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи;

– обеспечить защиту сведений, составляющих государственную тайну;

– расширять международное сотрудничество Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

Одной из важнейших социально-политических предпосылок перехода к информационному обществу представляется достижение баланса интересов граждан, организаций и государства в информационной сфере. Именно поэтому совершенствование информационного права должно стать локомотивом демократического развития России. При этом следует исходить из принципа безусловного правового равенства всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса. Должен быть обеспечен доступ к мировым информационным ресурсам, глобальным информационным сетям.

Проблемы реализации информационной политики

Государственную информационную политику следует рассматривать через призму перехода России к информационному обществу. В этом плане приоритетные направления и задачи государственной информационной политики выступают как актуальные проблемы построения в нашей стране информационного общества.

Можно выделить три класса этих проблем.

1) Проблемы развития технологического базиса информационного общества и перехода к нему. Главное здесь состоит в обеспечении адекватного социально-экономической ситуации уровня функционирования и развития следующих основных составляющих этого базиса:

– национальных информационных ресурсов - баз и банков данных, всех видов архивов, системы депозитариев государственных информационных ресурсов, библиотек и музейных хранений и пр. и обеспечения широкого свободного доступа к ним;
– информационно-коммуникационной инфраструктуры - территориально распределенных государственных и корпоративных компьютерных сетей, телекоммуникационных сетей и систем специального назначения и общего пользования, линий связи, сетей и каналов передачи данных, средств коммутации и управления информационными потоками, а также организационных структур и правовых механизмов, обеспечивающих ее эффективное функционирование;
– информационных, компьютерных и телекоммуникационных технологий - базовых, прикладных и обеспечивающих, систем и средств их реализации, сетевых технологий обеспечения доступа к информации;
– производства и потребления информационных продуктов и услуг для органов власти и управления всех уровней, субъектов экономической деятельности и населения;
– научно-производственного потенциала информатизации, телекоммуникаций и связи - организаций и предприятий фундаментальной и прикладной науки в областях информатики, вычислительной техники, телекоммуникаций и связи, конструкторско-технологической и производственной баз их развития, в том числе оборонного назначения;
– рынка информационных технологий, средств вычислительной техники, телекоммуникаций, связи, информационных продуктов и услуг;
– технологий, структур и механизмов функционирования и развития электронных СМИ.

2) Россия должна строить свою стратегию перехода к информационному обществу в тесном взаимодействии с другими странами. Здесь на первый план выходит проблема обеспечения национальной безопасности, защиты общества и граждан от угроз, связанных с возможностью применения новых информационных технологий в качестве оружия и распространением компьютерных преступлений.

3) Проблемы, определяющиеся социально-экономическими и социально-культурными предпосылками перехода сегодняшней России к информационному обществу.

Успешность продвижения к информационному обществу находится в прямой зависимости от информационной подготовки общества. В обществе доминирует недооценка роли информации в экономике, информация недостаточно востребуется аппаратом управления, отсутствует регулярное информирование населения органами государственной власти и управления о своей деятельности. Совершенно недостаточна компьютерная грамотность населения. Значительна

роль негативных факторов в экономике и демократизации общественной жизни, определяемая традициями и стереотипами общественного сознания и поведения.

Большой остротой отличаются региональные проблемы информатизации. Информационные системы в разных городах и регионах, базы данных государственного значения, например, земельный кадастр, создаются по разной идеологии. Необходимо учитывать реальную неравномерность процессов информатизации по регионам страны.

То, что в России регионы просто чудовищно отстают от мегаполисов в развитии информационно-коммуникационных технологий известно. Но надо также понимать, что это представляет собой не только гуманистическую проблему неравномерного доступа людей к информационным благам. Проблема гораздо глубже, так как в рамках отдельного государства (особенно такого, как Россия) – это разрыв между целыми слоями общества в культурном, экономическом, политическом и других аспектах. Невозможно построить информационное общество, пока значительная масса людей ограничена в доступе к информационно-коммуникационным технологиям. Существенное выравнивание потенциала информатизации по регионам страны потребует значительного времени и серьезных изменений в социально-экономической политике федерального центра.

Пути преодоления проблем и противоречий формирования и реализации государственной информационной политики

Проблемы технологического базиса в рыночной экономике, как правило, решаются независимо от усилий, предпринимаемых государством. Однако в большей степени успешность их решения обусловлена политической стабильностью и макроэкономическими подходами и решениями по выходу страны из сегодняшнего социально-экономического кризиса. Поэтому должна быть усилена роль государственного регулирования развития информационно-телекоммуникационной инфраструктуры, информационных технологий и системы производства информационных продуктов и услуг.

В первую очередь должны осуществляться:

– бюджетное финансирование социально значимых информационных систем (образования, трудоустройства, социального обеспечения и т.п.), а также систем налоговой и таможенных служб, информационного обеспечения госорганов, выборов, правопорядка, ликвидации последствий чрезвычайных ситуаций;

– государственная поддержка приоритетных информационных, компьютерных и телекоммуникационных технологий, открытое конкурсное размещение госзаказов на новые технологии при гарантиях госзакупок и открытый конкурсный отбор технологий при реализации государственных проектов информатизации;

– бюджетная поддержка перспективных научных исследований, в первую очередь национальных научных школ, в области создания отечественных информационных и телекоммуникационных технологий и стимулирование их разработки, производства и использования (разумеется, при их конкурентоспособности) в различных финансируемых из бюджета проектах и программах информатизации государственных объектов;

– государственная поддержка продвижения отечественных информационных и программных продуктов и технических средств информатизации на мировой рынок;

– разработка на государственном уровне программы массовой домашней компьютеризации.

Должна быть создана единая система обеспечения информационной безопасности, которой необходимо эффективно управлять. Сегодня в стране имеется конгломерат отдельных ведомственных систем, решающих отдельные задачи защиты информации в системах и сетях только в пределах своей компетенции и в своих ведомственных интересах. Необходимы согласование усилий всех подсистем и координация их деятельности.

Поддержание необходимого уровня информационной безопасности требует постоянного отслеживания политических, социальных, экономических, научно-технических и других изменений как за рубежом, так и внутри страны. Эти изменения могут порождать новые информационные угрозы. Система должна быстро реагировать на эти изменения и перманентно проверять возможности отражения реальных или потенциальных угроз.

Международное информационное сотрудничество должно быть переведено на новый уровень, ориентировано на разработку и принятие правовых положений и международных соглашений, обеспечивающих информационную безопасность. Необходимо активное участие России в создании межгосударственного законодательства и международных стандартов в области информационной безопасности.

Следует проводить международные переговоры по проблемам обеспечения безопасности в информационной сфере. В частности, должны быть достигнуты соглашения между возможно большим числом стран о координации деятельности в сфере борьбы с информационным терроризмом и информационным криминалом, по предотвращению этих угроз и согласовании действий по минимизации их последствий.

В последние годы ни одно Обращение Президента к Федеральному Собранию не обходится без упоминания о необходимости развития в России информационного общества, внедрения новейших информационных технологий и коммуникационных систем во все сферы жизни общества. Дополняется и укрепляется нормативно-правовая база в области информации и информатизации. Это значит, что власть понимает всю важность процессов, протекающих в информационной сфере, и готова поддерживать и развивать их в соответствии с интересами общества путем проведения эффективной государственной информационной политики.

Литература

1. Конституция РФ.
2. Концепция государственной информационной политики Российской Федерации.
3. Концепция формирования информационного общества в России.
4. Доктрина информационной безопасности Российской Федерации.
5. Игнатьев В.И., Розанов Ф.И. Россия в информационной цивилизации: проблемы вхождения и национальная специфика. // Социальная онтология России. Новосибирский государственный технический университет. – Новосибирск, 2008.
6. Информационная политика: Учебник/ Под общ. ред. В.Д.Попова. – М.: Изд-во РАГС, 2003.
7. http://www.infwar.ru/ Гриняев С.Н. Информационная политика: история, день сегодняшний и перспективы.

УДК 004.056.5

СПОСОБЫ ПРОНИКНОВЕНИЯ ВРЕДОНОСНЫХ ПРОГРАММ

Шибаева Т.А.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Научный руководитель – д.т.н., проф. Щеглов А.Ю.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Компьютерный вирус, троянская программа, червь, хакерские утилиты и другие вредоносные программы являются одной из главных угроз информационной безопасности. По данным ежеквартального отчета компании PandaLabs о вирусной активности за второй квартал 2011 года с апреля по май месяц этого года различные виды вредоносного программного обеспечения в значительной мере получили распространение: каждую минуту создается 42 новых образца угроз. Троянские программы в очередной раз стали самой опасной угрозой, составив почти 70% от всех новых вредоносных программ. Далее следуют классические вирусы (16%) и черви (11,6%).[2]

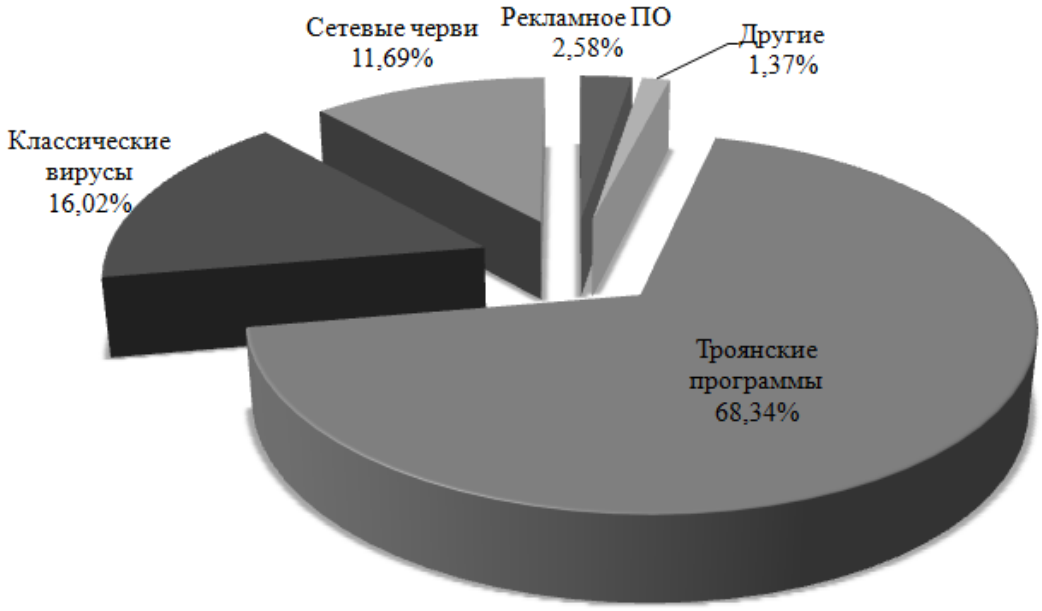


Рисунок 1. Статистика новых вредоносных программ, обнаруженных компанией PandaLabs

При этом среди вредоносного программного обеспечения растет количество рекламного, в том числе количество поддельных антивирусных программ. Рекламное ПО (adware), которое составило лишь 1,37% от всего обнаруженного вредоносного ПО, уже привело к 9% заражений. [3]

Как видно из графика на рис. 2 образцы, вошедшие в первую десятку, стали причиной более 50% всех случаев заражения. Вы можете посчитать, что это заблуждения, поскольку многие угрозы, входящие в первую десятку, являются представителями так называемого «generic malware», которые были обнаружены при помощи технологии Коллективного Разума [4].

Рисунок 2. Статистика по конкретным представителям различных семейств вредоносного ПО

Рисунок 3. Пути проникновения вредоносных программ в систему

Прежде чем пытаться защититься от вредоносных программ, следует определить каким способом происходит их внедрение в компьютер-жертву. Данную цель можно достигнуть различными способами, которые поделим на две основные категории:

- социальная инженерия;
- технические приемы.

В отчете по угрозам “2011 Data Breach Investigation Report” была представлена статистика по способам внедрения вредоносных программ. 80% всех угроз составляют инсталляция/внедрение при помощи удаленного доступа.

Если говорить о социальной инженерии, то ее позиции ослабевают, по сравнению с прошлым годом уменьшились на 17%:.

Таблица 1. Способы внедрения вредоносных программ

Доля угрозы	Вид нарушения	Изменения
9%	Внедрение вредоносных программ	+ 11%
7%	Атаки на повышение привилегий	– 31%
1%	Использование социальной инженерии	– 17%

Каналами распространения вредоносных программ могут быть: внешние накопители (дискеты, флешки), электронная почта, системы обмена мгновенными сообщениями, веб-страницы, интернет и локальные сети.

Первым самым распространенным каналом заражения еще в 1980–1990 годах были дискеты. Сейчас практически отсутствует данный канал из-за появления более эффективных и отсутствия флоппи-дисководов в комплектации многих современных компьютерах.

USB-накопители заменили дискеты и теперь повторяют их судьбу – большое количество вредоносных программ распространяется через съемные накопители, в том числе цифровые фотоаппараты, цифровые видеокамеры, цифровые плееры (MP3-плееры), сотовые телефоны, в которых есть как встроенная память, так и всевозможные карты памяти. По данным лаборатории PandaLabs в 2010 году 25% всех новых вирусов было разработано специально для распространения через USB-устройства [2]. Использование данного канала обусловлено возможностью создания на накопителе специального файла autorun.inf, в котором можно указать программу, запускаемую Проводником Windows при открытии накопителя. В последней версии Windows 7 возможность автозапуска файлов с переносных носителей была отключена по умолчанию. Внешние накопители являются основным источником заражения компьютеров, которые не имеют подключений к Интернету.

Так же распространена рассылка через программы мгновенного обмена сообщениями (например, ICQ) ссылок на фото, музыку либо программы, которые в действительности являются вредоносными программами.

В марте текущего года, чтобы заманить пользователей на зараженный сайт, распространяющий подложные антивирусы, злоумышленники использовали звонки в Skype. Подбирались имена учетных записей пользователей, у которых в настройках Skype не была установлена политика, позволяющая принимать звонки только от лиц из списка контактов. Им звонили незнакомцы от имени “Online report notice”, “System service” или каким-либо подобным. В случае если пользователь принимал звонок, то робот извещал его о том, что система подверглась опасности, в связи с этим необходимо посетить некий сайт. На нем пользователю демонстрировалась проверка системы. Естественно в системе находились уязвимости или вредоносные программы. Чтобы устранить данные ошибки или излечить от вредоносных программ, потенциальной жертве предлагалось купить антивирусное ПО, которое на самом деле лишь имитировало защиту и являлось «лжеантивирусом».

Возможно также заражение через страницы всемирной паутины ввиду наличия на них различного «активного» содержимого: скриптов, ActiveX-компонентов. В таком случае используются уязвимости программного обеспечения, установленного на компьютере-жертве, либо уязвимости в ПО владельца сайта. Последний вариант является наиболее опасным, так как заражению подвергаются добропорядочные сайты с большим потоком посетителей, при этом ничего не подозревающие пользователи зайдя на такой сайт рискуют заразить свой компьютер.

Во втором квартале 2011 года в десяти странах мира было сконцентрировано 87% веб-ресурсов, используемых для распространения вредоносных программ (на 2% меньше, чем в прошлом квартале). Для определения географического источника атаки использовалась методика сопоставления доменного имени с реальным IP-адресом, на котором размещен домен, и установление географического местоположения IP-адреса (GEOIP) [5].

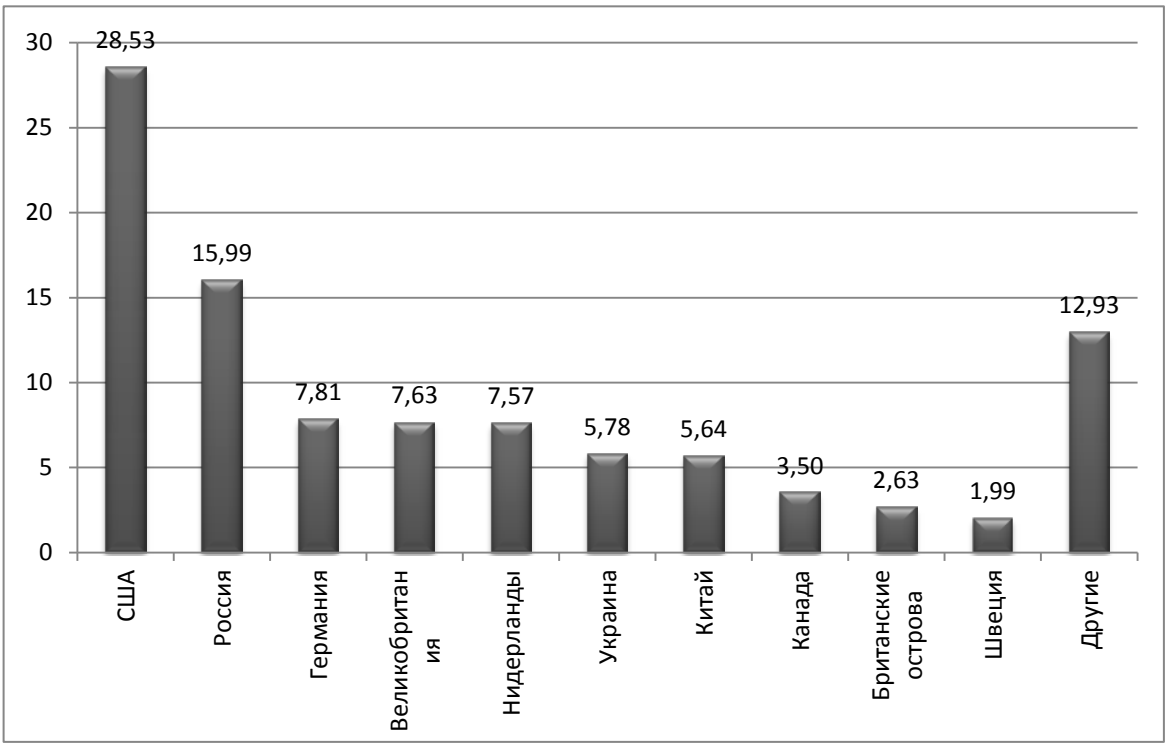


Рисунок 4. Уровень заражения вредоносным ПО в каждой стране

Развитие законодательства и успехи в борьбе с киберпреступниками в США и странах Западной Европы могут привести к постепенному перемещению хостингов, используемых для распространения вредоносных программ, из развитых стран в развивающиеся. Лидируют по уменьшению количества хостингов с вредоносным кодом Нидерланды, чья доля по сравнению с прошлым месяцем уменьшилась на 4,3% и составила 7,8%. Активные действия нидерландской полиции, в том числе по нейтрализации ботнетов (Bredolab, Rustock), отпугивают киберпреступников. [5]

Сетевые черви – вид вредоносного ПО, которые проникают на компьютер-жертву без участия пользователя. Для проникновения на удаленные компьютеры и запуска своей копии черви используют различные методы: социальная инжинерия (например, текст электронного письма, призывающий открыть вложенный файл), недочеты в конфигурации сети (например, копирование на диск, открытый на полный доступ), ошибки в службах безопасности операционных систем и приложений. Также они используют уязвимости в операционных системах и в программном обеспечении (например, Adobe Reader, Internet Explorer, Outlook), чтобы проникнуть на компьютер. Для своего распространения сетевые черви используют и разнообразные компьютерные и мобильные сети: электронную почту, системы обмена мгновенными сообщениями, файлообменные (P2P) и IRC-сети, LAN, сети обмена данными между мобильными устройствами (телефонами, карманными компьютерами) и т. д. Ошибки и недоработки, которые позволяют удаленно загрузить и выполнить машинный код, в результате чего червь попадает в операционную системы и, как правило, начинает действия по заражению других компьютеров через локальную сеть или Интернет. Впоследствии в ряде случаев злоумышленники используют зараженные компьютеры для DDoS-атак или для рассылки спама.

Электронная почта является одним из основных каналов распространения вредоносных программ. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения:

картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться ссылки, если открыть такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу из установленных почтовых клиентов (например, Outlook) для рассылки самого себя дальше.

Создатели вирусов зачастую соединяют в одной вредоносной программе различные способы заражения компьютера и закрепления его в операционной системе. При этом находят новые места для автозагрузки вредоносных программ. На данный момент вирусописатели большей частью используют идеи, которые были известны ранее (не пренебрегают даже просто концепциями) и отчасти уже забытые, и реализуют их.

Как было упомянуто, существует большое количество разновидностей вирусов, различающихся как по способу распространения, так и по функциональности. Если изначально вредоносные программы распространялись на дискетах и других носителях, то сейчас доминирует распространение через Интернет: при помощи веб-страниц, уязвимостей и эксплойтов. На ряду со всем, растет функционал вредоносного ПО: руткиты; бэкдоры (создают «черный ход» в систему), кейлоггеры (регистрация активности пользователей); программы-шпионы (крадут пароли от банковских счетов и номера кредитных карт); ботнеты (превращают зараженные компьютеры в станции по рассылке спама или в часть компьютерных сетей, занимающихся спамом и прочей противоправной активностью).

Исследования показали, что все существующие способы проникновения вредоносных программ приводят к записи (внедрению).

Прежде чем создавать новую вредоносную программу следует вспомнить, что их создание и распространение преследуется в России согласно Уголовному Кодексу РФ (глава 28 «Преступления в сфере компьютерной информации», статья 273 «Создание, использование и распространение вредоносных программ для ЭВМ», до семи лет лишения свободы).

Литература

1. Data Breach Investigation Report. // Аналитика компании Verizon. [Электронный ресурс]. Режим доступа: http://www.verizonbusiness.com/resources/reports/ rp_data-breach-investigations-report-2011_en_xg.pdf, свободный. – Загл. с экрана. – Яз. англ. – 2011.

2. Годовой отчет PandaLabs (2010). // Аналитика компании Panda Security. – Режим доступа: http://www.viruslab.ru/download/wp/wp_reports_2010.pdf, свободный. – Загл. с экрана. – Яз. англ.

3. Ежеквартальный отчет PandaLabs (2 квартал, 2011). // Аналитика компании Panda Security. [Электронный ресурс]. Режим доступа: http://www.viruslab.ru/download/wp/ wp_reports_2011_2.pdf, свободный. – Загл. с экрана. – Яз. англ.

4. Как он работает? // Panda Cloud Antivirus. [Электронный ресурс]. Режим доступа: http://www.cloudantivirus.com/ru/forHome/, свободный. – Загл. с экрана. – Яз. рус.

5. Наместников Ю., Развитие информационных угроз во втором квартале 2011 года. // SecureList «Лаборатория Касперского». [Электронный ресурс]: Режим доступа: http://www.securelist.com/ru/analysis/208050710/Razvitie_informatsionnykh_ugroz_vo_vtorom_kvartale_2011_goda, свободный. – Загл. с экрана. – Яз. рус.

СЕКЦИЯ В. ПУТИ СОВЕРШЕНСТВОВАНИЯ ЭКСПЛУАТАЦИИ ВООРУЖЕНИЯ И ВОЕННОЙ ТЕХНИКИ

УДК 539.2-022.532

КИНЕТИЧЕСКОЕ ОПИСАНИЕ ПРОЦЕССОВ КОАГУЛЯЦИИ, ОПРЕДЕЛЯЮЩИХ ЭФФЕКТИВНОСТЬ СГОРАНИЯ ДИЗЕЛЬНОГО ТОПЛИВА И СНИЖЕНИЕ ВРЕДНЫХ ВЫБРОСОВ В АТМОСФЕРУ

Альфимов А.В., Пантелеев А.В.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Научные руководители: к.ф.-м.н., доц. Чивилихин С.А., капитан 1 ранга, доц. Громов А.В.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Военно-промышленный комплекс во все времена являлся движущей силой научно-технического прогресса. Военная область является доминирующей в политике, проводимой нашим государством, и поэтому ей уделяется особое внимание.

В данной работе предлагается расчет модели процесса коагуляции наночастиц в жидкой среде.

На дизельном топливе, как известно, работает почти вся военная техника. Это бронетранспортеры БТР-80, танки Т-90, комплексы «Искандер-М», «Тополь-М» и многие другие.

В поисках повышения энергетических параметров жидких топлив, ученые обнаружили, что добавление наночастиц алюминия к дизельному топливу повышает его зажигательные свойства.

В простых экспериментах с нагревательным прибором, инженер-механик из Аризонского государственного университета Патрик Е. Фелан с сотрудниками обнаружили, что дизельное топливо, содержащее 0,1% наночастиц алюминия зажигается более легко при низких температурах, чем чистое дизельное топливо. Исследователи подозревают, что добавление наночастиц к дизельному топливу увеличивают испускающие свойства топлива и его способности к тепло- и массопереносу.

Наночастицы увеличивают вероятность того, что одна капля топлива будет возгораться всего лишь около 700°C. Вероятность увеличивается с 15% для чистого дизельного топлива до 50-60%, для обогащенного наночастицами дизельного топлива. Группа Фелана также обратила внимание на разные размеры частиц Al_2O_3 и обнаружила, что 50-нанометровые частицы были немного лучше для разжигания дизельного топлива чем 15-нанометровые частицы, однако эти измерения были проведены только в интервалах низких температур.

Следовательно, добавление наночастиц в топливо увеличивает эффективность его сгорания, одновременно снижается количество выбрасываемых в атмосферу вредных веществ.

Находящиеся в масле наночастицы способствуют увеличению ресурса двигателя: применение таких добавок снижает износ деталей в 1,5-2 раза.

Кинетическая модель коагуляции наночастиц

Пусть $f(t,V)$ – плотность вероятности распределения по объемам. Функция распределения плотности вероятности нормирована на единицу:

$$\int_0^\infty f(t,V)dV = 1 .$$

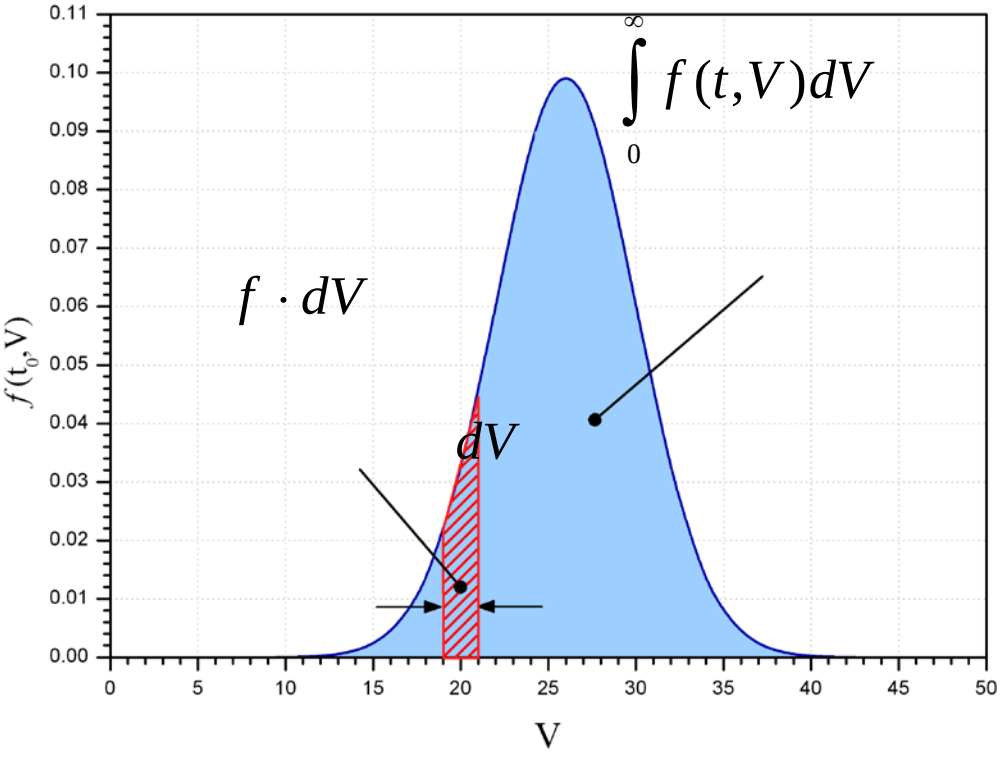


Рисунок 1. Плотность распределения *f*(*t*,*V*) частиц в пространстве их объемов *V* в фиксированный момент времени t_0

Построим модель простейшего процесса коагуляции наночастиц. Полагаем, что частицы в ходе хаотического броуновского движения сближаются с частотой $\nu(t)$ до расстояний, на которых становятся существенными короткодействующие силы притяжения. Будем считать, что, за счет малой исходной концентрации частиц, в системе имеют место только двухчастичные взаимодействия, которые с вероятностью $p(V_1,V_2)$, являющейся функцией размеров взаимодействующих частиц V_1 и V_2, слипаются в новую частицу (агломерат) суммарного объема $V = V_1 + V_2$. Процессами разрушения частиц пренебрегаем.

Для описанной системы эволюция плотности распределения частиц по объемам описывается с помощью кинетического уравнения:

$$\frac{\partial f(t,V)}{\partial t} = \nu(t) \cdot \left[\int_0^V f(t,V') \cdot f(t,V-V') \cdot p(V',V-V') dV' - \right.$$
$$\left. - \int_0^\infty f(t,V') \cdot f(t,V) \cdot p(V',V) dV' \right]. \quad (1)$$

Рассматривая систему на протяжение малого промежутка времени t, полагаем, что частоту их соударений можно считать постоянной:

$$\nu = const. \quad (2)$$

Кроме того, будем считать, что в рассматриваемом промежутке времени частицы любых размеров слипаются с вероятностью, близкой к единице:

$$p = 1. \quad (3)$$

Используя приведенные упрощения, кинетическое уравнение (2) перепишется как:

$$\frac{1}{\nu} \cdot \frac{\partial f(t,V)}{\partial t} = \int_0^V f(t,V') \cdot f(t,V-V') dV' - f(t,V) \int_0^\infty f(t,V') dV'. \quad (4)$$

Для решения интегро-дифференциального уравнения (4) выполним преобразование Фурье обеих частей уравнения по объему V. Для Фурье-образа функции распределения получим следующее уравнение:

$$\frac{1}{\nu} \cdot \frac{\partial \hat{f}(t,\omega)}{\partial t} = \sqrt{2\pi}\, \hat{f}^2(t,\omega) - \hat{f}(t,\omega), \quad (5)$$

где $\hat{f}(t,\omega)$ – преобразование Фурье от функции распределения.

Решая уравнение (5), получаем выражение для Фурье-образа:

$$\hat{f}(\omega,t) = \frac{\hat{f}_0(\omega) \cdot e^{-\nu t}}{1 - (1 - e^{-\nu t}) \cdot \hat{f}_0(\omega)}, \quad (6)$$

где $\hat{f}_0(\omega)$ - Фурье-образ функции распределения в начальный момент времени.

Чтобы избежать процедуры обратного преобразования Фурье, получим основные характеристики распределения из его Фурье-образа.

Найдем выражение для математического ожидания:

$$\frac{\partial}{\partial \omega} \hat{f}(\omega,t) = \frac{\partial}{\partial \omega} \cdot \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} f(V,t) \cdot e^{-iV\omega} dV = \frac{-i}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} f(V,t) \cdot V \cdot e^{-iV\omega} dV,$$

$$\left. \frac{\partial}{\partial \omega} \right|_{\omega=0} \hat{f}(\omega,t) = \frac{-i}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} V \cdot f(V,t) dV = \frac{-i}{\sqrt{2\pi}} \cdot \overline{V}.$$

Таким образом, математическое ожидание можно рассчитать, зная выражения для Фурье-образа искомой функции:

$$M[V]=\overline{V}=i\cdot\sqrt{2\pi}\cdot\frac{\partial}{\partial\omega}\bigg|_{\omega=0}\hat{f}(\omega,t). \tag{7}$$

Аналогично получим выражение для коэффициента дисперсии

$$\frac{\partial^2}{\partial\omega^2}\bigg|_{\omega=0}\hat{f}(\omega,t)=\frac{-1}{\sqrt{2\pi}}\int_{-\infty}^{+\infty}V^2\cdot f(V,t)dV=\frac{1}{\sqrt{2\pi}}\cdot\overline{V^2}(t),$$

$$\overline{V^2}(t)=-\frac{\sqrt{2\pi}}{N}\cdot\frac{\partial^2}{\partial\omega^2}\bigg|_{\omega=0}\hat{f}(\omega,t).$$

Запишем выражение для коэффициента дисперсии:

$$D[V]=\frac{\partial^2}{\partial\omega^2}\bigg|_{\omega=0}\hat{f}(\omega,t)\cdot\sqrt{2\pi}\cdot(\sqrt{2\pi}-1). \tag{8}$$

Используя формулы (7) и (8), определим параметры распределения (6). Для математического объема частицы получим:

$$\overline{V}(t)=\overline{V_0}\cdot e^{\nu t}, \tag{9}$$

а коэффициент дисперсии запишется как:

$$D(t)=e^{\nu t}\cdot\left[D_0+\overline{V_0^2}\cdot(e^{\nu t}-1)\right]. \tag{10}$$

Для удобства анализа полученных выражений введем безразмерное время, нормированное на среднее время между соударениями частиц:

$$\tau=\nu t.$$

На рис. 2 представлены зависимости среднего значения (9) и среднеквадратического отклонения [равного корню из дисперсии (10)] от времени.

Очевидно, что хвост распределения не может зайти в отрицательную зону, следовательно, модель имеет физический смысл только при $\overline{V}\geq 3\sigma$, что, согласно рис. 2, соответствует временам $\tau=0...0.1$.

Предполагая распределение частиц гауссовым, запишем выражение для функции распределения:

$$f(V,\tau)=\frac{1}{\sqrt{2\pi}\cdot\sqrt{e^{\tau}\cdot(D_0+\overline{V_0^2}\cdot(e^{\tau}-1))}}\cdot\exp\left[\frac{-(V-\overline{V_0}\cdot e^{\tau})^2}{2e^{\tau}\cdot(D_0+\overline{V_0^2}\cdot(e^{\tau}-1))}\right]. \tag{11}$$

Эволюция распределения частиц в рамках указанных временных ограничений применимости модели проиллюстрирована на рис. 3.

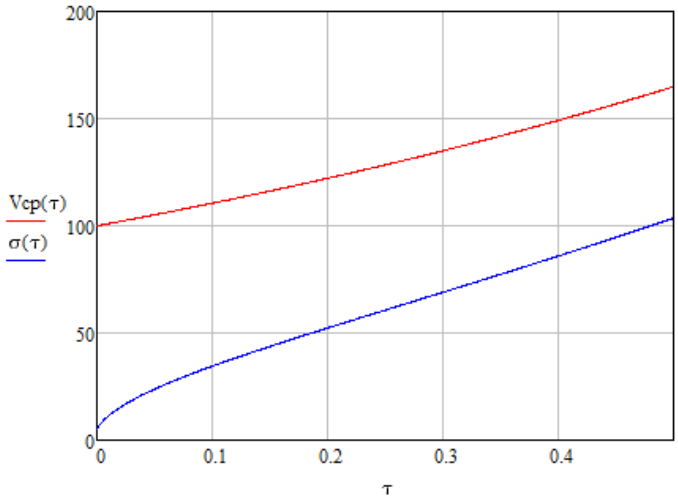


Рисунок 2. Зависимость математического ожидания и среднеквадратического отклонения объема частиц от приведенного времени τ , для начального распределения с $\overline{V}$ = 100 нм; σ_0 = 5 нм

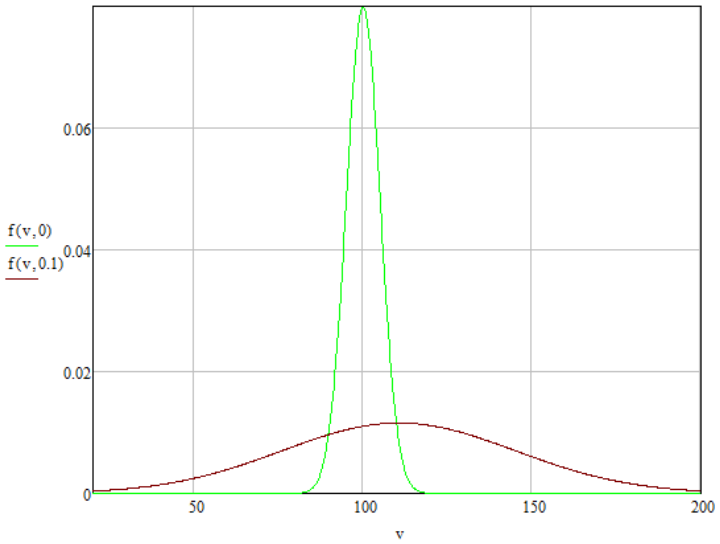


Рисунок 3. Распределения частиц в моменты времени τ =0 и τ =0,1. для начального распределения с $\overline{V}$ = 100 нм; σ_0 = 5 нм

В настоящей работе предложена методика анализа определяемой интегро-дифференциальным кинетическим уравнением функции распределения частиц по размеров, не требующая сложных математических операций, например обратного преобразования Фурье.

На основе полученной методики проанализирована простейшая модель начальной стадии процессов коагуляции наночастиц. Рассмотрение границ применимости предложенной модели показало, что описание системы, основанное на предположении о слипании любых сблизившихся частиц можно использовать крайне ограниченно, лишь на протяжении времен, много меньших среднего времени между столкновениями частиц.

Литература

1. Рудяк В.Я., Белкин А.А., Краснолуцкий С.Л. Теплофизика и аэромеханика. – 2005. – Т.12. – №2. С525-544.

2. Альфимов А.В., Арысланова Е.М., Чивилихин С.А., Попов И.Ю., Гусаров В.В. Компьютерное моделирование процесса формирования нанокластеров методами флуктуационно-диссипативной ланжевеновской динамики // Нанотехнологии функциональных материалов. Труды международной научно-технической конференции 22–24 сентября 2010 г. С. 530, 531.

3. Лифшиц Е.М., Питаевский Л.П. Физическая Кинетика. – М. : «Наука», Главная редакция физико-математической литературы, 1961. – Т. 73. – №3. С. 381–422.

4. Кузнецов А.В. Топливо и смазочные материалы. – «КолосС», 2009. – С. 155–170.

УДК 681.7.06

МЕТОДОЛОГИЯ ВНЕДРЕНИЯ СИСТЕМ КВАНТОВОЙ РАССЫЛКИ КРИПТОГРАФИЧЕСКОГО КЛЮЧА В УЧЕБНЫЕ ВОЕННЫЕ ЦЕНТРЫ ВОЙСКОВОЙ СВЯЗИ

Баймуратов А.С., Глейм А.В., Громов А.В., Медвинский Д.А.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В данной работе мы рассматриваем возможность внедрения в курс обучения военных центров войсковой связи использования установок квантовой рассылки криптографического ключа на примере установки, сделанной на базе кафедры ФиОИ СПбГУ ИТМО. В основе предлагаемой методики лежит разработанный в ходе работы лабораторный практикум, который уже успешно опробируется курсантами последнего года обучения.

Ключевые слова: квантовая криптография, военные коммуникации.

Квантовая криптография – перспективная технология скрытой передачи информации, которая в ближайшем будущем будет использоваться и в военных целях. Основной задачей квантовой криптографии, как и в других системах скрытой передачи данных, является передача скрытого ключа.

На данный момент имеется основательная теоретическая база, и предложено достаточное количество различных протоколов распространения ключа. Текущие исследования, в основном несущие практический характер, можно подразделить на два основных направления: совершенствование технологии и поиск наиболее удачных структурных и схемотехнических решений, обеспечивающих увеличение дальности связи, повышение скорости формирования ключей и снижение влияния дестабилизирующих факторов [1–3]; изучается влияние параметров функциональных узлов на эффективность систем квантовой криптографии и неидеальности характеристик компонентов на условия несанкционированного приема информации [4, 5].

Использование таких технологических решений для рассылки криптографического ключа безусловно требует внимательного подхода, тщательного набора специалистов для эксплуатации и

обучения другого военнослужащих. Обучение персонала потребует специализированных лабораторных центров, снаряженных учебными установками. Одна из предлагаемых систем уже создана на базе кафедры Фотоники и Оптоинформатики Санкт-Петербургского Государственного Университета Информационных Технологий, Механики и Оптики. Данная схема используется в научной деятельности некоторых научно-исследовательских групп и в обучении студентов соответствующих специальностей [6]. На данный момент создаются методические пособия и лабораторный практикум, которые могут лечь в основу учебного материала для использования в обучающих военных центрах. В основе обучения лежит практическая деятельность обучаемых, выполняемая в виде лабораторных работ.

Принцип генерации и квантового распределения ключа

Квантовая криптография является, по всей видимости, единственной ветвью науки о квантовой информации и квантовой связи, реализованной на приборном уровне. Безусловная скрытность ключа, распределенного между легитимными пользователями при помощи квантовых систем, определяется теоремой о запрете клонирования неизвестного квантового состояния. В известных на сегодняшний день квантовых криптографических системах используется кодирование информации в неортогональных состояниях двухуровневых систем, или кубитах, наиболее известными из которых являются протокол на двух (B92) и на четырех состояниях (BB84). Вместе с тем в литературе рассматривается множество других способов реализации скрытых сообщений на основе квантовых состояний, например, протокол на перепутанных состояниях. Однако на практике скрытность квантового распределения ключа (КРК) ограничена рядом факторов: ошибки и потери, возникающие в канале связи при передаче, отличие подготовленных состояний от идеальных, погрешности системы измерения (например, вызванные темновыми отсчетами фотодетекторов) и т. д. Именно перечисленные ошибки в основном ограничивают длину канала связи, в пределах которой гарантирована скрытность квантового распределения ключа.

Квантовая рассылка ключа происходит между отправителем, называемым Алисой (Alice), и получателем, называемым Бобом (Bob). Последовательность битов передается по квантовому каналу.

Описание экспериментальной установки

В данной демонстрационной системе генерация кода осуществляется по протоколу B92, а информационную нагрузку несет фазовое состояние частицы. При этом используются базис: фазовые сдвиги, вносимые модулятором **0** и **π** для логических значений **0** и **1** соответственно. Для кодирования битовой последовательности в данном случае используется несимметричный интерферометр Майкельсона. На основе данного интерферометра построена так называемая самосогласованная установка (англ. Plug&Play), которая несколько сложнее базовой модели на двух интерферометрах Маха-Цендера. Однако она обладает несколькими важными преимуществами:

– интерферирующие импульсы проходят один и тот же путь по линиям связи, что позволяет избежать влияния флуктуаций параметров, вызванных внешними условиями и несовершенством используемого оптического волокна;

– применение Фарадеевских зеркал вместо обычных позволяет избавиться от негативного влияния эффектов двулучепреломления в волокне и избавляет от необходимости постоянного контроля поляризации;

– отсутствует необходимость точной оптической подстройки интерферометров Алисы и Боба. Они могут просто подключиться к существующей оптической линии связи на одномодовом волокне. Необходимо только подстроить время задержки для включения счетчика фотонов.

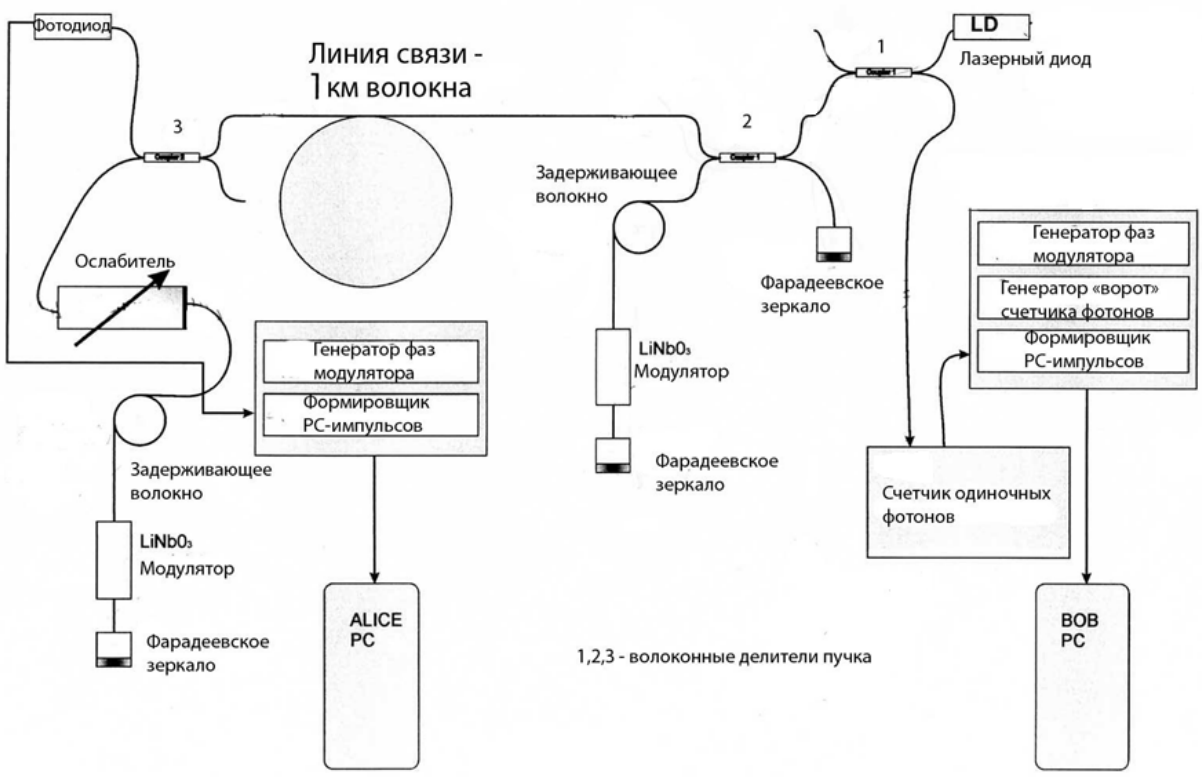


Рисунок 1. Схема Plug&Play системы квантовой криптографии

Рассмотрим ключевые моменты работы этой системы (рис. 1). Лазерный импульс (λ = 1310 нм, τ = 5 нс), излучаемый со стороны Боба, пройдя волоконный светоделитель (1), делится в отношении $1/1$ светоделителем (2). Один из световых импульсов попадает сразу на линию связи и именуется как **Fast**. Другой пучок сначала проходит через линию задержки (задерживающее волокно) и фазовый модулятор, затем отражается от Фарадеевского зеркала и проходит обратный путь к светоделителю, попадает на второе Фарадеевское зеркало, отражается и только после этого выходит на линию связи. Этот луч именуется как **Slow**. Разделенные по времени импульсы Fast и Slow двигаются к Алисе: 90% света через светоделитель Алисы (3) уходит на фотодиод Алисы. Более мощный импульс Fast используется для синхронизации срабатывания модулятора Алисы, а оставшиеся 10% проходят через ослабитель (аттенюатор) и фазовый модулятор Алисы, затем отражаются от Фарадеевского зеркала и двигаются обратно к Бобу.

Прибывшие к Бобу импульсы проходят через делитель (2) с зеркалами Фарадея в обратном порядке и попадают на светоделитель (1). После этого делителя образуются четыре импульса **FastFast, FastSlow, SlowFast** и **SlowSlow**, два из которых **– FastSlow** и **SlowFast –** интерферируют. Необходимо отметить, что фазовый модулятор Боба активен только для импульса **Fast**, уже вернувшегося со стороны Алисы. Разница фаз импульсов **FastSlow** и **SlowFast** может быть равной **0**

или **π**, что соответствует конструктивной или деструктивной интерференции на входе счетчика фотонов на стороне Боба.

Результат интерференции измеряется счетчиком единичных фотонов. Для правильной работы счетчика фотонов необходим точный выбор времени задержки открывания счетчика фотонов. Счетчик должен открываться только на время, в течение которого ожидается приход интерферирующих импульсов. Время открытия счетчика (10 нс, так называемые «ворота») выбрано немного больше длительности импульса (5 нс). Время задержки «ворот» можно менять в двоичном коде с помощью восьми переключателей, расположенных на передней панели блока Боба. Справа расположены младшие разряды, слева старшие. Процесс передачи информации можно описать следующим образом:

– Алиса случайным образом выбирает фазовый сдвиг, но только для импульса **Slow**. Для **Fast** ее фазовый модулятор не активен. В итоге она модулирует импульсы **SlowFast** и **SlowSlow**.

– Боб случайным образом и независимо от Алисы выбирает фазовый сдвиг только для импульсов, возвращающихся от Алисы. В итоге он модулирует импульсы **FastSlow** и **SlowSlow**.

– Боб включает счетчик фотонов на короткий промежуток времени (10 нс), в течение которого ожидается приход интерферирующих импульсов **FastSlow** и **SlowFast**.

– Боб по открытому каналу сообщает Алисе последовательность, полученную от счетчика фотонов. В этой последовательности каждому такту задающего генератора присваивается **0,** если Боб не принял фотон, и **1** в случае принятия фотона. Для каждого такта задающего генератора, для которого был получен отсчет счетчика фотонов, Боб и Алиса формируют «сырой» ключ по правилу: если модулятор абонента стоял в положении **0**, то биту ключа присваивается логический ноль. Для положения модулятора **π**, присваивается логическая единица.

Следует учесть, что из-за низкой квантовой эффективности детектирования единичных фотонов (порядка 10%) и малой средней оптической мощности (меньше одного фотона на импульс в интерферирующих импульсах) средний процент зарегистрированных фотонов в единицу времени значительно меньше числа передаваемых импульсов за тот же промежуток времени. Это приводит к тому, что длина сырого ключа оказывается значительно меньше длины передаваемой последовательности импульсов в течение сеанса связи, но это не дает ошибки в сыром ключе. Ошибки сырого ключа возникают из-за несовершенства оптической схемы (видность интерференции не равна 100%), темновых отсчетов и деятельности потенциального злоумышленника. В данной работе основной вклад в ошибку дают темновые отсчеты. Это приводит к тому, что криптографические сырые ключи Боба и Алисы будут в некоторой степени различаться; ошибка порядка 1,5% считается допустимой.

Данная методика может стать толчком к использованию вышеприведенных схем в военных коммуникациях, а создаваемые методические пособия и лабораторные практикумы могут послужить учебным материалом для самостоятельного изучения механизмов работы установки и для подготовки к самостоятельному контролю ее работы. В дальнейшем обученный персонал сможет самостоятельно работать с установкой и обеспечивать передачу скрытого ключа.

Курсанты кафедры военного обучения проходят стажировку на данных системах по соответсвующим темам. Метод успешно опробируется среди курсантов последнего года обучения. Возможно также создание и других лабораторных практикумов, которые могут охватить

более полно возможности криптографической установки и помогут изучить конкретные проблемы.

Литература

1. Мазуренко Ю.Т., Меролла Ж.-М., Годжебюр Ж.-П. Квантовая передача информации с помощью поднесущей частоты. Применение к квантовой криптографии // Оптика и спектроскопия. – 1999. – Т.86. – №2. – С. 181–183.

2. Risk W.P., Bethune D.S. Quantum cryptography using autocompensating fiber-optic interferometers // Optics & Photonics News. – July 2002. – P. 26–32.

3. Bloch M., McLaughlin S.W., Merolla J.-M. Frequency-coded quantum key distribution // Optics Letters. – 2007. – Vol.32. – №3. – P. 301–303.

4. Bennett C., Bessette F., Brassard G., Salvail L., Smolin J. Experimental quantum cryptography // J. Cryptology. – 1992. – vol.5. – P. 3–28.

5. Румянцев К.Е., Хайров И.Е. Эффективность волоконно-оптической системы передачи информации – Информационное противодействие угрозам терроризма. 2004.

6. Рупасов А.В., Глейм А.В., Егоров В.И., Мазуренко Ю.Т. Согласованная система квантовой рассылки криптографического ключа на поднесущей частоте модулированного света // Научно-технический Вестник СПбГУ ИТМО. – 2011. – С. 95–99.

УДК 681.51

СПОСОБ ПОВЫШЕНИЯ ЗАЩИТЫ УПРАЛЯЕМЫХ ПОДВОДНЫХ СНАРЯДОВ ОТ СРЕДСТВ СОЗДАНИЯ ИСКУССТВЕННЫХ ПОМЕХ

Будкин Н.И.[1], Глотов И.В.[2], Усов А.П.[3]

[1)] *Морской Корпус Петра Великого – Санкт-Петербургский военно-морской институт (филиал) ВУЦЦ «Военно-морская академия»*

[2)] *Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики*

[3)] *Морской Корпус Петра Великого – Санкт-Петербургский военно-морской институт (филиал) ВУЦЦ «Военно-морская академия»*

Ключевые слова: вооружение и военная техника (ВВТ), управляемый подводный снаряд, система самонаведения, ретрансляция акустического сигнала.

В данной статье рассматривается возможность распознавания системой самонаведения (ССН) управляемого подводного снаряда (УПС) средства создания искусственных помех (ССИП) типа имитатора подводной лодки, работающего в режиме ретранслятора.

Развитие и совершенствование самонаводящихся управляемых подводных снарядов (УПС) привело к необходимости создания и развития разнообразных средств создания искусственных помех (ССИП), которые оказывая воздействие на систему самонаведения (ССН) УПС, снижают их эффективность.

Современные ССИП при всем их многообразии могут оказывать воздействие на ССН УПС в виде [1]:

- имитация первичного поля подводной лодки (пл);
- ретрансляции (переизлучении) получаемых от ССН посылок;
- подавление работы ССН путем создания заградительной помехи.

Поскольку на современные УПС устанавливаются активно-пассивные ССН [1], при этом основным режимом работы является активный, весьма актуальной является проблема защиты активных каналов ССН от воздействия средств СИП и, таким образом, повышения их помехозащищенности, что, в с конечном итоге, приводит к повышению эффективности применения управляемых подводных снарядов.

Следует обратить внимание, что характерной особенностью современных пл по сравнению со средствами СИП типа имитатор, представляющие по существу, как правило, точечные объекты, является их значительная протяженность.

Для получения селектирующего признака, позволяющего отличить реальную цель от имитатора пл, целесообразно осуществлять сканирование характеристики направленности (ХН) в горизонтальной плоскости (ГП) либо иметь ХН, состоящую из отдельных лепестков.

Примем, что реальная цель имеет эффективную длину $L_{цэ}$, а имитатор представляет из себя точечный объект. Если аппроксимировать пл цилиндром длиной $L_ц$, и диаметром $B_ц$, то

$$L_{цэ} = L_ц \cdot \sin q_ц + B_ц \cdot q_ц , \tag{1}$$

где $q_ц$ – курсовой угол цели.

Нетрудно видеть, что если угол остроты ХН ССН в режиме излучения в ГП составляет $\lambda_u^г$, то (при угловой скорости сканирования ω_T) время нахождения цели ($t_ц$) и имитатора (t_u) в зоне реагирования аппаратуры будет определяться

$$t_ц = 2 \cdot (\lambda_И^Г \cdot \lambda_Ц^Г) / \omega_T , \tag{2}$$

$$t_И = 2 \cdot \lambda_И^Г / \omega_T , \tag{3}$$

где $2 \cdot \lambda_u^г$ – угловая протяженность цели.

Величина угловой протяженности цели есть

$$2 \cdot \lambda_И^Г \approx arctq(L_Ц \cdot \sin(q_Ц + B_Ц \cdot \cos(q_Ц)) / r , \tag{4}$$

где r – расстояние от УПС до цели.

Если посылка будет состоять из N импульсов, то (при интервале между импульсами T_u) количество сигналов, полученных аппаратурой, соответственно от пл и имитатора определяется как

$$N_Ц = 2 \cdot (\lambda_И^Г \cdot \lambda_Ц^Г) / \omega_T \cdot T_И ; \tag{5}$$

$$N_Ц = 2 \cdot \lambda_И^Г / \omega_T \cdot T_И . \tag{6}$$

Очевидно, что различие в воздействии на ССН реальной цели и имитатора будет

$$\Delta t = t_Ц - t_П = 2\lambda_И^Г / \omega_Т . \quad (7)$$

$$\Delta N = n_Ц - n_И = 2\lambda_И^Г / \omega_Т \cdot T_И . \quad (8)$$

Если принять, что длительность сигнала, получаемого ССН, равна длительности импульса посылки $\tau_И$, то разность в длительности сигнала от пл и имитатора составит

$$\Delta t = \Delta N \cdot \tau_И = 2 \cdot \lambda_И^Г \cdot \tau_И / \omega_Т \cdot T_И . \quad (9)$$

Известно, что длительность отраженного от пл сигнала зависит от ее эффективной длины, курсового угла и зоны реагирования ССН.

При полном облучении пл увеличение длительности эхо-сигнала определяется [3]

$$\Delta\tau_{И1} \approx 2L_Ц \cdot \cos(q_Ц) / C . \quad (10)$$

где C – скорость звука в воде.

При полном облучении пл увеличение длительности эхо-сигнала определяется зоной облучения ССН [3]

$$\Delta\tau_{И2} = 2 \cdot L_a \cdot \cos(q) / C , \quad (11)$$

где $L_a \approx 2r \cdot tq \cdot \lambda_И^Г / \sin(q_Ц)$

После подстановки последнего выражения в формулу (11) получаем

$$\Delta\tau_{И2} = 4 \cdot r \cdot tq \cdot \lambda_И^Г \cdot ctq \cdot q_Ц / C . \quad (12)$$

Таким образом, можно ожидать, что при

$$\lambda_И^Г \geq \lambda_Ц^Г ,\ \Delta t = \Delta N(\tau_И + \Delta\tau_{И1}) . \quad (13)$$

$$\lambda_И^Г < \lambda_Ц^Г ,\ \Delta t = \Delta N(\tau_И + \Delta\tau_{И2}) . \quad (14)$$

Окончательно, после подстановки можно записать

$$\lambda_И^Г \geq_Ц^Г ,\ \Delta t_2 = 2\lambda_Ц^Г(\tau_И + 4 \cdot r \cdot tq \cdot \lambda_Ц^Г \cdot ctq \cdot q_Ц / C) / \omega_Т \cdot T_И . \quad (15)$$

$$\lambda_И^Г < \lambda_Ц^Г ,\ \Delta t_2 = 2\lambda_Ц^Г(\tau_И + 4 \cdot r \cdot tq_И^Г \cdot ctq \cdot q_Ц / C) / \omega_Т \cdot T_И \quad (16)$$

Рассмотрим несколько подробнее воздействие пл и ССИП на ССН учитывая то обстоятельство, что имитатор может ретранслировать посылку аппаратуры с удлинением.

Очевидно, что при $\lambda_И^Г > \lambda_Ц^Г$ длительность сигнала от имитатора, осуществляющего ретрансляцию посылки ССН без удлинения и с удлинением, соответственно, будем иметь

$$t_{И1} = 2 \cdot \lambda_И^Г \cdot \tau_И / \omega_Т \cdot T_И . \quad (17)$$

$$t_{И2} = 2 \cdot \lambda_И^Г \cdot (\tau_И + \Delta\tau_{И1}) / \omega_Т \cdot T_И . \quad (18)$$

Длительность сигнала от пл (как при полном ее облучении, так и при частичном) будет

$$t_{Ц2} = \frac{2 \cdot (\lambda_{И}^{Г} + \lambda_{Ц}^{Г}) \cdot \tau_{И}}{\omega_{Т} \cdot T_{И}} + \frac{2 \cdot (\lambda_{И}^{Г} - \lambda_{Ц}^{Г}) \cdot \Delta\tau_{И1}}{\omega_{Т} \cdot T_{И}} + \frac{4 \cdot \lambda_{И}^{Г} \cdot \Delta\tau_{И1}}{2 \cdot \omega_{Т} \cdot T_{И}}.$$

После преобразования получаем

$$t_{Ц2} = 2 \cdot [\lambda_{Ц}^{Г} \cdot (\tau_{И} - \Delta\tau_{И1}) + \lambda_{И}^{Г} \cdot (\tau_{И} + 2 \cdot \Delta\tau_{И1})] / \omega_{Т} \cdot T_{И}. \quad (19)$$

При полном облучении пл ($\lambda_{И}^{Г} \geq_{Ц}^{Г}$) временное различие в воздействии реальной уели и имитатора на ССН составит:

– имитатор ретранслирует посылки без их удлинения

$$\Delta t_1 = 2 \cdot [\lambda_{Ц}^{Г} \cdot \tau_{И} + (\lambda_{Ц}^{Г} - \lambda_{И}^{Г}) \cdot \Delta\tau_{И1})] / \omega_{Т} \cdot T_{И}; \quad (20)$$

– имитатор ретранслирует посылки с их удлинением ($\lambda_{И}^{Г} < \lambda_{Ц}^{Г}$)

$$\Delta t_2 = 2 \cdot \lambda_{Ц}^{Г} \cdot (\tau_{И} - \Delta\tau_{И1}) / \omega_{Т} \cdot T_{И}. \quad (21)$$

При неполном облучении цели ($\lambda_{И}^{Г} \leq_{Ц}^{Г}$) с учетом преобразований длительность сигнала от пл есть

$$t_{Ц2} = 2 \cdot [(\lambda_{Ц}^{Г} + \lambda_{И}^{Г}) \cdot \tau_{И} + (\lambda_{Ц}^{Г} - \lambda_{И}^{Г}) \cdot \Delta\tau_{И2}] / \omega_{Т} \cdot T_{И}. \quad (22)$$

Окончательно получаем выражение временных различий сигналов от пл и имитатора:

– ретрансляция осуществляется без удлинения посылки

$$\Delta t_1 = 2 \cdot [\lambda_{Ц}^{Г} \cdot (\tau_{И} + \Delta\tau_{И2}) - \lambda_{Ц}^{Г} \cdot \Delta\tau_{И2}] / \omega_{Т} \cdot T_{И}; \quad (23)$$

$$\Delta t_2 = 2 \cdot [\lambda_{Ц}^{Г} \cdot (\tau_{И} + \Delta\tau_{И2}) - 2 \cdot \lambda_{Ц}^{Г} \cdot \Delta\tau_{И2}] / \omega_{Т} \cdot T_{И}. \quad (24)$$

Расчеты по возможности распознавания ССН средств СИП (типа имитатор) были выполнены для цели длиной 100м и шириной 8м.

Для имитатора, осуществляющего «чистую» ретрансляцию сигналов (И-1), анализ формулы (23) и выполненные расчеты показали, что:

– временное различие (величина Δt) при воздействии реальной цели и имитатора на ССН возрастает с уменьшением угловой скорости сканирования ХН и временного интервала между импульсами посылок;

– наибольшее значение величины Δt принимает на курсовых углах 0–45°, когда наблюдается значительный прирост длительности эхо-сигналов;

– с уменьшением дистанции до цели величина Δt увеличивается и возможности ССН по распознаванию ССИП возрастают.

Если принять, что курсовой угол цели распределен по равновероятному закону в интервале 0–180°, то вероятность распознавания ССН имитатора (при выбранном пороге Δt) будет определяться данными, представленными в табл. 1.

Расчеты выполнены для следующих условий: r = 1000м; $T_{И}$ = 0,01с; $\tau_{И}$ = 0,001с; $\lambda_{И}^{Г}$ = 7°.

Таблица 1

Δt,с / $\omega_т$, °/с	1	2	3	4	5	6
3	0,97	0,97	0,96	0,95	0,94	0,93
10	0,96	0,92	0,86	0,81	0,76	0,71
17	0,94	0,87	0,80	0,69	0,60	0,53

Полученные данные свидетельствуют о том, что при дистанции до цели 1000м и пороге срабатывания ССНΔ t = 2–3с при угловой скорости сканированияω $_т$ = 8–17 °/с обеспечивается вероятность распознавания не ниже 0,8.

Таким образом, для повышения возможности распознавания ССН имитатора, работающего в режиме «чистого» регистратора, целесообразно уменьшить угловую скорость сканирования, временной интервал между импульсами и увеличивать длительность импульсов посылки.

Для имитатора, осуществляющего ретрансляцию сигналов с их удлинением (И-II), результаты расчетов вероятности распознавания, выполненные по формуле (24) (для $\tau_И$ = 0,001с; $\lambda_И^г$ = 2,5° представлены в табл. 2.

Таблица 2

$T_И$, с / r,м		0,01			0,08		
Δt,с	$\omega_т$, °/с	200	400	600	200	400	600
0,05	3	0,78	0,59	0,15	0,84	0,61	0,25
0,10		0,78	0,59	0,10	0,83	0,60	0,23
0,50		0,77	0,58	0	0,79	0,51	0
0,05	10	0,78	0,58	0,05	0,83	0,59	0,21
0,10		0,77	0,56	0	0,82	0,54	0
0,50		0,77	0,41	0	0	0	0
0,05	17	0,78	0,58	0	0,82	0,54	0
0,10		0,77	0,57	0	0,48	0,42	0
0,50		0,69	0,19	0	0	0	0

Анализ полученных результатов показывает, что возможности ССН по распознаванию имитатора, осуществляющего ретрансляцию сигналов с их удлинением, весьма ограничены даже на небольших расстояниях, до цели. Для повышения вероятности распознавания ССН имитатора (И-II) целесообразно, в первую очередь, при облучении цели применять более узкую характеристику направленности. Так, для обеспечения распознавания ССН имитатора с вероятностью около 0,8 (при пороге срабатыванияΔ t = 0,005–0,1 с) зона реагирования АСН должна составлять не более 2° на дистанции 600м и не более 5° на дистанции до 200м.

Как указывалось выше, в качестве селектирующего признака можно использовать и различие в воздействии на ССН реальной цели и имитатора, заключающегося в различии получаемых ею отраженных сигналов (ΔN).

Анализ формулы (8) и полученные расчеты показывают, что величина ΔN в существенной степени зависит от угловой протяженности цели и параметров аппаратуры – угловой скорости сканирования ХН и временного интервала между импульсами.

При равновероятном законе распределения курсового угла цели на расстоянии 1000м при $T_И$ = 0,01с, $\tau_И$ = 0,001с и пороге ΔN = 5–6 вероятность распознавания ССН реальной цели составляет около 0,9 (табл. 3).

Таблица 3

Δt,с / $\omega_т$, о/с	1	2	3	4	5	6
3	1	1	1	1	1	1
10	1	1	1	1	1	0,99
17	1	1	1	0,99	0,98	0,96
24	1	1	0,97	0,98	0,91	0,89

При этом имитатор работает, как в режиме И-I, так и в режиме И-II.

Таким образом, как показали проведенные исследовании, наиболее благоприятные условия по распознаванию имитатора пл образуются, если в качестве селектирующего признака принять разницу в качестве импульсов, получаемых ССН, соответственно, от реальной и ложной цели.

При этом предполагается, что классификация цели будет осуществляться после ее обнаружения. В результате этого торпеда будет наводиться либо на реальную цель (пл), либо будет выполнять маневр уклонения, исключающий ее наведение на ложную цель (имитатор).

Литература

1. Алиев Ш.Г и др. Торпедное оружие. – М. : Наука, 2002.
2. Подобрий Г.М. и др. Теоретические основы торпедного оружия. – М. : Воениздат, 1971.
3. Урик Д.А. Основы гидроакустики. – Л. : Судостроение, 1978.
4. Утенин Л.Н. и др. 60 лет разработок торпедного оружия. – СПб : НИИ морской теплотехники, 2008.

УДК 35

ОБОСНОВАНИЕ ПУТЕЙ РЕШЕНИЯ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ЗИП КОМПЛЕКСОВ УДАРНОГО РАКЕТНОГО ОРУЖИЯ

Бычков В.В.[1], Мануйленко В.Г.[2]

[1)] *Санкт-Петербургский Военно-Морской Институт имени Петра Великого*

[2)] *Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики*

Гибкая стратегия управления количеством ЗИП КУРО одно из направлений решение проблемы определения совокупности объемов и сроков их заказа, а также поставок флоту в течение всего периода эксплуатации комплексов РО, использование его на кораблях в процессе технического обслуживания и ремонта КУРО.

Ключевые слова: технический осмотр (ТО), ремонт, запасные инструменты и части (ЗИП), планирование, научно-методический подход, оптимизация, финансирование.

Несмотря на достаточно очевидные преимущества гибких стратегий для технического обслуживания (ТО) и ремонта, с учетом обеспечения запасными частями ракетного комплекса, их непосредственное внедрение затруднено в силу необходимости решения ряда проблем. Эти проблемы условно можно подразделить, на следующие: организационные, технические и научно-методические. Организационные и технические проблемы могут быть решены только после решения научно-методических проблем.

Обоснование путей решения проблемы обеспечения ЗИП комплексов ударного ракетного оружия

Научно-методический подход, который необходимо внедрить в техническое обслуживание и ремонт по состоянию элементов ракетного комплекса (РК), связан с тем, что параметры ТО и ремонта (периодичность и объем), а также вопросы обеспеченности ЗИП должны определяться по результатам решения оптимальных задач. В этой связи необходима разработка методики для оптимизации пороговых значений вероятности работоспособного состояния составных частей комплексов ударного ракетного оружия (СЧ КУРО) по различным уровням, например: ТО в море, ТО в базе, плановый ремонт, а также методики оптимизации пороговых значений обеспечивающего количества запасных инструментов, имущества, приспособлений, приборов в составе одиночного (возимого, невозимого), группового, ремонтного комплектов [2, 3].

Если говорить о материальных затратах, сопровождающих процесс эксплуатации КУРО, и в частности формирования системы технического обслуживания и ремонта немаловажную роль играют и экономические факторы. Считается, что годовые затраты на ремонт и техническое обслуживание будут оправданными, если они за срок службы ракетного комплекса не превысят стоимости его постройки. Большие затраты на ТО являются дополнительными побудительными причинами, заставляющими уделять значимое внимание его организационным формам и методам управления. Значительную долю материальных затрат представляют затраты на комплектацию ЗИП КУРО во время проведения технического обслуживания и ремонта [3].

Однако, существующая система планирования ЗИП, основанная на вероятно-статистических методах расчета их нормативного количества, зачастую оказывается недостаточно экономичной.

В современных условиях ограниченного финансирования и развития Военно-морского флота России, задача поиска путей экономичного планирования обеспечением ЗИП становится весьма актуальной.

Реализация принципов гибкой стратегии технического обслуживания и ремонта, и обеспечения ЗИП, учитывающих текущее и прогнозируемое техническое состояние КУРО, предполагает экономию их ресурса и средств на ТО и ремонта примерно на 30–40%. Однако в этой связи возникает проблема планирования ЗИП, особенно для кораблей, назначенных к длительному плаванию (отрыву от пунктов основного базирования). Так как в длительном плавании осуществлять пополнение ЗИП невозможно, если необходимо производство восстановительных работ, вышедшей из строя системы, или когда техническое состояние не удовлетворяет заданным требованиям [4].

Пути решения названной проблемы видятся в следующих основных направлениях движения развития:

– планирование ЗИП по традиционным методикам с расчетом на наихудший случай (с запасом). Такой подход обеспечит гарантированное количество средств на эксплуатацию, однако, если говорить о реализации гибких принципов технического обслуживания и ремонта, предусматривающих увеличение межрегламентных периодов и сокращение объема профилактик, такой подход к планированию средств будет еще более расточительным, чем при использовании традиционных принципов проведения мероприятий ТОР;

– по возможности создание электронной базы данных на соединениях флотов, накопление статистических данных – интенсивности отказов составных частей комплексов ударного ракетного оружия и формирование обоснованной и целесообразной заявки в довольствующий орган на поставку ЗИП;

– индивидуальное планирование ЗИП каждого КУРО в зависимости от прогнозируемого технического состояния каждого корабля с его ракетным оружием на планируемый период эксплуатации.

Под стратегией управления количеством ЗИП КУРО будем понимать совокупность объемов и сроков их заказа и поставок флоту в течение всего периода эксплуатации комплекса, а также порядка его использования на кораблях в процессе технического обслуживания и ремонта [3].

Рациональная стратегия управления запасами инструмента, имущества и принадлежностей обеспечивается в том случае, когда ее реализация приводит к минимальным энергетическим и материальным расходам, но по выбранному критерию максимальной оптимизации.

При решении задач определения рациональной гибкой стратегии управления ЗИП будем руководствоваться следующим основным единым принципом**:** обеспечить требуемую боеспособность и заданную боеготовность необходимого количества ЗИП при минимальных возможных экономических затратах на изготовление и использование, для выполнения поставленных перед ракетным комплексом задач.

Исходя из сказанного, а также для выполнения приведенного выше основного принципа оптимизации необходимо стремиться к минимизации суммарного количества поставляемого флоту ЗИП при выполнении требуемых дисциплинирующих ограничений, а критерий

оптимизации для определения количественных значений управляемых переменных может быть представлен в виде

$$R_з^{\,P} = \min_{j \in J} [R_з^{\,j}], \qquad (1)$$

где $R_з^{\,P}$ – суммарное количество заказываемого и поставляемого на флот ЗИП за период эксплуатации $T_э$ при рациональной стратегии управления ЗИП;

$R_з^{\,j}$ – суммарное количество заказываемого и поставляемого флоту ЗИП за весь период эксплуатации *Тэ* для реализации *j*-го варианта функции поставок ЗИП;

j – совокупность всех возможных вариантов функций поставок ЗИП.

По результатам прогноза сравнивается потребное количество ЗИП с планируемым на аналогичный период без учета длительного плавания, при этом выбирается рациональный показатель, обеспечивающий максимум технической готовности РК [3].

Исходя из основных положений системного анализа, возможно наметить последовательность решения многовариантной задачи с помощью имитационной модели.

Многовариантность решения задачи заключается в том, что с учетом классификации ЗИП (комплектов или россыпью), необходимо учитывать вопросы прогнозирования его: производства, поставок, хранения, и самой организации обеспечения ЗИП КУРО при проведении ТОР. Учитывая взаимосвязи между требованиями эксплуатации КУРО и требованиями, предъявляемыми к вопросам обеспеченности ЗИП, можем сформировать алгоритм постановки задач, с помощью создания имитационной модели.

Схема системных исследований применительно к обеспеченности ЗИП, прежде всего, должна быть четко поставлена проблема в виде имитационной модели, затем последовательно общая и частная задачи также в форме имитационных моделей. При формализации связей может оказаться, что потребуется провести дополнительные научно-исследовательские работы, а при формализации задачи может потребоваться разработка новых математических методов решения задачи с функционально-параметрическим подходом.

Важными этапами процесса решения задачи являются те, в которых происходит разветвление путей дальнейшего хода решения. К ним могут отнести следующие этапы решения такие, как возможность:

1) решения общей и частной задачи;
2) использования существующих зависимостей;
3) решения задачи существующими математическими зависимостями;
4) разработки новых математических методов;
5) проверки достоверности результатов.

Каждый из этих этапов позволяет идти по нескольким направлениям, каждое из которых получает свое дальнейшее развитие. Получение частичного решения нежелательно, так как нет уверенности, что оно может привести к оптимальному общему решению. Поэтому полученное частичное решение требует проверки.

В случае, если не подтверждается приемлемость полученного решения, в действие вступают обратные связи, которые приводят к разработке дополнительных альтернатив или к уточнению постановки и решению задачи создания имитационной модели обеспечения ЗИП КУРО, см. рис. [1].

Решение задачи обеспеченности ЗИП будем считать приемлемым, если:

– решение определяет действия, которые позволяют изменить параметры системы в нужном направлении исследования с целью достижения требуемого результата;

– решение выражено в терминах постановки задачи или вытекает из этих терминов;

– постановка задачи и найденное решение рассматриваются как составляющие одной системы;

– решение по объему и сложности соизмеримо с решаемой задачей (решение не должно быть более сложным, чем рассматриваемая задача, но должно быть достаточно полным и не содержать противоречий;

– частичное решение согласованно с полным (общим) решением, так как противоречия между частичными решениями, а также между ними и общим решением не позволит установить оптимального решения для всей системы обеспеченности КУРО ЗИП;

– для каждого частичного и общего решения можно, при необходимости проверить их достоверность. В то же время для установления предпочтительности рассматриваемых решений необходимо использовать соответствующие критерии.

В общем виде схема решения любой инженерной или эксплуатационной задачи, в том числе и задачи управления системой обеспечения ЗИП комплексов ударного ракетного оружия с учетом прогнозируемых изменений их технического состояния СЧ КУРО, на базе системного анализа, и как составной части функционально-параметрического подхода, состоит в следующем (рис. 1).

1) Постановка решаемой задачи; установление цели; выявление условий и ограничений при решении и достижении поставленной цели; установление границы исследуемой системы и критерия эффективности состояния системы и ее структурных составляющих; выявление взаимосвязей и их оценка.

2) Анализ решаемой задачи; установление границ структурных составляющих и существующие связи между структурными составляющими; уточнение данных, проверка возможности использования установленных критериев; разработка схемы решения задачи; установление возможных вариантов решения задачи, подлежащих сравнению для выбора оптимального.

3) Решение поставленной задачи: разработка методики решения задачи; установление количественной оценки связей между структурными, функциональными и параметрическими составляющими; оценка частичных и полных решений; принятие решения, подлежащего реализации в системе производства, обеспечения и управления запасами ЗИП [5].

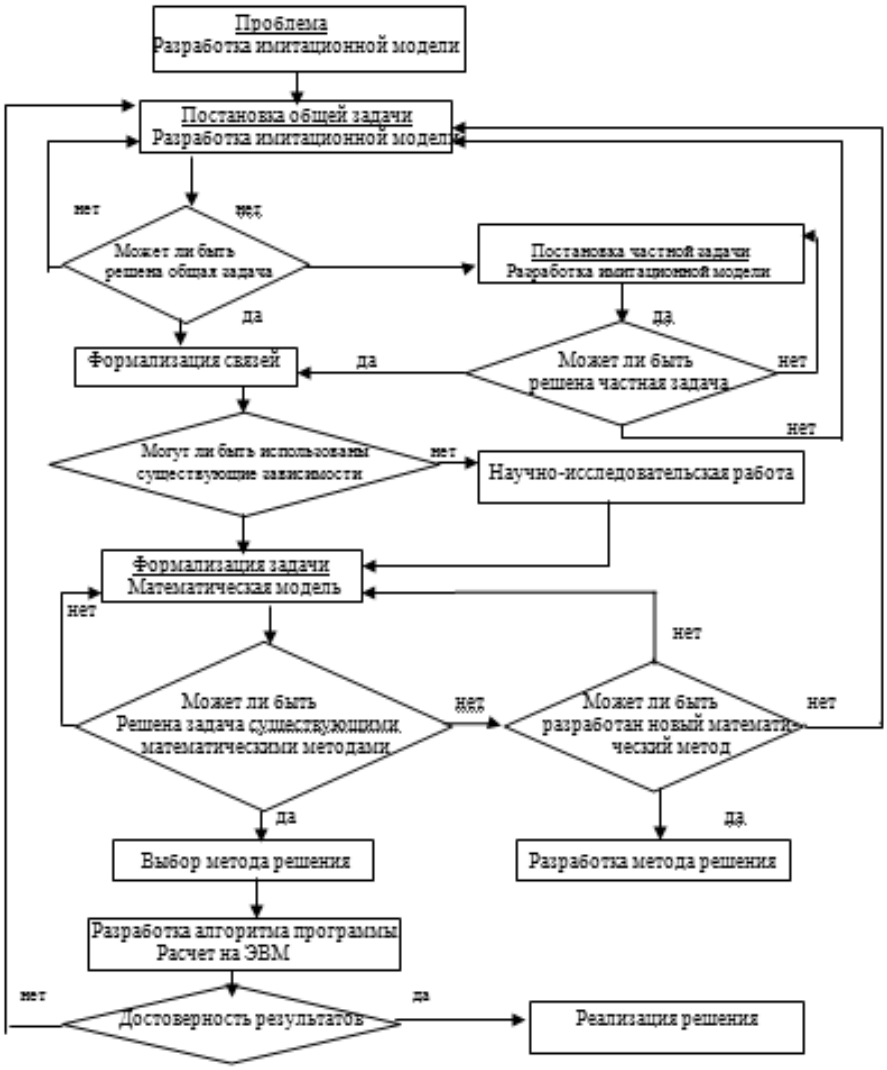


Рисунок 1. Алгоритм разработки имитационной модели обеспеченности ЗИП КУРО

Методы решения задач планирования ТО, ремонта и соответственно поставок и обеспечения ЗИП, зависят от полноты и достоверности исходных данных. В понятии описания входит наличие априорных статических характеристик закономерностей выхода из строя СЧ КУРО, позволяющих учесть влияние управляющих процессов эксплуатации с учетом необходимого количества ЗИП.

С точки зрения приложений наибольший интерес представляют методы, позволяющие получать решения в условиях ограниченности исходных данных.

Предварительные оценки ожидаемого эффекта от введения такой системы планирования ЗИП позволяют надеяться на экономию до 50% средств, выделяемых на эксплуатацию КУРО, что приблизительно на порядок меньше предполагаемых затрат на технические и организационные мероприятия, необходимые для ее практической реализации.

Проведенное обоснование путей решения задачи планирования необходимого количества ЗИП для ТО и ремонта с учетом технического состояния элементов КУРО, позволяет сделать общую формулировку задачи планирования профилактической коррекции, но не дает гарантии в

получении общего решения. Такая задача относится к классу задач стохастической оптимизации, и ее решение следует искать алгоритмическими методами на основы моделирования на ПЭВМ.

Литература

1. Бычков В.В. Основы разработки автоматизированных корабельных комплексов, конструкции и действие их элементов. Ч. 2. Основы разработки и конструирования корабельных систем повседневного и предстартового обслуживания ракетного комплекса. – СПб : СПб ВМИ, 2000. – С. 180.

2. Бычков В.В. Автоматизированные корабельные комплексы. Ч. 1. Основы устройства и эксплуатации пусковых установок и систем обслуживания ракетных комплексов. – СПб : СПб ВМИ, 2007. – С. 168.

3. Бычков В.В., Новиков В.В. Система обеспечения ЗИП корабельных комплексов ударного ракетного оружия с учетом прогнозируемых изменений технического состояния. Научно-методический сборник статей. Вып. 8. – СПб : СПб ВМИ, 2007. – С. 94–97.

4. Кудрявцев И.Б., Петрунин А.В., Бычков В.В. Технология производства и эксплуатации корабельных комплексов. – СПб : СПб ВМИ, 2005. – С. 367.

5. Новиков В.В. Совершенствование системы технического обслуживания и ремонта комплексов ракетного и артиллерийского вооружения ВМФ на основе прогнозирования их технического состояния. Диссертация д.т.н. – СПб : ВМА, 2005. – С. 267.

УДК 35

ОБРАБОТКА РЕЗУЛЬТАТОВ ПРЯМЫХ МНОГОКРАТНЫХ ИЗМЕРЕНИЙ В ПРОЦЕССЕ ЭКСПЛУАТАЦИИ РАКЕТНОГО ВООРУЖЕНИЯ И ВОЕННОЙ ТЕХНИКИ

Бычков В.В.[1], **Мануйленко В.Г.**[2]

[1)] *Санкт-Петербургский Военно-Морской институт имени Петра Великого*

[2)] *Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики*

Разработка новых методов позволяет повысить точность измерений и способствует повышению эффективности использования ракетного вооружения и военной техники на корабле, что положительно скажется на боеготовности в целом.

Ключевые слова: вооружение и военная техника (ВВТ), средства измерений, программный метод обработки, алгоритм обработки результатов, эксплуатация, эффективность.

Сегодня стало очевидным, что поддержание боевой готовности корабля невозможно осуществить без измерений большого числа параметров и характеристик средств его вооружения. Успех современных боевых действий также во многом зависит от того, насколько полно используются возможности вооружения и военной техники (ВВТ), т.е. реализуются их тактико-технические характеристики, значения которых определяются и контролируются с помощью средств измерений (СИ). Иначе говоря, измерения составляют неотъемлемую часть боевой

деятельности подводной лодки, являются основным способом получения объективной информации о состоянии ракетного вооружения (РВ) и подводной лодки, условиях их эксплуатации. Поэтому достичь высокой боевой готовности можно лишь при обеспечении высокого качества и достоверности измерений различных электрических параметров.

Методика и модель обработки результатов прямых многократных измерений в процессе эксплуатации РВ.

Качество результата измерения характеризуется его погрешностью. Процедура измерения всегда строится таким образом, чтобы обеспечить малую погрешность результата измерений. Для этого, в частности, существуют методы, основанные на использовании избыточной информации об измеряемой физической величине - на обработке многократных измерений. Сегодня для обработки таких измерений используют в основном статистические методы [1]. Они отражают близость отдельного результата измерения к истинному значению измеряемой величины. Однако их широкое внедрение в практику повседневной деятельности специалистов-ракетчиков затруднено трудоемкостью выполняемых процедур, а также их недостаточными знаниями теории математической статистики в этой области. Поэтому для обработки результатов измерений должны быть разработаны алгоритмы и программы на ПЭВМ, точно указывающие порядок действий и дающие возможность получить искомый результат наиболее простым и быстрым путем. Это особенно необходимо при однотипных вычислениях, так как такая схема при автоматизации вычислений позволит выполнять их более быстро и надежно, при комплексных регламентных проверках и предстартовой подготовке ракетного оружия (РО).

Методика выполнения прямых измерений с многократными независимыми наблюдениями и основные положения обработки их результатов установлены ГОСТ 8.207-76 «Прямые измерения с многократными наблюдениями. Методы обработки результатов наблюдений. Основные положения». Согласно данному документу обработка группы результатов из n измерительных наблюдений $x_1, x_2, \ldots, x_n$, состоит из следующих операций:

1) исключения известных систематических погрешностей введением поправок для получения исправленных результатов наблюдений (если поправки известны);

2) вычисления среднего арифметического исправленных результатов наблюдений, которое принимается равным, результату измерения x;

3) вычисления оценки среднеквадратического отклонения (СКО) результатов наблюдения σ_i согласно ГОСТ 11.004-74 в предположении, что случайная величина подчиняется нормальному закону распределения;

4) вычисления оценки среднеквадратического отклонения (СКО) результата измерения σ_x;

5) проверки гипотезы о том, что результаты наблюдений принадлежат нормальному распределению по ГОСТ 11.006 -74 «Прикладная статистика. Правила проверки согласия опытного распределения с теоретическим». Данный пункт выполняется только при числе наблюдений n >15;

6) вычисления доверительных границ случайной составляющей погрешности измерения, которые без учета знака определяются по формуле:

$$\Delta^0 = t\,(n, P)\,\sigma_x, \qquad (1)$$

где t (n, P) – коэффициент Стьюдента, который в зависимости от доверительной вероятности P и числа результатов наблюдений n находящихся в табл. 2, которые выбираются при расчетах из ГОСТ 8.207-76;

σ_x – среднее квадратическое отклонение результата измерения.

7) вычисления границ неисключенной систематической погрешности j-го результата наблюдения по формуле:

$$\Delta Sj = \pm k \sqrt{\sum (m)^2}, \tag{2}$$

где Δs_J – граница i - й учитываемой неисключенной систематической погрешности;

K = 1,1 при P = 0,95;

m – число суммируемых погрешностей.

Поскольку измерения выполняются одинаковыми по точности средствами измерения, в одних и тех же условиях одним оператором, то их можно считать равноточными. В этом случае, отмечается в [2], в качестве предела допускаемой погрешности средств измерения, учитываемой как не исключенная систематическая составляющая погрешности измерения параметров приборов ракетного вооружения при многократных наблюдениях ввиду их близости, используется геометрическая сумма пределов допускаемых погрешностей при каждом наблюдении:

$$\Delta s = \pm \sqrt{\left(\frac{1}{n} \sum \left(\Delta S_j\right)^2\right)}, \tag{3}$$

где Δs_J – предел допускаемой погрешности СИ при j -м наблюдении;

n – число наблюдений;

Δs – сумма пределов допустимых погрешностей при каждом наблюдении.

Вычисления доверительных границ погрешности результата измерений Δ, которое при определенных условиях, оговоренных в ГОСТ 8.207-76, производится по следующим формулам:

$$\begin{gathered} \Delta = \Delta^0 \text{ при } (\Delta s/\sigma_x) < 0{,}8, \\ \Delta = \Delta s \text{ при } (\Delta s/\sigma_x) > 8, \\ \Delta = t_\Sigma \, \sigma_\Sigma \text{ при } 8 < (\Delta s/\sigma_x) > 0{,}8; \end{gathered} \tag{4}$$

$$\sigma_\Sigma = \pm \sqrt{\sigma^2{}_{\Delta S} + \sigma_x{}^2}, \tag{5}$$

где σ_Σ – суммарное среднеквадратическое отклонение результатов измерений;

σ_x – среднеквадратическое отклонение результатов измерения, в зависимости от измерительных наблюдений x.

$\sigma_{\Delta s}$ – среднеквадратическое отклонение суммы пределов допустимых погрешностей при каждом наблюдении.

$$t\Sigma = \frac{\left(\Delta^0 + \Delta S\right)}{\left(\sigma_{\Delta S} + \sigma_X\right)}, \tag{6}$$

где среднеквадратическое отклонение суммы пределов допустимых погрешностей при каждом измерении будет равно:

$$\sigma_{\Delta s} = \pm\sqrt{\sum \frac{(\Delta Sj)^2}{3}} \ , \qquad (7)$$

Если считать приемлемой в обоснованных случаях погрешность определения результата измерений до ±15%, то суммирование не исключенной систематической и случайной составляющей погрешности можно производить по упрощенной формуле:

$$\Delta = \pm\sqrt{\Delta S^2 + \Delta_0{}^2} \ , \qquad (8)$$

Расчет характеристик погрешности измерений при известных типах средств измерения основывается на использовании метрологических характеристик этих средств, нормированных по ГОСТ 8.009-84, если таковые приведены. В этом случае сначала объединяют отдельно характеристики случайной и систематической составляющих погрешностей, а затем находят пределы допускаемых погрешностей (для корабельной аппаратуры системы управления ракетных комплексов) по соответствующим формулам, приведенным ранее.

В соответствии с руководящим документом «Метрологические измерения 1317 – 86» при представлении результатов измерений и характеристик погрешности измерений указываются оценки нижней Δ_l и верхней Δ_h границ интервала, в котором погрешность измерений находится с вероятностью *P*, а также число наблюдений *n*, в течение которого они получены. Рекомендуемое значение доверительной вероятности *P* = 0,95. При одинаковых числовых значениях (без учета знака) Δ_l и Δ_h указывается $\pm\Delta$.

Описанная выше процедура обработки результатов многократных измерений при проведении ее в процессе повседневной эксплуатации и боевого применения ракетного оружия на подводной лодке, выражена составленным алгоритмом, блок-схема которого приведена на рис. 1. Каждый элемент схемы выражает отдельный шаг обработки. Например, шаг 4 описывает стандартную процедуру исключения систематических погрешностей (исправления результатов наблюдений).

Однако необходимо помнить, что в процессе эксплуатации комплексов ударного ракетного оружия характеристика разных приборов ухудшается по многим причинам. Прибор считается неисправным, если его метрологические (погрешность, чувствительность, вариация и т.п.) и технические (вибростойкость, ударостойкость, влияние колебания напряжения питающей сети и др.) характеристики не соответствуют его классу точности и требуемым условиям применения, к числу которых можно отнести следующие:

- износ осей, подшипников, шарниров, зубчатых передач;
- остаточную деформацию пружин;
- ослабление магнитов, перегрузки;
- нестабильность во времени элементов;
- изменение сопротивления реохорда вследствие его износа;
- изменение сопротивления манганиновых катушек вследствие химических и структурных изменений манганина;

– изменение переходного сопротивления коммутирующих устройств (переключателей и т. п.) многоточечных приборов;
– химические и структурные изменения материала полупроводников;
– смещение нуля усилителя;
– вибрацию деталей и элементов и т.п.

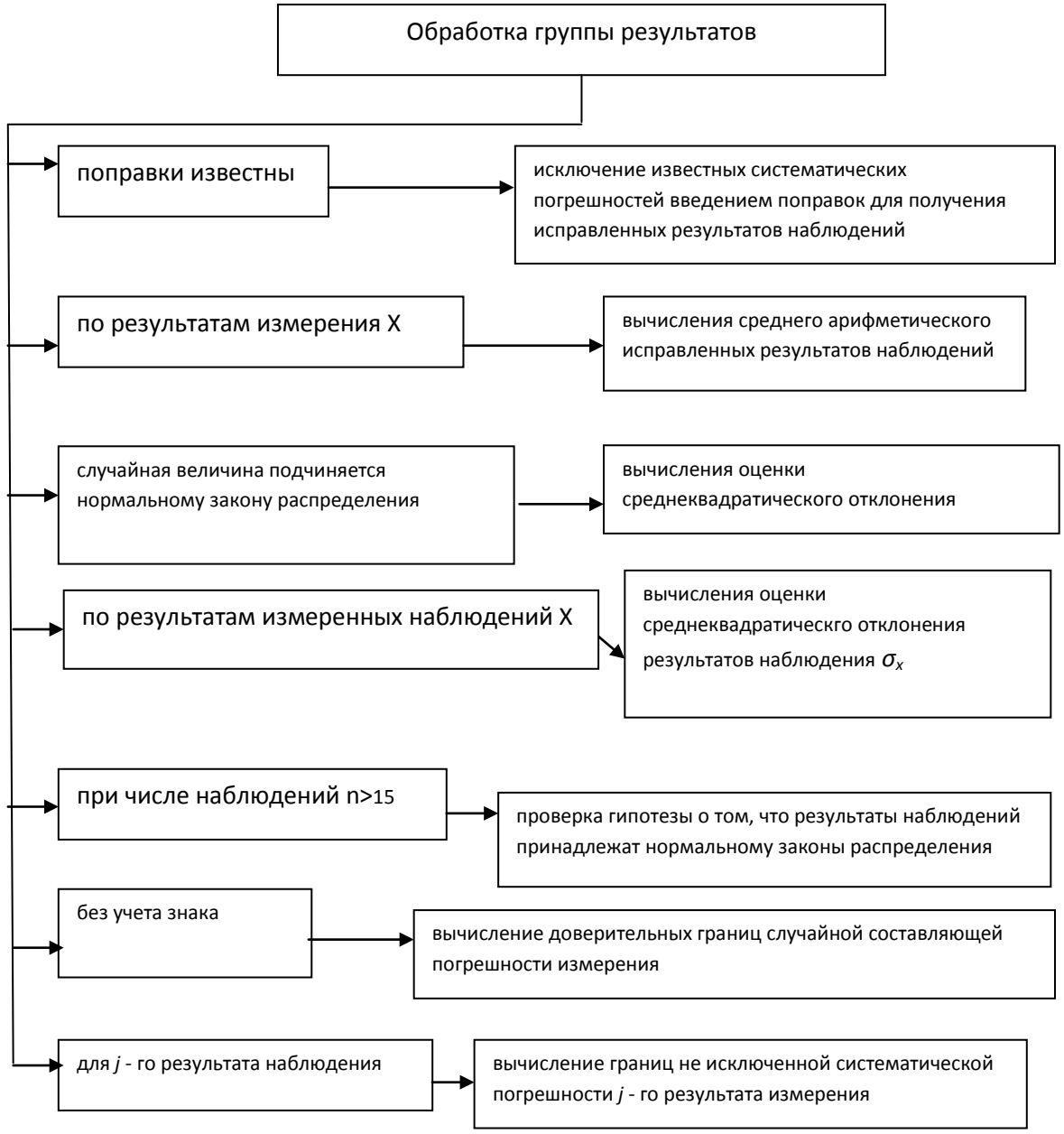


Рисунок 1. Модель обработки результатов многократных измерений

Характеристики приборов (метрологические, технические) могут ухудшаться и вследствие непосредственного выхода из строя их механических деталей, электрических и электронных элементов.

При длительном хранении приборов на складах, особенно в условиях переменной температуры и сырости, возможна коррозия металлических деталей и осей измерительных механизмов, в результате чего увеличиваются трение в осях и вариация показаний. При

плохом уплотнении корпусов внутрь приборов проникает пыль, способствующая ускоренному износу его подвижных деталей [3].

Разработанная методика и модель обработки результатов многократных измерений точно определяют порядок действий, которые необходимо выполнять при обработке многократных измерений контролируемых параметров ракетного вооружения на корабле. Они могут быть реализованы в виде программы на ПЭВМ, что даст возможность получить искомый результат измерения параметров более простым и быстрым путем. Данное исследование и рекомендации позволяют повысить точность измерений и способствует повышению эффективности использования ракетного вооружения и военной техники на подводной лодке, что положительно скажется на повышении боеготовности.

Литература

1. Фрумкин В. Д., Рубичев Н. А. Теория вероятностей и статистика в метрологии и измерительной технике. – М. : Машиностроение, 1987. – 145 с.

2. Хромой Б. П. Метрологическое обеспечение систем передачи. – М. : Радио и связь, 1991. – 392 с.

3. Бычков В.В. Автоматизированные корабельные комплексы. Ч. 1. Основы устройства и эксплуатации пусковых установок и систем обслуживания ракетных комплексов. – СПб : СПб ВМИ, 2007, 180 с.

УДК 35

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ЗИП ПРИ ЭКСПЛУАТАЦИИ КОМПЛЕКСОВ УДАРНОГО РАКЕТНОГО ОРУЖИЯ

Бычков В.В.[1], Мануйленко В.Г.[2]

[1)] *Санкт-Петербургский Военно-Морской Институт имени Петра Великого*

[2)] *Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики*

Одной из актуальных и трудноразрешимых задач при организации ТО и ремонта по техническому состоянию элементов ракетных комплексов является задача планирования количества запасных инструментов, частей и принадлежностей (ЗИП) на новых организационно-технических принципах.

Ключевые слова: Комплекс ударного ракетного оружия, запасные инструменты принадлежности и части (ЗИП), жизненный цикл, эксплуатация, обеспечение ЗИП.

Конструктивно комплексы ударного ракетного оружия (КУРО) в техническом отношении должно быть на уровне современных достижений науки и техники, обеспечивать высокую боевую эффективность применения в определенных условиях эксплуатации. Составные части (СЧ) КУРО должны соответствовать заданному функциональному назначению, отвечать высоким эксплуатационным требованиям, иметь основные параметры не ниже стандартов мирового уровня, для высокоточного оружия, в тоже время с учетом экономических затрат. Особое

внимание следует уделять не только боевому применению КУРО при эксплуатации, но и к процессам проведения технического обслуживания и ремонта, с использованием ЗИП.

Проблемы обеспечения ЗИП при эксплуатации КУРО

В процессе жизненного цикла КУРО зачастую разработанный путь разрешения противоречия между требованиями эксплуатации и требованиями обеспеченности ЗИП не совсем правильный, или не достаточно серьезно подходят к оценке критерия оптимизации взаимосвязей. Данное противоречие возникает за счет удовлетворения одних требований и ущемления других. С позиции системного подхода, принимая все требования за систему, требования эксплуатации и обеспеченности ЗИП будем представлять как две подсистемы. Рассмотрение подсистем с позиции их действия, приводит к тому, что на границе между требованиями эксплуатационными и обеспеченности ЗИП возникают внешние противоречия. В границах только требований эксплуатационных или только требований обеспеченности ЗИП возникают внутренние противоречия.

Требования эксплуатации и обеспеченности ЗИП, представляющие собой ограничения, могут носить текущий и перспективный характер. Ограничения текущего порядка отражают уже достигнутый уровень развития науки и техники, использование существующих методик расчета необходимого количества и организации обеспечения ЗИП [1].

Однако эти ограничения не следует учитывать при проектировании и подготовке производства КУРО, изготовление и эксплуатация которых намечается в будущем. В этом случае следует пользоваться перспективными данными в науке и технике, соизмеримыми с периодом проектирования, постановки на производство и эксплуатации составных частей КУРО, с учетом оптимального планирования, производством и обеспечение ЗИП.

Полное удовлетворение всех требований эксплуатации и обеспечения ЗИП представляет большие трудности и во многих случаях не представляется возможным. Поэтому необходимы комплексные решения по наиболее полному удовлетворению важнейших требований. При этом компромиссное решение можно рассматривать, как оптимальное направление, только применительно к определенному уровню науки и технике, а также конкретным производственным условиям, в которых намечается изготовление СЧ КУРО и запасных частей и принадлежностей [4].

Разрешая возникающие противоречия между требованиями в процессе проектирования, необходимо провести системный анализ, разработать имитационную модель, учитывать существенные факторы и взаимосвязи между ними (качественный анализ). Затем необходимо установить закономерности взаимосвязей и влияние их на количество производства СЧ КУРО и ЗИП (количественный анализ). Точность решения такой задачи определяется полнотой выявления существенных факторов и установления взаимосвязей. Оптимальный уровень удовлетворения требований эксплуатации КУРО и обеспеченности ЗИП выбирают на основании технико-экономических расчетов.

Важной характеристикой стоимости и эффективной эксплуатации комплексов ударного ракетного оружия являются затраты времени и средств на его техническое обслуживание и ремонт. При разработке ракетного комплекса предполагается, что его работоспособность в

эксплуатации будет поддерживать периодическим проведением определенных работ, входящих в состав технического обслуживания и ремонта [3].

Выполнение требований технического обслуживания, ремонта и обеспечением ЗИП в этих процессах, приводит к необходимости решения следующих задач:

– выявление факторов, определяющих технологию и организацию технического обслуживания и ремонта;

– установление зависимостей между параметрами, характеризующими технологию и организацию технического обслуживания и ремонта;

– разработка трудовых и материальных нормативов на выполнение технического обслуживания и ремонта;

– разработка методов прогнозирования объемов и периодичности выполнения ТО и ремонта применительно к проектируемым составным частям РК и условиям эксплуатации и обеспечением ЗИП;

– оценка эффективности конструктивных вариантов, обеспечивающих выполнение требований технологии и организации технического обслуживания и ремонта;

– рассмотрения организации поставок и использования ЗИП;

– обоснования производства необходимого количества ЗИП;

– рассмотрение организации хранения, технического обслуживания ЗИП;

– планирование комплекта ЗИП, с целью оценки уровня удовлетворения требований технологий производства и организации ТО и ремонта СЧ КУРО.

Таким образом, говоря об оптимальном уровне удовлетворения требований эксплуатации КУРО и по обеспечению ЗИП на основании технико-экономических расчетов, составил схему взаимосвязей между этими требованиями см. рис., при организации ТО и ремонта, а также обеспеченности ЗИП [2].

В последнее время все более широкое распространение для сложных технических систем, каковыми являются корабельные комплексы ударного ракетного оружия, находят гибкие стратегии технического обслуживания и ремонта (ТОР), при использовании которых период и объем ТОР обслуживаемого элемента являются переменными и зависят от его фактического технического состояния. Результаты теоретических и экспериментальных исследований показывают, что применение гибких стратегий ТОР для технических устройств КУРО позволяет значительно снизить затраты на их эксплуатацию без снижения показателей готовности [3].

Одной из актуальных и трудноразрешимых задач при организации ТО и ремонта по состоянию элементов ракетных комплексов является задача планирования запасными инструментами, частями и принадлежностями (ЗИП) на новых организационно-технических принципах. В этой связи необходимо обоснование и разработка методики прогнозирования технического состояния составных элементов КУРО и планирование по результатам прогноза обеспечивающего качественное проведение восстановительных работ, количества запасных частей для комплексов ударного ракетного оружия (рис. 1).

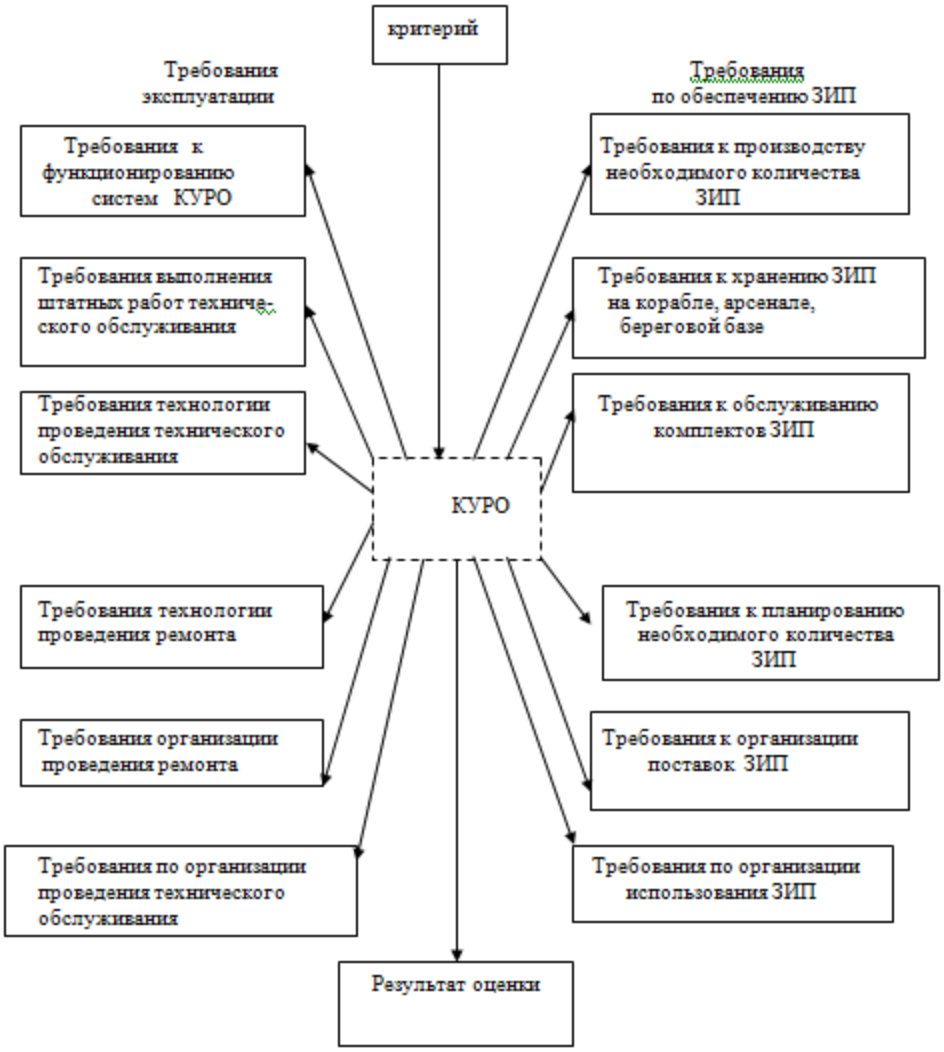


Рисунок 1. Схема взаимосвязей требований эксплуатации и обеспечения ЗИП

В соответствии с требованиями последних руководящих документов в целях повышения качественных показателей технического состояния (ТС) вооружения и военной техники (В и ВТ) на протяжении их жизненного цикла, при одновременном снижении расходов на эксплуатацию в существующих и перспективных образцах вооружения и военной технике, необходимо внедрять техническое обслуживание с периодическим контролем и ремонт по техническому состоянию составных частей комплексов ударного ракетного оружия подводных лодок. Таким образом, систему проведения технического обслуживания и ремонта необходимо проводить с учетом технического состояния составных частей КУРО, с учетом гибкой структуры в производстве и обеспечении ЗИП СЧ КУРО подводных лодок, осуществление индивидуального подхода к поставкам ЗИП на каждую подводную лодку.

Литература

1. Бычков В.В. Автоматизированные корабельные комплексы. Ч. 1. Основы устройства и эксплуатации пусковых установок и систем обслуживания ракетных комплексов. – СПб : СПб ВМИ, 2007. – 168 с.

2. Бычков В.В. Основы разработки автоматизированных корабельных комплексов, конструкции и действие их элементов. Ч. 2. Основы разработки и конструирования корабельных

систем повседневного и предстартового обслуживания ракетного комплекса. – СПб : СПб ВМИ, 2000. – 180 с.

3. Чернов Л.Б. Основы методологии проектирования машин. – М. : Машиностроение, 1978. – 97 с.

4. Осипов Б.Н., Смукул А.О., Федурин А.С. Ремонт и техническое обслуживание кораблей ВМФ. – М. : Воениздат,1978. – 263 с.

УДК 004.056.5

«СТРАТЕГИЧЕСКИЕ КОММУНИКАЦИИ» – ОСНОВОПОЛАГАЮЩАЯ КОНЦЕПЦИЯ В СИСТЕМЕ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА США

Гавриш В.М.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Ведение информационных войн с конца XX века стало носить систематический характер.

Термин «информационная война» используется:

– в широком смысле – для обозначения противоборства в информационной сфере и средствах массовой информации для достижения различных политических целей;

– в узком смысле – как информационные военные действия для обозначения военного противоборства в военной информационной сфере.

«Стратегические коммуникации» – это новая концепция информационной войны, разработанная в США. Она принята с целью максимального учета развития стран, культуры, избирательной системы и создания средств и базы данных, адаптированных к лингвистическим, социальным и культурным особенностям целевой аудитории.

Многие страны пересматривают в последнее время свои взгляды на формы и способы ведения войны.

Военные эксперты все больше рассматривают в качестве сферы ведения боевых действий информационное пространство. Ущерб, нанесенный противнику на идеологическом фронте, может превысить прямую выгоду, полученную в ходе военных действий.

Используя информационные ресурсы, можно уравнять общественным мнением. Манипулируя информацией, можно даже свести военную победу к поражению и наоборот.

Таким образом, информационное превосходство – одно из необходимых условий для достижения победы в современной войне.

Особенность информационных войн в том, что они могут вестись и в военное и мирное время, а для их маскировки придумывается «отвлекающие термины».

На сегодняшний день наибольшим опытом в этой области обладают США. Так, например, впервые в США появился термин «информационные операции». А сравнительно недавно введено в оборот по США понятие «стратегические коммуникации».

«Стратегические коммуникации» – это новая концепция информационных войн, принятое в развитие теории информационных операций. Под ней понимается комплекс мероприятий по целенаправленному воздействию на военно-политические силы, международные организации других стран, не только враждебных, предпринимаемые различными правительственными и неправительственными, военными учреждениями организациями США, а так же их союзниками.

Цель стратегической коммуникации – убеждение или принуждение целевой аудитории к принятию решений или совершению действий, направленных на формирование, сохранение или развитие благоприятных условий провидения американских национальных интересов. При этом используется, как согласованные информационные акции, идеологическая обработка, различные информационно-пропагандистские планы и прогнозы.

В США к основным структурам, реализующим концепцию «Стратегических коммуникаций», относятся:

- Госдепартамент;
- Министерство Обороны;
- Боевое командование Вооруженными Силами США;
- Агентство США по международному развитию;
- Инженерные войска стратегической коммуникации;
- Неправительственные организации.

В американском госдепартаменте понятие «Стратегические коммуникации» подменяют термином «публичная дипломатия». «Публичная дипломатия» заключается в преднамеренном создании в представлении целевой аудитории идеального имиджа США, американских идеалов и образа жизни посредством проведения информационных кампаний, акций, экономической, технической и гуманитарной помощи.

В качестве носителей информации согласно концепции «Стратегических коммуникаций» могут выступать информационные и физические домены (рис. 1).

К информационным доменам относятся радио, кабельное м спутниковое телевидение, печать, интернет, потоковое видео, мобильные телефоны, общественные организации и слухи.

Физическими доменами являются войсковые учения, демонстрации силы, визиты, конференции, различные рабочие семинары, научные и военные обмены, ассоциации выпускников, организация и проведение восстановительных работ, торговля и гуманитарная помощь, благодаря которым военно-политическое руководство США пытается вызвать симпатии к своей стране и ее Вооруженным Силам или страх перед их мощью.

Наиболее ярко это может проявляться для распространения специально подобранной информации (дезинформации).

Оно осуществляется путем: рассылки электронных писем по e-mail; организации новостных групп; создания сайтов для обмена мнениями; размещения информации на отдельных страницах или в электронных версиях периодических изданий и сетевого вещания (трансляции передач радио- и телестанций).

Так, в ходе конфликта в Косово компьютерная сеть Интернет использовалась для осуществления комплекса мероприятий информационно-пропагандистского и психологического

характера. Югославской стороной широко применялась рассылка электронных писем. Почтовые ящики более 10 тыс. пользователей, различных агентств новостей и правительственных чиновников (в основном в США) регулярно заполнялись посланием с описанием результатов бомбардировок и ракетных ударов по гражданским объектам, числа жертв среди мирного населения, а также страданий рядовых граждан, заставляя тем самым сомневаться в правильности официальной пропаганды. В свою очередь, действия НАТО впервые сопровождались мощнейшей информационной поддержкой в Интернете, для чего использовалось множество освещавших военную операцию сайтов. Большинство из них было создано непосредственно американскими специалистами по компьютерным технологиям или с их помощью. В течение только первых двух недель операции в Косово американское информационное агентство CNN подготовило более 30 статей, размещенных затем во всемирной сети. В среднем в каждой из них около 10 раз встречались слова «беженцы», «этнические чистки», «массовые убийства». О тщательной подготовке содержания публикаций говорит также тот факт, что в состав специальной группы, непосредственно работавшей в CNN, были включены пять военнослужащих 3-го батальона подготовки и распространения материалов 4-й группы психологических операций (ПсО) ВС США.

Во время военной кампании в Ираке ВС Соединенных Штатов также активно использовали глобальную сеть для оказания информационно-психологического воздействия на противника. Так, в начале января 2003 года была проведена широкомасштабная акция с помощью электронной почты. Рассылались послания на арабском языке иракским генералам с призывами не выполнять приказы С. Хусейна. Кроме того, в электронных сообщениях, составленных американскими военными психологами, содержались обращения к гражданам Ирака помочь предотвратить использование ОМП. В электронных письмах также звучал призыв обозначать местонахождение складов химического, биологического и ядерного оружия «световыми сигналами».

Следует отметить, что широкомасштабное адресное обращение к иракскому военному руководству – сравнительно новый момент в психологических операциях, проводимых в настоящее время ВС США. Высшим офицерам внушалась мысль о том, что «иракцы понесут огромные потери, если не присоединятся к борьбе против Саддама или, по крайней мере, не откажутся поднимать оружие против вторжения».

Примером может быть активное и целенаправленное использование возможностей Интернета чеченскими сепаратистами для пропаганды своих позиций, распространения дезинформации, сбора средств в свою поддержку и привлечения новых наемников. Множество сайтов, размещенных организациями и частными лицами на серверах разных стран, содержат статьи «прочеченской» направленности, фото- и видеоматериалы с соответствующими комментариями, призывами, а также ссылки на сообщения крупнейших мировых информационных агентств, в которых критикуется политика России и ее действия в регионе. Многие сайты дублируются на различных языках.

Арсенал средств «Стратегических коммуникаций» разнообразен. К ним, прежде всего, относятся средства массовой информации (СМИ), а так же связь и телекоммуникации, инфраструктура беспроводной связи, социологические исследования, избирательные технологии и методики подсчета голосов избирателей, массовые тренинги и образовательные программы.

Согласно решению американского конгресса научно – исследовательские работы по использованию теории «Стратегических коммуникаций» организуются, и проводятся в Министерстве Обороны США, в боевых командованиях, управлении заместителя Министерства Обороны по разведке, объединенном штабе и Госдепартаменте.

Таким образом, концепция «Стратегических коммуникаций» является одной из основополагающих в системе информационного противоборства США.

Мероприятия по информационному воздействию на военно-политическое руководство и общественное мнение различных стран, на мировое сообщество в целом проводятся не только как составная часть комплекса мероприятий по подготовке к операциям (Боевым Действиям), а уже стали их основным содержанием.

Средства массовой информации и коммуникации, открытые информационные ресурсы, глобальная информационная сеть Интернет активно используются Министерством Обороны и Госдепартаментом США не только для мониторинга угроз Национальной Безопасности страны, изучения общественного мнения, позиции государств, но и в целях манипулирования общественным мнением, дезинформации и введения в заблуждение военно-политического руководства других стран, принуждения его к принятию выгодных США и их союзникам решений.

Развитие концепции «Стратегических коммуникаций» является стратегией непрямых действий, заключающейся в воздействии на отдельные элементы системы информационного противоборства для требуемого результата.

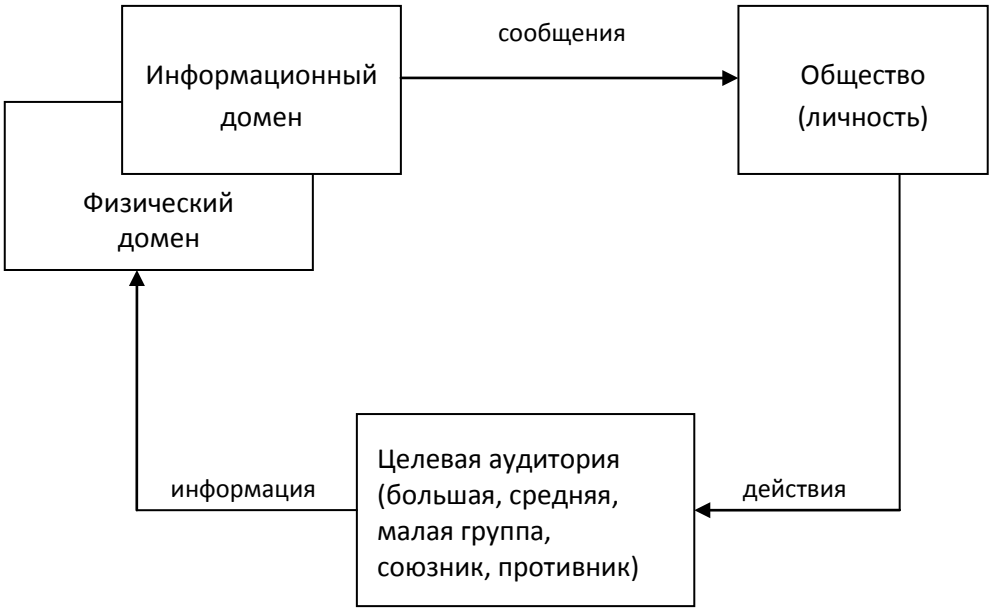


Рисунок 1. Взаимное влияние областей применения концепции «СК»

УДК 681.3

СИСТЕМА НЕПРЕРЫВНОГО МОНИТОРИНГА ЛИЧНОГО СОСТАВА НА ОТВЕТСТВЕННЫХ ПОСТАХ

Громов А.В., Зиновьев В.В., Касьянов Н.Н.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В данной статье рассматривается разработанный метод и устройства непрерывного контроля и прогнозирования состояния дыхательной и сердечнососудистой систем обслуживающего персонала объектов ответственного назначения. Рассмотрена возможность организации обратной связи системы мониторинга с личным составом.

Ключевые слова: Дыхательная система, сердечно-сосудистая система, неинвазивный метод, мониторинг, прогноз состояния, человеко-машинная система, терморезистор, микроэлектронный магнитный датчик.

Значение человека в опросах управления современными техническими комплексами, в том числе и стратегическими (такими как ядерные объекты, оборонные комплексы, химическая промышленность), в условиях случайных внешних воздействий, остается важным в обозримом будущем.

Поэтому все более актуальным становится оценка состояния технической системы совместно с оценкой психологического и физиологического состояния персонала, управляющего техникой. По сложившейся терминологии, сложные системы ответственного назначения рассматриваются как человеко-машинные системы, в которых роль технической и человеческой составляющих оцениваются равнозначно.

В сложившейся ситуации, наличия большого количества методов и систем контроля над аппаратной частью, наблюдается заметное отставание в системах контроля состояния организма личного состава. Отсутствие систем мониторинга способных непрерывно передавать информативные данные в режиме реального времени, обусловлено сложностью адаптации тех или иных устройств контроля к индивидуальным особенностям отдельно взятого человека.

Зачастую требования компактности и автономности средств измерения находятся в противоречии с ключевыми параметрами любых измерительных систем, а именно информативностью и надежностью.

Основной целью представленной работы является создание автономного компактного прибора, способного оценивать и прогнозировать психофизическое состояние личного состава. Так же ставится задача оснастить систему непрерывного мониторинга механизмом обратной связи, с наблюдаемым личным составом. Обратная связь позволит передавать личному составу инструкцию, позволяющую оптимизировать трудоспособность и стрессоустойчивость личного состава.

Инновационность представленной системы непрерывного мониторинг заключается в том, что измеряемым параметром в данной работе является не только пульсации в сердечнососудистой системе, а так же измерение ритмов дыхания посредствам измерения пульсации температуры потоков воздуха в носовой полости.

Комплексное измерение пульсаций сердечнососудистой системы и ритмов дыхание позволит наиболее полно и своевременно оценить физическое и психологическое личного состава. Дыхательная и сердечно сосудистая системы взаимосвязаны очень тесно. При дыхании изменяется объем грудной клетки, сердечной мышце приходится работать в уменьшающемся объеме. Для адаптации работы сердца в условиях переменного объема, происходит постоянное варьирование частоты и амплитуды сокращения сердечной мышцы.

Данный факт позволяет создать устройство, с помощью которого можно изменить ритм сердцебиения, варьируя ритм дыхания. Другим словами не смотря на то, что человек не может напрямую управлять частотой сердцебиения, тем не менее, управление ритмом сердца возможно по средствам сознательного изменения частоты и глубины дыхания. Существуют приборы, выполняющие подобного рода задачи. Принцип действия подобного рода приборов основан на обратной связи с исследуемым человеком. Недостатком такого рода приборов является отсутствие механизма, который мог бы оценить, насколько правильно была выполнена рекомендация, полученная человеком от устройства.

Задачи разработки средства оперативного контроля психофизического состояния личного состава

Главной задачей данной работы является разработка прибора способного точно и комплексно исследовать состояние человека-оператора.

Для решения поставленной задачи планируется вести непрерывный мониторинг за параметрами дыхания (частота, амплитуда, характер турбулизации потока воздуха) и параметрами кровотока по средствам ЭКГ–мониторинга.

В настоящее время в большинстве развитых стран в минимальный пакет медицинских обследований входят флюорография, электрокардиограмма (ЭКГ) иринограмма. В отечественных медицинских исследованиях так же практикуется флюорография и ЭКГ, но ринологические исследования фактически не проводятся, основными причинами сложившейся ситуации являются в первую очередь отсутствие установленных предписаний касательно ринологических исследований при проведении общего обследования организма. Кроме того высокая стоимость препятствует широкому использованию ринометров и риноманометров.

Ринология (от греч. rhís, родительный падеж rhinós – нос и logos – наука), раздел оториноларингологии, классифицирующий виды носового дыхания и внутреннюю структуру носа. Для решения широкого круга задач было разработано большое количество различных методов. В частности для исследования пропускной способности носовых каналов широкое распространение получили приборы, основанные на резистивном и акустическом принципах.

Перечисленные выше приборы и методы не пригодны для создания средств оперативного контроля состояния человека по ряду причин. Во-первых, большие габаритные размеры не позволяет проводить измерения длительное время, во-вторых существующие приборы, основанные на различных принципах действия, оснащаются масками и системой трубок, которые вносят искажения в параметры исследуемого воздушного потока. В результате параметры дыхания частично теряются и искажаются.

Существующие системы диагностики дыхательных путей не способны измерить малых колебаний скорости и температуры потока воздуха в внутри носовой полости при дыхании. Этот

недостаток является весьма существенным, по причине того, что малые колебания параметров несут в себе наибольшую информативную ценность. Именно колебания параметров дыхания в пределах от 1% до 10% среднего значения служат объектом исследования при проведении ранней диагностики и классификации дыхания Приборно-Программного Комплекса (ППК), разработанном в СПбГУ ИТМО[2].

Предпосылкой для разработки системы непрерывного мониторинга было создание миниатюрного и прецизионно информативного ППК, параметром измерения в котором является пульсация температуры в потоке вдыхаемого и выдыхаемого воздуха. Размеры чувствительной части не превышают 1 мм в диаметре, что позволяет разместить данное устройство в преддверии носа как показано на рис. 1.

Рисунок 1. Размещение чувствительного элемента (терморезистора) Приборно-программного комплекса (ППК)

Так же не составит труда расположить чувствительный элемент внутри дыхательной маски или спецодежды. Устройство неинвазивно, поэтому при использовании ППК личный состав не будет испытывать неудобства.

Разрабатываемое устройство должно отвечать требованиям, предъявляемым к приборам диагностирования. Большинство существующих приборов в качестве общеинтегрального параметра используют сердечный ритм и электрокардиограмму (ЭКГ). На сегодняшний день существует множество устройств, для проведения ЭКГ-мониторинга. Наибольший интерес представляет устройство оперативного контроля состояния параметров кровотока, разработанный Институтом Автоматики и Управления ДВО РАН [1]. Это устройство по своей сути представляет систему ЭКГ мониторинга. Данное устройство разрабатывалось специально для создания средства оперативного мониторинга и обладает такими необходимыми свойствами как компактность и мобильность. Кроме того разработчиками была решена проблема присущая устройствам данного типа, а именно были усовершенствована конструкция чувствительного элемента.

Как было заявлено разработчиками [1] устройство измерения параметров кровотока обладает высокой эргономичностью, и может быть использовано в качестве элемента штатной формы или спецодежды.

Одной из ключевых задач при создании корпоративной системы мониторинга является передача информации по средствам радиоканала.

Передающее устройство должно быть миниатюрных размеров, и обладать низким энергопотреблением, так как система должна работать длительное время в автономном режиме. Благодаря успехам современной электронике на рынке представлено большое количество миниатюрных беспроводных приемо-предающих устройств с системами энергосбережения. Для реализации ППК был использован комплект трансмиттеров и отладочных плат Texas Instruments EZ430-RF2500. Используемый стек протоколов сетевой стек SimpliciTI позволяет организовывать сенсорные сети различных топологий, кроме того наличие в стеке SimpliciTI интеллектуальной системы позволяет увеличить площадь покрытия радиосигнала и при этом существенно повысить надежность беспроводной сети.

Так как в современных человеко-машинных системах может находиться большое количество обслуживающего персонала (например, атомные стратегические объекты), то при разработке системы ставилась задача создания развитой беспроводной сети для осуществления мониторинга всего расчета или рабочей смены.

Описание работы приборно-программного комплекса

Одной из функций каналов носовой полости является нормализация температуры вдыхаемого воздуха до температуры тела. С этой целю, для улучшения теплообмена воздушного потока со стенками каналов носовой полости, поток максимально турбулизируется неоднородностями сечения и пазухами носовой полости. Значение температуры вдыхаемого воздуха периодически отклоняется от значения среднеобъемной температуры в измеряемом сечении потока. Периодическая пульсация температуры вдыхаемого и выдыхаемого воздуха, является объектом измерения в ППК.

Стенки носовых каналов представляют собой ткани насыщенные капиллярами. В зависимости от состояния организма геометрия стенок изменяется, следовательно, изменяется тип дыхания и характер турбулизации. Изменения температурных пульсаций возможно отслеживать с помощью чувствительного элемента.

Приборно-программный комплекс представляет собой устройство, состоящее из двух чувствительных элементов располагаемых в преддверии ноздрей. Полученный сигнал усиливается и оцифровывается. Устройство содержит трансмиттер, по средствам которого оцифрованный сигнал передается по радиоканалу на сервер. Для приема данных так же используется трансмиттер, подключенный к компьютеру по средствам USB порта.

Ключевым элементом в ППК является чувствительный элемент, которой представляет собой миниатюрный (диаметр бусинки не превышает 1 мм) малоинерционный(постоянная времени которого не превышает 0,2 с) терморезистор. Благодаря малой тепловой инерции достигается очень высокая чувствительность. Выбранная частота дискретизации позволяет оценить характер турбулизации. Характер движения турбулизированного потока и представляет исследуемый параметр, который обрабатывается совместно с данными о течении кровотока. Вывод о состоянии здоровья организма делается на основании совместного исследования двух перечисленных параметров.

Описание работы устройства неинвазивного измерения параметров кровотока

Неинвазивное измерение параметров кровотока производится по средствам наложения магнитного датчика на артерию. Параметры, предаваемые датчиком, отцифровываются и передаются по средствам радиоканала.

Запатентованное устройство [4] состоит из микроэлектронного магнитного датчика (рис. 2), обладающего унифицированными метрологическими характеристиками [3]. Передачу и обработку измеренных параметров, планируется передавать по средствам того же трансмиттера, что и в ППК. Так как на борту приемо-предающего устройства находится быстродействующий (200000 преобразований в секунду), многоканальный (12 входов) АЦП разрядность 10 bit и 12 bit, следует так же отметить скорость передачи, которая для стека протоколов SipliciTI достигает 250 кбит/с, такая скорость с избытком удовлетворяет требованиям поставленной задачи.

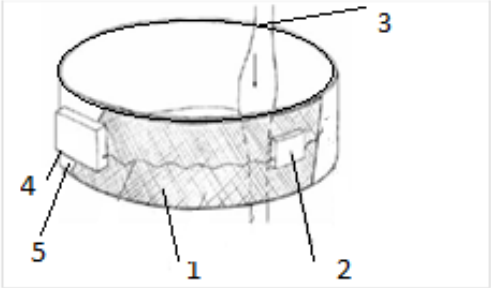


Рисунок 2. Внешний вид микроэлектронного магнитного датчика и артерии [1]. 1 – магнитный экран; 2 – схема узла измерений параметров кровотока; 3 – артерия; 4 – корпус приемопередатчика и аккумулятора; 5 – эластичная лента

Датчик температуры (терморезистор) и магнитный датчик подключены к блокам усиления и обработки и усиления сигналов по средствам мостовой схемы Уитстона.
Общая схема совместного подключения ППК и устройства ЭКГ мониторинга изображена на рис. 3.

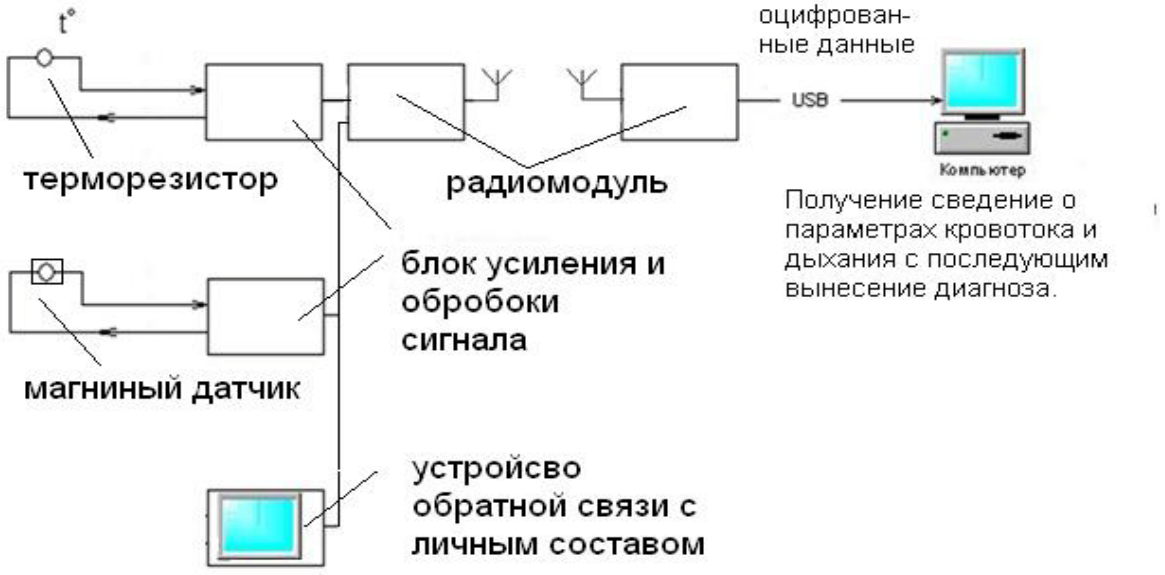


Рисунок 3. Принципиальная схема системы непрерывного мониторинга

Исследование взаимосвязи сердечносудистого пульса и дыхания

В результате проведения экспериментов были получены зависимости температуры выдыхаемого воздуха и электрических потенциалов сердца от времени.

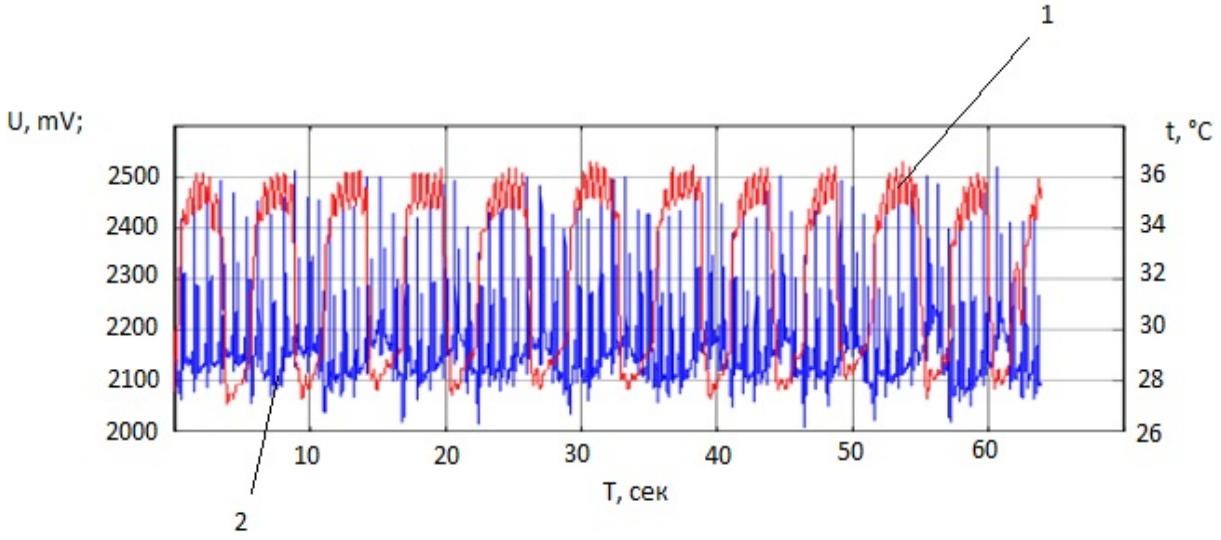


Рисунок 4. Зависимость температуры выдыхаемого воздуха и электрических потенциалов сердца от времени: 1 – график колебания температуры; 2 – график электрических потенциалов

Была рассчитана взаимная спектральная плотность мощности данных процессов с целью выявления характерных частот, на которых происходит взаимодействие дыхательной и сердечнососудистой систем пациентов. Выяснилось, что наибольшая мощность приходится на частоты порядка (0.3–0.8) Гц, что соответствует частоте дыхания. При этом у большинства обследованных с заболеваниями сердца были также выявлены характерные частоты взаимодействия на уровне выше одного герца.

Математическая обработка результатов

Процессы дыхания и сердцебиения быть идентифицированы методом нелинейной динамики и спектрального анализа.

Метод заключается в реконструкции фазовой траектории наблюдаемых флуктуаций скорости воздушного потока и электрических потенциалов сердца в фазовом пространстве, вычислении корреляционной размерности и энтропии и построении спектральной плотности мощности исследуемых процессов. В работе [2] приведены данные исследований около 500 пациентов. Полученные сведения обобщены в виде таблицы. В табл. 1 приведены типы дыхания в зависимости от корреляционной размерности и корреляционной энтропии.

Таблица 1. Количественная оценка типа дыхания в зависимости от корреляционной энтропии и корреляционной размерности

Тип дыхания	Корреляционная размерность D	Корреляционная энтропия K
Естественное дыхание	2,76	0,76
Прерывистое дыхание	3,27	1,02
Через одну ноздрю	3,25	0,63

Через одну ноздрю прерывистое	3,75	1,107

В настоящее время проводятся исследования по разработке методик организации обратной связи оператора и исследуемого *личного состава.*

Центральная нервная система регулирует взаимосвязь организма как единого целого. Сердечнососудистая деятельность обладает большой долей автоматизма, непосредственное управление сердцебиением сознательным усилием нервной системы не возможно, но ритмом дыхания человек может управлять вполне сознательно. При грамотном выборе ритма дыхания можно изменить ритм сердца, тем самым скорректировать аритмические изменения ритма сердца, или просто подобрать ритм дыхания, способствующий наименьшему утомлению. Именно такого рода «инструкцию» предполагается передавать исследуемому персоналу по средствам механизмов подающих рекомендации исследуемому персоналу (например наручных жидкокристаллических дисплеев, шлемофонов, и т.д), на основании текущие и оптимальные ЭКГ и ринограммы.

Подобного рода системы используются в медицине западноевропейских стран с целью вывода пациента из состояния депрессии или шока, или напротив концентрации внимания. К сожалению, подобного рода устройства регистрируют лишь ЭКГ, и не способны непосредственно проконтролировать правильно ли была выполнена «инструкция». Данная проблема связанна с отсутствием мобильных приборов, способных достаточно точно оценить параметры дыхания, не причиняя при этом неудобств и не затрудняя деятельности личного состава (экипажа машины).

Использование в системе оперативного мониторинга ППК позволяет оценить параметры дыхания с прецизионной точностью, при этом, не затрудняя деятельности исследуемого персонала. То есть становится возможным контроль и коррекция дыхания, а по средствам дыхания частичный контроль сердечного ритма.

Разработка ППК и успехи в области ЭКГ–мониторинга позволили вести разработку устройства дистанционного мониторинга на качественно новом уровне.

Данные получаемые от ППК не только находятся в полном согласии с данными полученными с помощью классических приборов (таких как риноманометров и ринометры), но и в значительной степени превосходят их по информативности. При этом чувствительный элемент не превосходит в диаметре 1 мм и блок обработки и радиопередачи немногим более спичечного коробка. Устройство мобильно, некритично к длительности измерений и в полной мере отвечает требованиям предъявляемым устройствам мобильного мониторинга.

Обнаружена взаимосвязь не только между ритмом дыхания и сердечнососудистым пульсом, но корреляция между малыми гармониками ринограммы и частотой, и интенсивностью Р–зубцов сердечного ритма. Подобного рода зависимости позволяют однозначно оценить как состояние сердечнососудистой системы, так и состояние организма в целом. Более того, опираясь на данный факт корреляции возможно предположить, что при накоплении достаточного количества статистических данных, точное диагностирование и прогнозирование систем организма будет возможно используя только данные полученный средствами ППК.

Немаловажным является ведение непрерывного мониторинга параметров кровотока и дыхания, благодаря непрерывному мониторингу накапливается достаточно статистического

материала о деятельности исследуемых систем, в результате чего появляется возможность с высокой степенью достоверности прогнозировать состояние организма и выявлять даже скрытые патологии на ранней стадии.

Современный уровень развития беспроводных систем передачи данных позволяет создать надежные сети с широкой зоной покрытия, в результате чего появляется возможность оперативного получения и обработки информации о психофизическом состоянии личного состава с целью оценки и прогнозирования состояния здоровья.

Реализация механизма обратной связи личного состава и системы непрерывного мониторинга, благодаря контролю параметров дыхания, позволяет решать такие задачи как повышение стрессоустойчивости и трудоспособности на качественно новом уровне.

Реализация представленной технологии непрерывного мониторинга позволит в значительной степени снизить риск возникновения техногенных катастроф по причине «человеческого фактора».

Литература

1. Розенбаум А.Н., Никитин А.И., Супоня А.А.Средства оперативного контроля состояния обслуживающего персонала человеко-машинных систем ответственного назначения. – Владивосток : Институт Автоматики и Процессов Управления ПВО РАН, 2010. – 7 с.

2. Рассадина А. А. Измерения и анализ флуктуаций температур, скорости и давления в каналах нерегулярной формы : автореф. дис. на соискание ученой степени канд. техн. наук. – СПб : 2007. – 16 с.

3. ГОСТ Р 51086-97. Датчики и преобразователи физических величин в электронные.

4. Патент на изобретение РФ 2378985 от 20.01.2010 г. Способ неконтактного измерения параметров кровотока, устройство для его осуществления и электронно-магнитный датчик.

УДК 358.2

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ ВОЕННОГО НАЗНАЧЕНИЯ И ТРЕБОВАНИЯ, ПРЕДЪЯВЛЯЕМЫЕ К НИМ В СОВРЕМЕННЫХ УСЛОВИЯХ

Зиновьев В.В.[1], **Морозов В.В.**[2]

[1)] *Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики*

[2)] *Михайловская военная артиллерийская академия*

Анализ современных военных конфликтов показывает, что на первый план выходят бесконтактные методы вооруженной борьбы. Побеждает тот, кто имеет о противнике высокоточную, актуальную и своевременную информацию, начиная от цифрового описания местности его территории, расположения войск и важных объектов до климатических и погодных условий районов предстоящих боевых действий.

В современных условиях в значительной степени возросли объемы и разнообразие данных, используемых при планировании (организации) и ведении боевых действий. Состав информации, необходимой органам управления (штабам) в ходе их деятельности в современных условиях, напоминает слоеный торт, с постоянно увеличивающимся количеством слоев – видов используемой информации. Кроме данных о противнике и местности возрастает объем и потоки используемой в процессе управления подчиненными соединениями (частями) оперативно–тактической, разведывательной, метеорологической и геофизической информации, которую необходимо учитывать и анализировать при подготовке и ведении боевых действий. На современном этапе необходимая разнородная информация в объемах, которые необходимы, не может быть своевременно принята, обработана и компилирована с использованием существующих технических средств управления органами управления при принятии решений на ведение боевых действий и применение средств поражения. В современных условиях объемы данной информации колоссальны. Для ее своевременной передачи и обработки требуются высокоскоростные каналы передачи данных, необходимы средства ее хранения в практически неограниченных объемах, высокопроизводительные компьютеры, средства отображения и обработки видео, фото и графической информации.

На сегодняшний день, очевидно, что противоречия, возникшие между возросшими потоками и объемами необходимой информации и имеющимися возможностями по их обработке, хранению и использованию, обуславливают необходимость разработки новых средств. Но такие средства современных информационных технологий уже созданы и используются в военном деле.

Среди них, на наш взгляд, особый интерес представляют, так называемые геоинформационные системы военного назначения (ГИС ВН), являющиеся неотъемлемой, составной частью современных автоматизированных систем управления (АСУ) войсками и оружием ведущих зарубежных государств.

Использование ГИС ВН предоставляет возможности для: сбора, накопления и визуализации цифровой информации о местности (ЦИМ), а также привязки и использования совместно с ЦИМ различной тематической пользовательской информации; разработки и выполнения ГИС–приложений, решающих широкий круг задач от анализа и оценки местности до моделирования действий войск на различных уровнях: от подразделения до оперативных объединений, использования их в АСУ войсками и оружием.

В первую очередь ГИС ВН позволяют резко сократить временные затраты на оценку обстановки и разработку планов боевого применения (действий) войск (сил) за счет комплексной обработки и отображения на единой основе всех видов используемой информации: картографической, оперативно-тактической, разведывательной, метеорологической, геофизической и др. При этом ГИС ВН позволяют решать в автоматизированном режиме задачи управления средствами поражения с учетом рельефа местности, мест расположения позиций огневых средств и объектов поражения (целей).

Основным требованием к ГИС ВН является преобразование и представление больших объемов разнообразной координатно-временной информации в виде, удобном для использования, органам управления войсками и оружием в процессе анализа и оценки

обстановки, планирования боевых действий, подготовки данных для целеуказания средствам поражения.

В современных условиях ГИС ВН должна обеспечивать: ввод цифровой информации о местности, векторных электронных карт, растровых электронных и фотокарт (фотоизображений) в различных форматах, астрономических и геодезических данных; преобразование ЦИМ в используемые в войсках проекции, системы координат и ее представление, и хранение в виде логически единых массивов информации;

Кроме того ГИС ВН должна обеспечивать ввод тематической информации: оперативно–тактической, разведывательной, гидрометеорологической.

Вместе с тем должно обеспечиваться отображение ЦИМ, тематической информации и результатов расчетных задач, в том числе с возможностью масштабирования и перемещения изображений, с возможностью выбора отдельных слоев и групп объектов.

ГИС ВН должна предоставлять возможность использования необходимой информации в режиме реального времени при подготовке и в ходе боевых действий; ввод, прием и отображение изменяющейся тематической информации и результатов расчетных задач; поиск различных объектов в задаваемой области по координатам и другим характеристикам с последующим их представлением и отображением на экране (определенным цветом, повышенной яркостью); создание, удаление и редактирование пользовательских объектов; обеспечивать увязку объектов геоинформации с тематическими базами данных с возможностью поиска одних через другие; обеспечивать логическую связь объектов, расположенных на различных листах; создание и вывод на печать тематических карт и отчетно-информационных документов.

Кроме того ГИС ВН должна позволять разработку и выполнение ГИС-приложений с помощью разработчика ГИС-приложений, предоставляющего возможность создавать приложения без программирования по алгоритму или схеме операций.

Таковы основные требования к ГИС ВН, выполнение которых позволит использовать потенциальные возможности современных геоинформационных технологий для своевременного и качественного решения задач передачи, обработки и хранения разнородной информации необходимой органам управления различных командных инстанций в современных условиях.

На сегодняшний день необходимо разработать развитое инструментальное ГИС-ядро и предоставить его системным интеграторам, которые должны компоновать на его основе тематические геоинформационные системы для конкретного пользователя (таких как, тематическая ГИС для планирования и моделирования действий войск (сил), тематическая ГИС обработки разведывательной информации, и др.). Безусловно, эти ГИС для каждого пользователя будут различны, но их методологическая основа будет близка, что создаст возможность объединения этих ГИС в рамках более крупных автоматизированных систем вплоть до АСУ Вооруженных Сил, тем самым появиться возможность для создания единого разведывательно-информационного пространства на базе ГИС.

Литература

1. Присяжнюк С.П., Филатов В.Н., Федоненков С.П. «Геоинформационные системы военного назначения». – СПб : СПб БГТУ, 2009.

2. Костров С. А., Бегларян С. Г. «Геоинформационные системы в управлении войсками и силами воздушно-космической обороны». – Воен. мысль, 2010. – № 3.

3. Воронин Е., Кашин В., Яблонский Л. Геоинформационное обеспечение вооруженных сил США. – Зарубежное военное обозрение, 2005. – № 10.

УДК 358.2

ПРОБЛЕМНЫЕ ВОПРОСЫ ПРИМЕНЕНИЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В КОАЛИЦИОННЫХ ВООРУЖЕННЫХ СИЛАХ НАТО В ХОДЕ ОПЕРАЦИИ «ШОК И ТРЕПЕТ» («СВОБОДА ИРАКУ»)

Красильников Н.И.[1], **Морозов В.В.**[2]

[1)] *Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики*

[2)] *Михайловская военная артиллерийская академия*

Операция «Шок и трепет» («Свободу Ираку») (в 2003 г.) коалиционных ВС НАТО в Ираке явилась закономерным продолжением предыдущих операций ВС НАТО последнего десятилетия («Буря в пустыне» (в 1991 г.) и «Лиса в пустыне» (в 1998 г.) против Ирака, «Союзническая сила» (в 1999 г.) на Балканах против Югославии, «Несгибаемая свобода» (в 2001 г.) в Афганистане) в которой широко применялись (испытывались) современные информационные технологии. При этом сам термин необходимо трактовать максимально широко – от пропаганды, использующей все каналы ее распространения, до электронной (компьютерной) начинки различных средств поражения, защиты и обеспечения боевых действий.

Наиболее очевидной, явилась информационная война. Накануне боевых действий администрация США составила планы информационно-пропагандистского обеспечения войны в Ираке, которые во многом опирались на опыт борьбы с талибами в ходе операции «Несгибаемая свобода». Главной целью этих мероприятий была игра на опережение и захват инициативы с тем, чтобы по 24 часа в сутки давать в средства массовой информации (СМИ) сообщения и комментарии, выдержанные в нужном Вашингтону ключе. Репортажи с места военных действий транслировались практически вживую, с минимальной задержкой. Все это было возможным благодаря не только спутниковой связи, но и современным алгоритмам сжатия и обработки видеоизображения и звука. Некоторые репортажи представлялось возможным транслировать, даже используя спутниковые телефоны.

Однако, по мнению западных экспертов, Пентагон явно переусердствовал с объемом специальной пропаганды, нацеленной на ослабление морального духа иракской армии. Большинство «сенсаций», появившихся накануне и в первые часы операции, оказались явной дезинформацией, в последствии раскрытой, рассчитанной, по–видимому, прежде всего не на иракцев, а на американских обывателей.

Следует подчеркнуть, что СМИ, как и во время операции «Союзническая сила» по–прежнему являлись главным источником информации, так же как и главной целью нападающей стороны. Утверждалось, что оборудование телевизионного центра в Багдаде было повреждено электромагнитной бомбой. Однако перерыв в вещании оказался небольшим, иракцы быстро перешли на резервные передатчики. Так что, возможно, применение боеприпасов в традиционном снаряжении было бы в данном случае гораздо эффективнее.

Перед началом боевых действий много говорилось о техническом оснащении коалиции. Это и разведка (воздушная и космическая), и высокоточные боеприпасы, наводящиеся на цель как самостоятельно, так и при помощи спутников, и автоматизированная система управления войсками, позволяющая в режиме реального времени доводить различного рода оперативно–тактическую информацию вплоть до каждого солдата, и персональная связь вместе со спутниковой навигацией. И даже электромагнитные бомбы – оружие, выводящее из строя электронные приборы.

В то же время необходимо подчеркнуть, что технологическое отставание Ирака было сильно преувеличено. Безусловно, традиционные проводные каналы телефонной связи плохи, однако следует отметить, что государственная и военная связь Ирака была построена на оптоволокне, поставки которого были ограничены экономическими санкциями. Но, в то же время, появление оптоволокна в Ираке через ряд посредников не представляется невозможным. Особенностью оптоволоконных линий связи является закрытость их для радиоэлектронной разведки и вследствие этого неуязвимость для ударов высокотехнологичного оружия. Вероятнее всего, руководство Ирака внимательно изучило и проанализировало опыт операций «Буря в пустыне» и «Лиса в пустыне» а, кроме того, и опыт операции «Союзническая сила», постаралось создать как можно более устойчивую систему управления. Хотя точная информация о ней, и отсутствует, не исключено, что она могла представлять собой закрытую, аналогичную Интернету, систему. Такая система может быть нечувствительна к выходу из строя отдельных узлов – необходимая информация может передаваться по обходному каналу связи (маршруту). Следует отметить, что ее можно смонтировать из обычных (стандартных) комплектующих, доступных для открытой продажи.

Однако после нескольких суток боевых действий оказалось, что использование современных информационных технологий само по себе не способно решить исход всей операции. Безусловно, и связь, и обмен оперативно–тактической информацией в ОВС НАТО поставлены более чем хорошо, однако это вовсе не спасало коалиционные ВС от трагических ошибок. Так, например полная передача принятия решений компьютерным системам стоила жизни двум британским летчикам: их истребитель «Торнадо» был по ошибке сбит системой «Петриот». В другом случае истребитель F-16, отреагировав на «захват» радиолокационной станцией комплекса ПВО, нанес ответный ракетный удар, уничтожив его. С точки зрения современных информационных технологий это примеры серьезных проблем в алгоритмах специального математического программного обеспечения. Во-первых, не сработала система «свой-чужой», а во-вторых, зенитно-ракетный комплекс, предназначенный для уничтожения ракет, принял за нее самолет, у которого иные скоростные характеристики.

С другой стороны, следует отметить проблемы в организации взаимодействия коалиционных ВС, о чем свидетельствуют многочисленные факты. Войска коалиции несли потери не только в результате столкновений с противником. Имели место случаи, когда наступающие

части попадали под так называемый «дружественный огнь», т.е. огонь собственных войск. Так, например: 26 марта 2003 г. в районе г. Эн-Насирия в результате «дружественного огня» по колонне были ранены 37 военнослужащих ВС США и уничтожены несколько единиц военной техники. Всего за время активных боевых действий в результате «дружественного огня» погибло более десятка и ранено более полутора сотен военнослужащих коалиционных ВС. Хотя современные информационные технологии вроде бы здесь и не причем, это лишнее доказательство того, что они не являются панацеей, способной решить все проблемы.

Еще одним очень уязвимым местом явилась спутниковая навигация. Удивительно, но факт: использование гражданского диапазона GPS на территории Ирака никак не ограничено. Возможно, разведка коалиционных сил посчитала, что на вооружении армии Ирака нет соответствующих навигационных устройств. Однако «неожиданно» выяснилось, что сигналы с GPS-спутников могут успешно забиваться недорогими, но эффективными устройствами (джаммерами), о такой возможности подозревали еще разработчики системы GPS. В России наиболее известна разработка фирмы «Авиаконверсия». Еще в 2000 г. появилась информация о том, что разработанные фирмой устройства создают помехи для полетов Объединенных ВВС НАТО, которые осуществляли патрулирование в небе над Ираком. Кроме того, гражданские чипы GPS используются в системах наведения высокоточного оружия (ВТО) и персональных навигационных системах военнослужащих. Несмотря на небольшую мощность, всего нескольких ватт, джаммер подавляет GPS-сигнал в радиусе до 500 км.

Командование коалиционных сил заявило о наличии в Ираке порядка шести таких устройств при том, что, по мнению специалистов, для прикрытия всей территории Ирака необходимо было около сотни. Затем последовало заявление об уничтожении всех засеченных джаммеров, однако, судя по не достаточно точным ударам ВТО, желаемое, скорее всего, выдавалось за действительное. Очевидцы бомбардировок Багдада сообщали о том, что часть ракет и бомб, коалиционных ВС, нацеленных на административные и военные здания иракской столицы, поразили жилые кварталы, расположенные вблизи от них. Так, например, у президентского комплекса «Диджла» были разрушены дома в районе «Кадиссия», а в 200 метрах от главного штаба ВВС Ирака пострадали здания района «Мансур». Высокоточные ракеты, бомбы и снаряды дорого обошлись мирному населению Ирака. По данным иракского министерства здравоохранения, от «точечных ударов» прежде всего, пострадали старики, женщины и дети. Следует отметить, что джаммеры в армии Ирака могли быть и собственного производства, для создания простых устройств подавления GPS не требуется специалистов высокой квалификации.

Безусловно, преждевременно делать окончательные выводы, но итоги операции «Шок и трепет» («Свобода Ирака») могут несколько пошатнуть веру во всемогущество современных информационных технологий, особенно в том случае, когда речь идет о ведении боевых действий в современных условиях. А если говорить о продолжающейся партизанской войне с применением тактики террора, то в этом случае и вовсе многое решает такой «нетехнологический» фактор, как моральный (боевой) дух войск.

Литература

1. Манойло А.В., 2003 г.: Государственная информационная политика в особых условиях, монография. – М. : Изд. МИФИ, 388 с.: ил.

2. Фролов Д.Б., Воронцова Л.В. Информационное противоборство: история и современное состояние. – М. : Горячая линия – Телеком, 2004.

3. Гриняев С.Н. Информационная война: история, день сегодняшний и перспектива// http://itblogs.ru/blogs/donskoy/archive/2006/10/20/8132.aspx

4. «Зарубежное военное обозрение», №7, 2005 г.

УДК 621.396.96

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ РАДИОЛОКАЦИОННЫХ КОМПЛЕКСОВ РАЗВЕДКИ ОГНЕВЫХ ПОЗИЦИЙ НА ОСНОВЕ МЕТОДА РАСПОЗНАВАНИЯ КАЛИБРА СНАРЯДА

Рудианов Г.В.

Санкт-Петербургский Государственный Горный университет

При определении радиолокационным комплексом разведки огневых позиций (РОП) параметров траектории снаряда решается система дифференциальных уравнений, одним из параметров которой является масса снаряда. Поскольку тип стреляющего орудия неизвестен (следовательно, неизвестна масса снаряда), то при решении системы уравнений используется усредненное значение массы снаряда. Данный факт, учитывая значительный разброс калибров снарядов (соответственно их масс), приводит к существенному снижению точности определения координат стреляющего орудия.

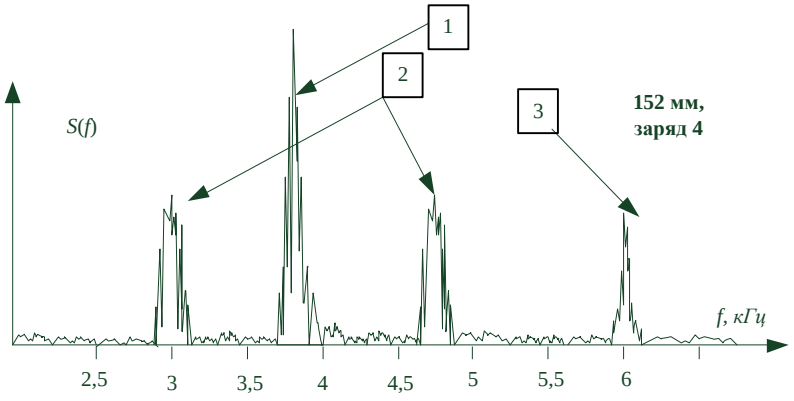
Поэтому актуальной является задача распознавания калибра снаряда с целью определения его массы.

В качестве признаков распознавания использованы частоты Доплера отраженного сигнала, обусловленные нутацией и прецессией оси вращения снаряда.

Прецессия создает амплитудную модуляцию сигнала, поэтому спектральные составляющие расположены симметрично относительно частоты вращения снаряда. Нутация обуславливает высокочастотные колебания оси снаряда и создает частотную модуляцию, поэтому спектральная составляющая расположена по одну сторону от частоты вращения.

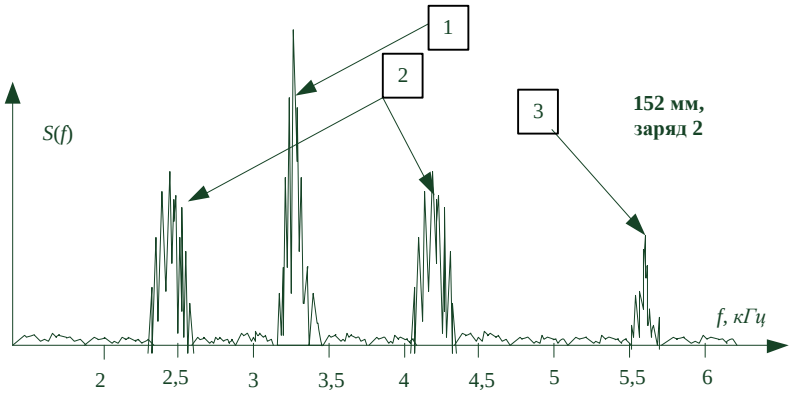
Спектры частот нутации и прецессии снарядов калибра 122 и 152 мм для различных зарядов, полученные по данным измерений РЛС «Зоопарк» при опытных стрельбах на испытательном полигоне, приведены на рис. 1.

При анализе данных спектров установлено, что при изменении номера заряда в значительной мере изменяется частота вращения, в то время как частоты нутации и прецессии для данного типа снаряда изменяются в небольших пределах и зависят только от конструктивных особенностей снаряда (коэффициента формы и массы). Поэтому на основе анализа частот нутации и прецессии вращения снаряда можно разделить классы различных типов снарядов.



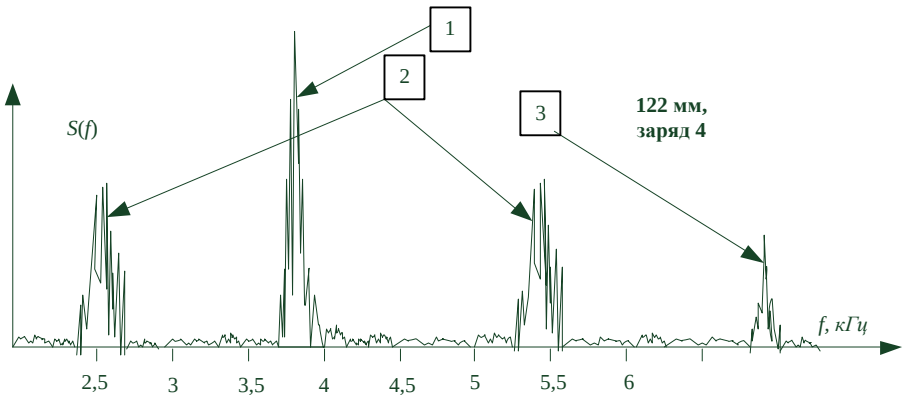
1 - вращение
2 - прецессия
3 - нутация

Рисунок 1. Снаряд калибра 152 мм, заряд 4



1 - вращение
2 - прецессия
3 - нутация

Рисунок 2. Снаряд калибра 152 мм, заряд 2



1 - вращение
2 - прецессия
3 - нутация

Рисунок 3. Снаряд калибра 122 мм, заряд 4

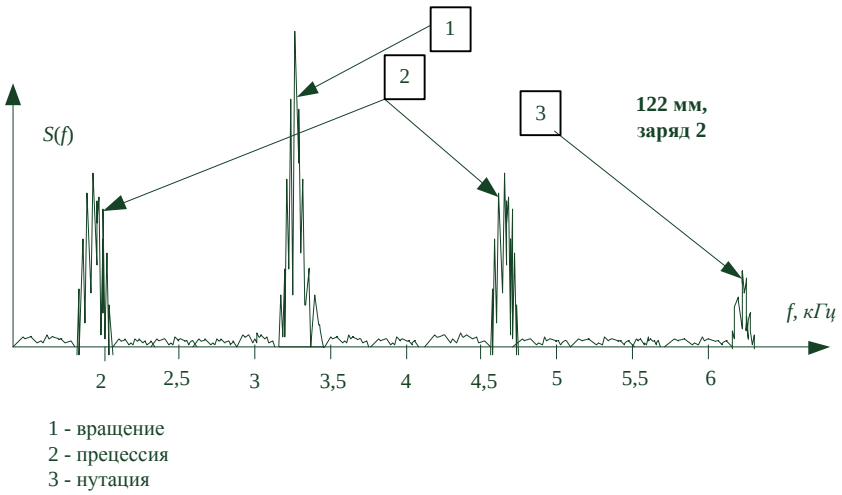


Рисунок 4. Снаряд калибра 122 мм, заряд 2

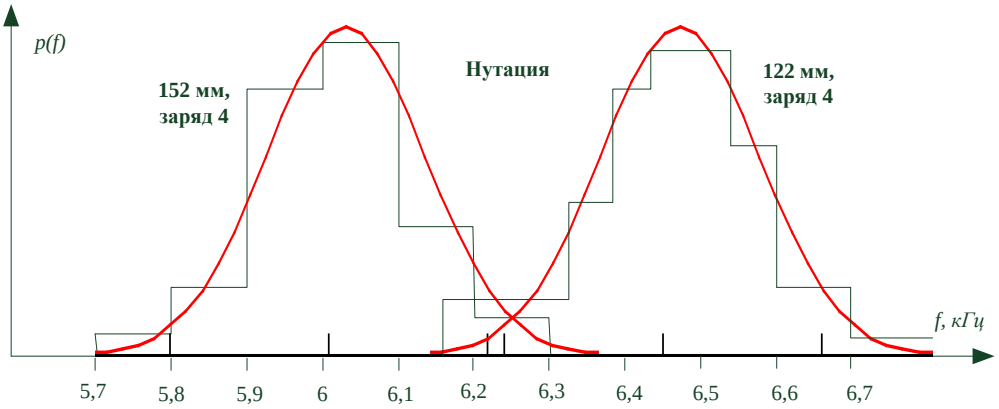


Рисунок 5. Спектры отраженных сигналов при нутации

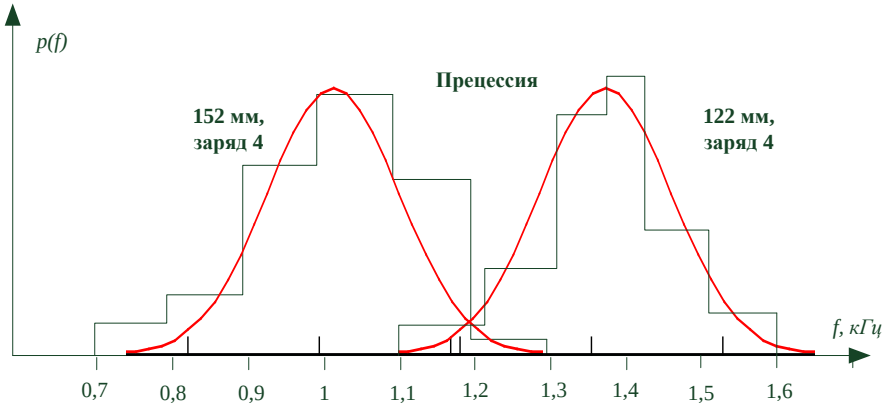


Рисунок 6. Спектры отраженных сигналов при прецессии

Для описания классов снарядов по результатам группы опытных стрельб построены законы распределения спектров нутации и прецессии снарядов калибра 122 и 152 мм для различных зарядов и определены их статистические характеристики – математические ожидания и дисперсии (принята гипотеза нормального распределения).

Для построения алгоритма распознавания использован критерий Неймана-Пирсона, заключающийся в том, что исходя из заданной вероятности ошибки 1-го рода (Q) определяется такая граница между классами, которая обеспечивала бы минимум условной вероятности ошибки 2-го рода. То есть требуется определить границу *A* между классами такую, чтобы

$$Q_1 = \int_x^{\infty} f_1(x)dx \le A \quad \text{при } \min Q_2 = \int_{\infty}^{x} f_2(x)dx \le A$$

Для определения границы между классами использован логарифм отношения правдоподобия для двух признаков [1]:

$$\log \lambda_2 = \log \frac{f_1(p)}{f_2(p)} + \log \frac{f_1(n)}{f_2(n)} =$$
$$= \log \frac{\sigma\sqrt{2\pi}\exp(-2\sigma^2(x_1 - m_1)^2)}{\sigma\sqrt{2\pi}\exp(-2\sigma^2(x_1 - m_2)^2)} + \log \frac{\sigma\sqrt{2\pi}\exp(-2\sigma^2(x_2 - m_2)^2)}{\sigma\sqrt{2\pi}\exp(-2\sigma^2(x_2 - m_2)^2)}$$

где f_1, f_2 – функции распределения первого и второго классов;

n и *p* – признаки (нутация и прецессия);

x_1, x_2 – границы между классами для первого и второго признаков (нутации и прецессии);

m, σ^2 – параметры законов распределения (математическое ожидание и дисперсия).

Из графиков распределений видно, что дисперсии σ^2 признаков несущественно отличаются, поэтому для упрощения вычислений приняты равными. Таким образом, после необходимых преобразований получаем:

$$\log \lambda_2 = \frac{m_1 - m_2}{\sigma^2}(x_1 + x_2 - (m_1 - m_2))$$

Это и есть величина порогов *A* и *B*, по которым распознаются первый или второй классы.

При этом ошибки первого и второго рода (Q_1, Q_2) определяются выражениями:

$$A \le \left|(1 - Q_1)/Q_2\right|, \quad B \ge \left|Q_1/(1 - Q_2)/\right|.$$

Таким образом, алгоритм распознавания заключается в следующем. Измеряются частоты нутации $f_{нут}$ и прецессии $f_{прец}$ снаряда. Производится сравнение суммы данных частот с пороговым уровнем.

Если

$$f_{нут} + f_{прец} \ge \frac{\sigma^2}{m_{нут} - m_{прец}} \log A + (m_{нут} + m_{прец}), \qquad (1)$$

то делается вывод о принадлежности объекта к первому классу.

Если

$$f_{нут} + f_{прец} \le \frac{\sigma^2}{m_{нут} - m_{прец}} \log B + (m_{нут} + m_{прец}), \quad (2)$$

то делается вывод о принадлежности объекта ко второму классу.

Если

$$\frac{\sigma^2}{m_{нут} - m_{прец}} \log B + (m_{нут} + m_{прец}) < f_{нут} + f_{прец} < \frac{\sigma^2}{m_{нут} - m_{прец}} \log A + (m_{нут} + m_{прец}), \quad (3)$$

то для устранения неопределенности необходимо продолжить наблюдение.

Параметры законов распределений частот нутации и прецессии для снарядов 122 и 152 мм представлены в табл. 1.

Таблица 1

122 мм			152 мм		
Нутация	$m_{нут}$	6,5	Нутация	$m_{нут}$	6
	$\sigma_{нут}$	0,3		$\sigma_{нут}$	0,3
Прецессия	$m_{прец}$	1,4	Прецессия	$m_{прец}$	1,1
	$\sigma_{прец}$	0,3		$\sigma_{прец}$	0,3

Задаваясь вероятностями 1 и 2 рода Q_1=Q_2=0,9, определяем величины порогов:

$$\frac{\sigma^2}{m_{нут} - m_{прец}} \log A + (m_{нут} + m_{прец}) = 7,88 \quad (4)$$

$$\frac{\sigma^2}{m_{нут} - m_{прец}} \log B + (m_{нут} + m_{прец}) = 7,11 \quad (5)$$

Для *оценки эффективности* данного алгоритма распознавания разработана математическая модель, структурная схема которой приведена на рис. 7. Показателем эффективности выбрана вероятность правильного распознавания (P_1) при фиксированной вероятности ложной тревоги (P_2).

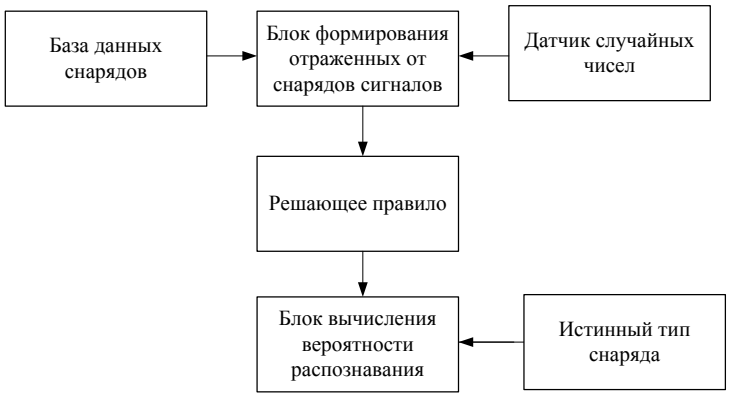


Рисунок 7. Структурная схема математической модели оценки эффективности алгоритма распознавания

Под воздействием датчика случайных чисел генерируется множество сигналов, отраженных от снарядов, с различными характеристиками нутации и прецессии (зависящими от номера заряда). Затем производится распознавание типа снаряда (согласно правилам 1–3) и расчет вероятности правильного распознавания.

Зависимости вероятности правильного распознавания (P_1) от вероятности ложной тревоги (P_2) представлены на рис. 8. Как видно, при вероятности ложной тревоги 0,3 вероятности правильного распознавания составляет не менее 0,8.

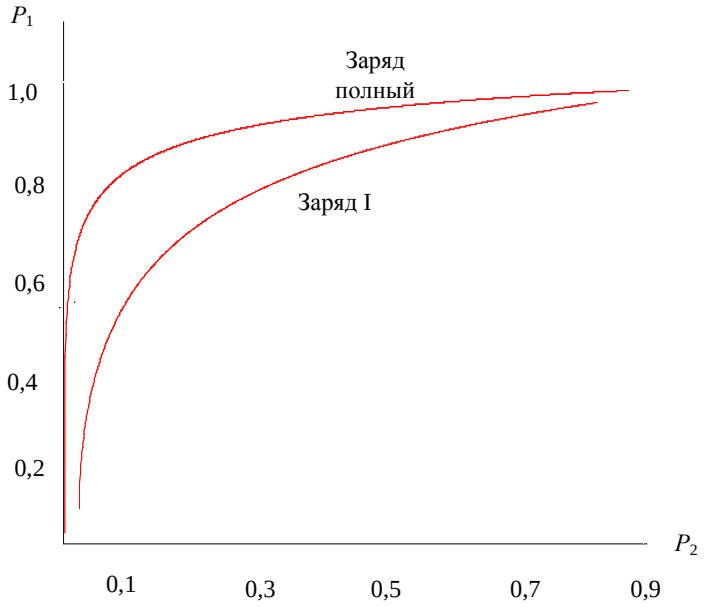


Рисунок 8. Зависимость вероятности правильного распознавания (P_1) от вероятности ложной тревоги (P_2)

Литература

1. Горелик А.Л., Скрипкин В.А. Методы распознавания. – М. : Высшая школа, 1984.

УДК 681.3

КОМПЛЕКСНОЕ ИСПОЛЬЗОВАНИЕ В ИНТЕРЕСАХ БЕЗОТКАЗНОСТИ СВОЙСТВ ВРЕМЕННОЙ ИЗБЫТОЧНОСТИ И ВОССТАНАВЛИВАЕМОСТИ В ПРОЦЕССЕ ФУНКЦИОНИРОВАНИЯ СИСТЕМ БЕЗОПАСНОСТИ

Супрун А.Ф.

Санкт-Петербургский государственный политехнический университет

Известно, что надежность систем характеризуется (согласно ГОСТ) безотказностью, долговечностью, восстанавливаемостью и сохраняемостью.

Большой интерес представляет работа по исследованию безотказности функционирования восстанавливаемых систем, а если предельно точно, то безотказности функционирования

восстанавливаемых в процессе функционирования технических систем обеспечивающих безопасность.

Здесь необходимо отметить, что целесообразно проводить работы не апеллируя к априорной информации о конкретном типе функций распределения случайных величин, участвующих в формализации задачи. Известно, что привилегия показательного распределения при анализе надежности восстанавливаемых систем объясняется характеристическим свойством этого класса распределений среди всех абсолютно непрерывных распределений. Отсутствие последствия обусловливает возможность применить аппарат теории цепей Маркова. Отказ, даже частичный, от экспоненты значительно усложняет соответствующий математический аппарат. В данном случае интерес представляет сначала задача «о двух лифтах», затем известные работы И.А. Рябинина (ВМА) и Г.Н. Черкесова (СПбГТУ) и, наконец, книга украинских математиков В.С. Королюка и А.Ф. Турбина: «Процессы марковского восстановления (ПМВ) в задачах надежности систем» (Киев, Наукова Думка, 1982).

Итак, ПМВ – двухмерные цепи Маркова, первая компонента которых (в свою очередь являющаяся цепью Маркова) описывает состояния системы, а вторая фиксирует времена пребывания этой системы в состояниях, то есть интервалы между моментами их изменений [Королюк В.С.,Турбин А.Ф.]. Полумарковское свойство состояний системы состоит в том, что время пребывания в состоянии зависит лишь от данного (и возможно следующего) состояния и не зависит от предыдущей эволюции системы. Поскольку в данных рассуждениях обходится какое бы то ни было упоминание о показательных распределениях, то физическое состояние реальной технической системы не обладает свойством полумарковости (отсутствие последействия). Согласно основной идее [Королюк В.С.,Турбин А.Ф.], физическое состояние технической системы определенным образом «расширяется» добавлением к этому физическому состоянию некоторой непрерывной компоненты, что обеспечивает новому расширенному состоянию обладание свойством марковости. Собственно, это и позволяет описать функционирование рассматриваемой восстанавливаемой системы с помощью ПМВ.

Заметим, что расширение множества физических состояний до множества полумарковских состояний даже в простейшем варианте (как в предлагаемой диссертации) приводит к тому, что приходится иметь дело не с матричными, как в случае цепей Маркова, а с матрично-интегральными уравнениями. Эффективным преодолением соответствующих трудностей является метод [Королюк В.С.,Турбин А.Ф.] асимптотического фазового укрупнения состояний случайных процессов. Его применимость связана с дополнительным предположением о высокой надежности исследуемой технической системы. Последнее имеет место, когда *среднее время* восстановления отказавшего элемента намного меньше среднего времени его безотказной работы. Действительно, *всякая* разумно спроектированная и грамотно эксплуатируемая система обязана быть высоконадежной.

Функционирование технической системы будем рассматривать как суперпозицию двух альтернирующих процессов восстановления, которые отражают взаимодействие подпроцесса внутреннего и внешнего функционирования технической системы.

Первый альтернирующий процесс «отвечает» за подпроцесс внутреннего функционирования технической системы:

В течение случайного времени α_1 техническая система находится в рабочем состоянии, затем происходит «частичный» отказ системы, и в течение случайного времени α_2 техническая система восстанавливается (до полного восстановления), далее подпроцесс неоднократно повторяется.

Второй альтернирующий процесс отражает потребность в объеме выполнения функций (в обеспечении энергией или другого сорта ресурсов) технической системы, другими словами, характеризует «тактический фон», формируемый системой вышестоящего иерархического уровня:

В течение случайного времени β_1 даже при нахождении технической системы на восстановлении (время α_2) функционального отказа системы в целом (с учетом потребностей среды, на «тактическом фоне») не наблюдаются.

В течение случайного времени β_2 имеет место потребность в использовании технической системы на максимальном уровне, который соответствует 100%-ой исправности системы.

Понятие функционального отказа при таком описании вводится естественным образом:

– Техническая система находится на восстановлении (α_2) и в этом состоянии возникает потребность в работе на 100% уровне;

– На потребность в работе на 100% - ом уровне технической системы (β_2) «накладывается» частичный технический отказ системы (α_2), исключающий возможность удовлетворять потребности вышестоящего уровня («тактического фона»).

$$\Lambda = \frac{(\mathrm{M}\beta_2 + \mathrm{M}\alpha_2)}{\mathrm{M}\beta_1 \cdot \mathrm{M}\alpha_1},$$

При такой интерпретации функционирования технической системы при сформулированных выше допущениях, а также при условии независимости (слабой зависимости) подпроцессов внешнего и внутреннего функционирования, функция распределения времени до функционального отказа технической системы оказывается *показательной* с параметром Λ, где символ M означает среднее (*МОЖ*) соответствующих случайных величин α_1, α_2, β_1 и β_2.

В заключение отметим, что время безотказного функционирования восстанавливаемой технической системы может быть достаточно точно аппроксимировано показательным распределением, как показано выше, что может быть интерпретировано геометрическим распределением.

УДК 152

ОБ ОПЫТЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММЫ MICROSOFT EXCEL ДЛЯ ПРОГНОЗИРОВАНИЯ ХОДОВЫХ ПАРАМЕТРОВ ППС ПРИ ОБРАБОТКЕ ДАННЫХ НАТУРНЫХ ИСПЫТАНИЙ

Шерстобитова А.А.

Санкт-Петербургский национальный исследовательский университет информационных технологий механики и оптики

ОАО «Концерн «Морское подводное оружие – Гидроприбор»

Научные руководители: к.т.н. Лев И.Г.[1], доц. Серебров А.И.[2]

[1)] *ОАО «Концерн «Морское подводное оружие – Гидроприбор»*

[2)] *Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики*

В работе описывается опыт использования программы EXCEL [1] для уточнения гидродинамических характеристик ППС: моментных, силовых гидродинамических коэффициентов ПА, а также коэффициента нормального сопротивления КБ.

Одним из важнейших средств проникновения в морские глубины являются привязные подводные аппараты (ППА), находящие в последнее время все более широкое применение. При проведении натурных ходовых испытаний привязных подводных систем зачастую возникает необходимость определения гидродинамических характеристик с целью уточнения математической модели системы. Целью данной работы является уточнение по данным натурных испытаний моментных и силовых гидродинамических характеристик ПА, а также коэффициента нормального сопротивления КБ.

Несмотря на функциональное и конструктивное разнообразие современных ППС, их создатели сталкиваются с рядом сходных проблем и нуждаются в разработке общих подходов к их разрешению. В частности, к таким проблемам относятся проблемы гидродинамики. Представляется очевидным, что при создании движущихся под водой привязных подводных систем и аппаратов изучение вопросов их динамики, силового воздействия среды и базового судна, вопросы управления и стабильности движения являются первостепенными и во многом определяют возможность нормального функционирования аппаратуры, установленной на них. На ранних этапах развития ППС превалировали экспериментальные методы обработки их ходовых характеристик. Ограниченные возможности вычислительных средств того времени позволяли оценивать расчетным путем лишь минимальное число необходимых динамических параметров. С появлением современной вычислительной техники возникла возможность развития и реализации ряда численных методов решения теоретических задач гидродинамики и математического моделирования динамики ППС, позволяющих глубоко исследовать вопросы их движения и динамики с привлечением минимального объема экспериментальных данных. Это обеспечивает возможность ускорить и существенно удешевить создание таких систем, а также их качества.

ППА принято называть подводные технические средства, имеющие механическую гибкую связь с судном или другой плавучей платформой, которые обеспечивают буксировку подводного аппарата. ППА вместе с гибкой связью составляет привязную подводную систему (ППС). В зависимости от назначения ППС может быть обеспечено движение привязного аппарата в толще

воды, вблизи ее поверхности или у морского дна. На рис. 1 представлена схема буксировки придонного подводного аппарата (ПА).

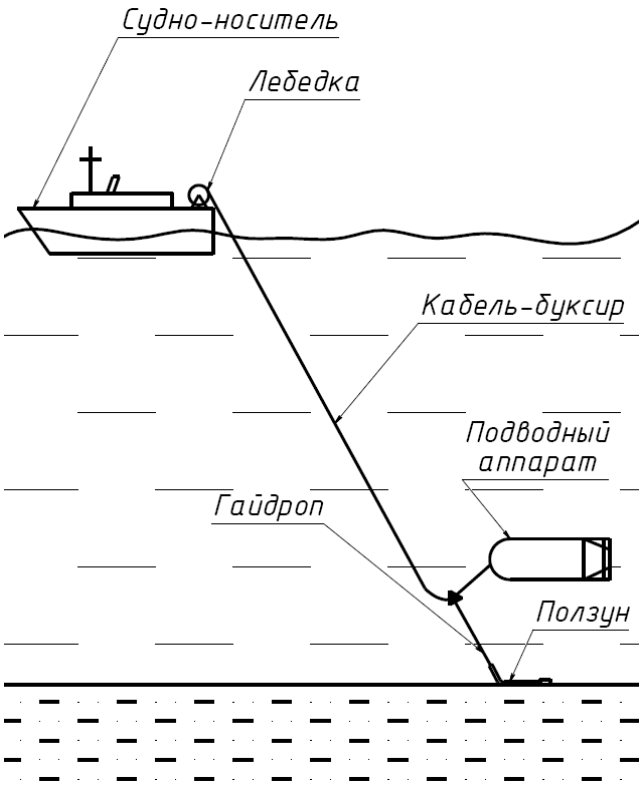


Рисунок 1. Схема буксировки ПА

Для проведения гидродинамического анализа были предоставлены выписки из судового журнала, в котором в процессе испытаний регистрировались: момент записи (дата, часы, мин); скорость буксировки – V (уз.); длина вытравленной части КБ – L (м), натяжение КБ – T (кгс), отстояние ПА от грунта – h (м), угол дифферента ПА – ϑ (град). Были предоставлены данные по двум однотипным ПА (№1 и №2).

Учитывая специфику содержания экспериментального материала, для оценки каждой из гидродинамических характеристик буксируемой системы необходимо было применить те или иные индивидуальные приемы обработки экспериментальных данных, которые описаны ниже.
Для уточнения моментных характеристик ПА обработка данных производилась на основе формулы зависимости угла дифферента ПА от скорости (рис. 2):

$$\vartheta = -\frac{m_{z_0} \cdot q + S_X}{m_z^{\alpha} \cdot q - S_Y}, \qquad (1)$$

где $q = \rho \cdot F_X \cdot L_X \cdot V^2 / 2$ – модуль гидродинамического момента; m_{z_0} и m_z^{α} (1/рад) - постоянные коэффициенты, зависящие от компоновки ПА и расположения точки буксировки, при этом величина m_{z_0} характеризует также его гидродинамическую несимметрию;

ϑ (рад) – угол дифферента, равный углу атаки ПА; V – скорость буксировки в установившемся режиме;

$S_X = W \cdot X_w - G \cdot X_g$ – статический момент «передней центровки» ПА; $S_Y = W \cdot Y_w - G \cdot Y_g$ – статический момент «нижней центровки» ПА; ρ – плотность воды; $F_X = \pi \cdot D^2 / 4$ – характерная площадь ПА; D (м) – диаметр поперечного сечения ПА; L_X (м) – характерный размер ПА; W – водоизмещение ПА; G – вес ПА; X_W, Y_W – координаты центра водоизмещения относительно точки буксировки; X_g, Y_g – координаты центра тяжести относительно точки буксировки.

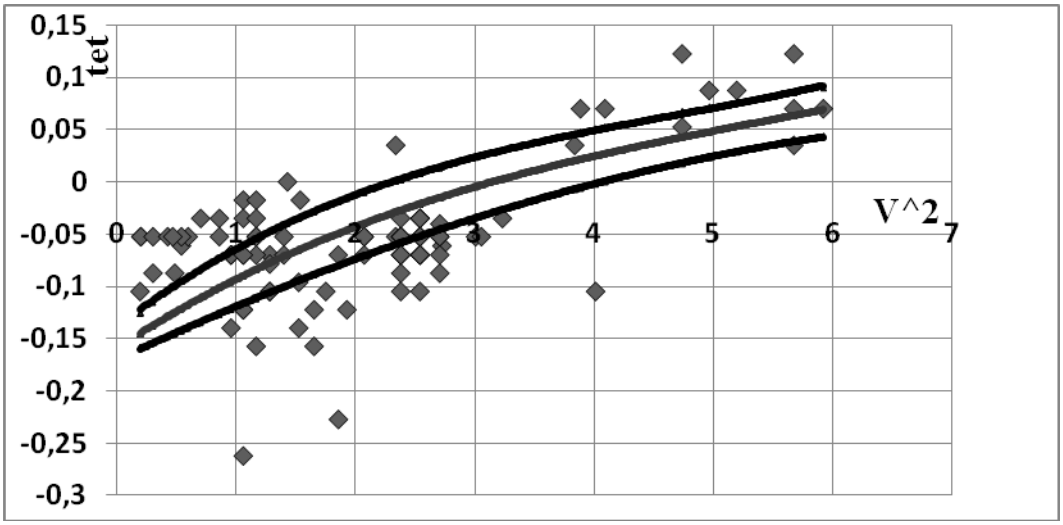


Рисунок 2. Зависимость угла дифферента ПА №1 от квадрата скорости буксировки

В процессе обработки пришлось столкнуться с большим разбросом данных, что, по-видимому, главным образом обусловлено как нестационарностью хода ПА при управлении по глубине с помощью судовой лебедки, так и погрешностями измерения скорости буксировки.

После ряда попыток преобразования формулы (1) для использования опции *Регрессия* из пакета *Анализ* EXCEL было принято ее представление как суммы постоянной и гиперболической составляющей [2]:

$$\vartheta = A_\vartheta + \frac{B_\vartheta}{C_\vartheta - V^2}, \qquad (2)$$

где: $A_\vartheta = -\frac{m_{z_0}}{m_z^\alpha}$; $B_\vartheta = \frac{2 \cdot (A_\vartheta \cdot S_Y - S_X)}{m_z^\alpha \cdot \rho \cdot F_X \cdot L_X}$; $C_\vartheta = -\frac{2 \cdot S_Y}{m_z^\varepsilon \cdot \rho \cdot F_X \cdot L_X}$ – постоянные величины, по которым пересчитывались искомые коэффициенты. В конечном итоге, для ПА№1 были получены значения моментных характеристик: $m_z^\alpha = -0{,}038$ (1/рад), $m_{z_0} = 0{,}011$(1/рад) и $S_X = -10{,}53$($кгс \cdot м$). S_Y принималось равным 65,5 ($кгс \cdot м$). При этом использование функции *Регрессия* EXCEL обеспечило величину показателя достоверности аппроксимации R^2 близкую к 1. Аналогичным образом оценивались параметры ПА №2.

На рис. 2 представлены экспериментальные значения угла дифферента ПА№1 и аппроксимирующая кривая угла дифферента ПА в зависимости от квадрата скорости буксировки

V^2. Здесь же приведены расчетные кривые с учетом возможной неточности значений скорости буксировки $V \pm dV$ при dV = 0,25 м/с.

При уточнении силовых гидродинамических характеристик ПА рассматривалась буксировка ПА у грунта.

Величина подъема ПА относительно узла стыковки h_b определяется гидродинамической нагрузкой на ПА и буйреп, а также их плавучестью. Величина подъема узла стыковки определяется главным образом «весом в воде» поднятой над грунтом носовой частью ползуна и силой трения о грунт располагающейся на грунте остальной его долей. Равновесие ползуна определялось с использованием дифференциальных уравнений тяжелой нити в потоке, а их интегрирование производилось в EXCEL методом Эйлера.

Для нахождения расчетных значений отстояний ПА от узла стыковки, исходя из опытных данных по аналогичным ПА (рис. 3), задаваясь некоторым набором значений коэффициентов c_{x0}, c_{y0}, c_y^{α} и плавучести ПА *P*, были использованы соотношения (3), где угол дифферента ϑ принимался достаточно малым, в результате чего $\cos(\vartheta) \approx 1$, $\sin(\vartheta) \approx \vartheta$.

$$h_b = L_b \cdot \sin\left[arctg(tg\alpha)\right] - X_{eh} \cdot tet - Y_{eh}$$
$$tg\alpha = \frac{Cy_0}{Cx_0} + \frac{C_y^{\alpha}}{Cx_0} + \frac{P}{Cx_0 \cdot q_1 \cdot V^2} \quad , \qquad (3)$$

где L_b – длина буйрепа; α (рад) – угол между буйрепом и горизонтом; ϑ (рад) – угол дифферента, X_{eh}, Y_{eh} – координаты расположения эхолота относительно точки буксировки, $q_1 = \rho \cdot F_X \cdot V^2 / 2$ – модуль гидродинамическоой силы.

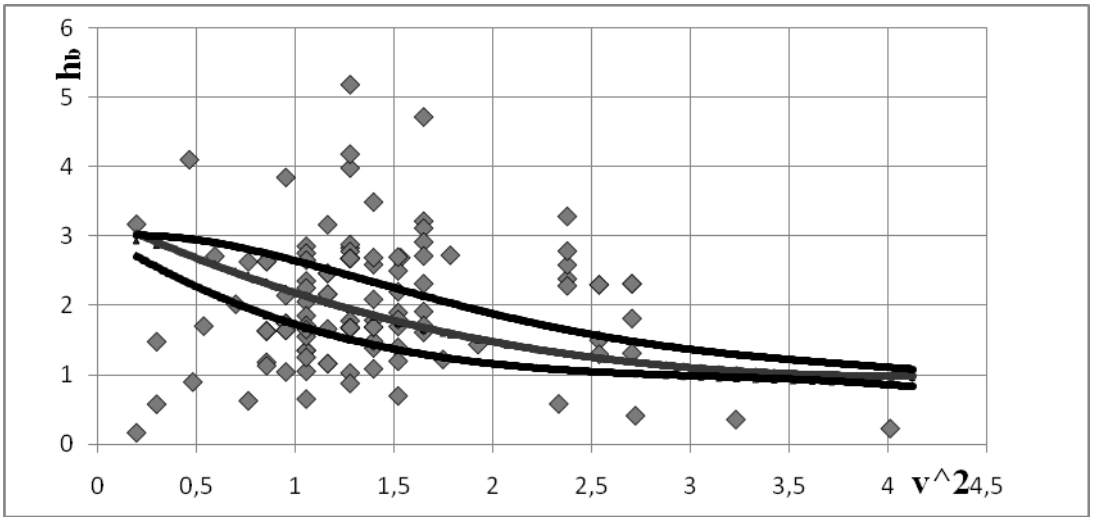


Рисунок 3. Зависимость расчетных значений отстояний ПА относительно узла стыковки h_b от квадрата скорости буксировки для ПА№1

В результате такого подхода для ПА№1 методом спирального спуска для минимального среднеквадратического отклонения экспериментальных значений отстояний ПА от узла стыковки

от теоретически определенных с учетом допустимых вариаций параметров были найдены следующие оценки искомых параметров: $c_{x0} = 0{,}5$, $c_{y0} = 0{,}1$, $c_y^{\alpha} = 1{,}95$, $P_{кг} = 50{,}3$( ).

Зависимость расчетных значений отстояний ПА относительно узла стыковки h_b, соответствующих значениям этих параметров, от скорости V с учетом возможной погрешности измерения скорости dV = 0,25 м/с в сравнении с экспериментальными данными для ПА№1 представлено на рис. 3.

Для оценки коэффициентов нормального гидродинамического сопротивления КБ было использовано соотношение[2]:

$$c_{n90} = \frac{2p \cdot \cos\alpha}{\rho \cdot d \cdot V^2 \cdot \sin^2\alpha} \qquad (4)$$

где: *d* – диаметр КБ; *p*– «вес в воде» КБ на единицу длины.

При этом необходимо отметить, что измерение скорости производилось с помощью судового навигационного измерительного прибора - лага, находящегося в области поверхностного течения, что может явиться одной из существенных причин погрешностей оценок искомых параметров, поэтому при обработке данных было учтено возможное влияние погрешности лага (0,5 уз).

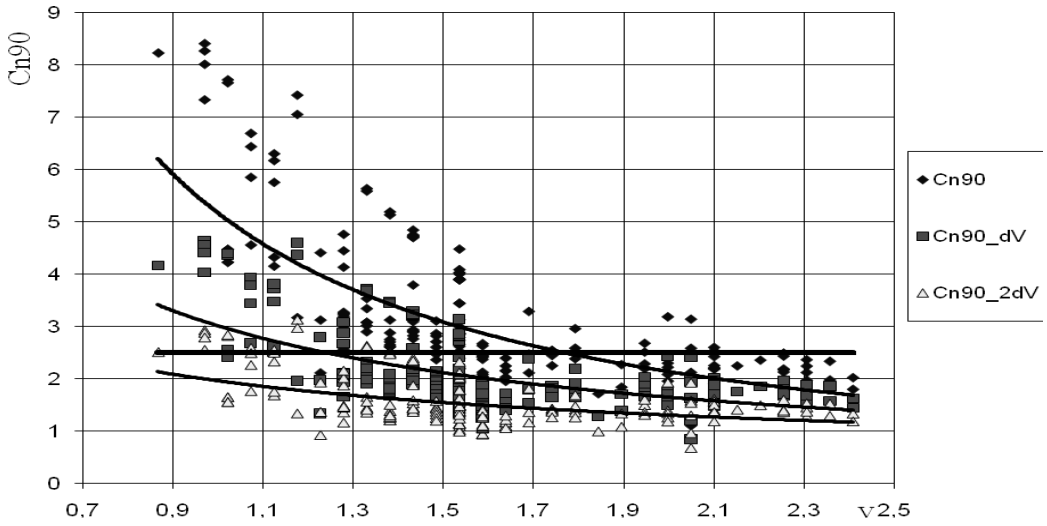


Рисунок 4. Зависимость $c_{n90}(V)$

На рис. 4 представлена зависимость коэффициента c_{n90} от скорости буксировки с учетом возможного встречного и попутного течения. Там же (горизонтальная линия) для сравнения приведено значение коэффициента Cn90, полученное при испытаниях шестипрядного стального троса при критических углах атаки [4].

По итогам обработки выборочных данных была произведена оценка гидродинамических параметров ППС с использованием программы Microsoft EXCEL. Программа EXCEL в данном случае послужила удобным инструментом для быстрого построения разнообразных диаграмм по заданным таблицам данных, подбора для этих данных аналитических выражений (линий тренда). Программа EXCEL незаменима при обработке больших массивов данных, когда при изменении

значения какого-либо исходного параметра автоматически происходит пересчет всей расчетной таблицы и изменение диаграммы, построенной по ней. Все вышеперечисленное позволяет пользователю легко устанавливать, как повлияло изменение того или иного исходного параметра на расхождение расчетных и опытных данных.

Данная работа была посвящена определению гидродинамических параметров и характеристик ГБС. Полученные в процессе статистической обработки оценки параметров могут позволить разработчикам ГБС грамотно подойти к проектированию.

Литература

1. Гельман В.Я. Решение математических задач средствами EXCEL. – СПб : Питер, 2003.

2. Виноградов Н.И., Гутман М.Л., Лев И.Г., Нисневич М.З. Привязные подводные системы. Прикладные задачи статики и динамики. – СПб : Изд. С.-Петерб. ун-та, 2000.

3. Виноградов Н.И., Крейндель С.А., Лев И.Г., Нисневич М.З. Привязные подводные системы. Аэрогидродинамические характеристики при установившемся движении. – СПб : Изд. С.-Петерб. ун-та, 2005.

4. Лев И.Г. К вопросу о гидродинамических характеристиках плохообтекаемых гибких связей // Подводное морское оружие. – вып. 12. – 2008.

СЕКЦИЯ С. СОВЕРШЕНСТВОВАНИЕ ОБРАЗОВАНИЯ ТЕХНИЧЕСКОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ОБОРОНЫ

УДК 355.54

УКРЕПЛЕНИЕ ЭЛЕМЕНТА «ДЕРЖАВНОСТИ» В СИСТЕМЕ СОВЕРШЕНСТВОВАНИЯ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ ПРИ ПОДГОТОВКЕ СТУДЕНТОВ, ОБУЧАЮЩИХСЯ НА ВОЕННОЙ КАФЕДРЕ СПБ ГУ ИТМО

Белошев В.А., Рыжков А.В.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В настоящее время уже вред ли существует необходимость доказывать кому либо, необходимость патриотической составляющей в воспитании и обучении специалистов силовых структур. Одним из ключевых понятий в системе патриотических ценностей приходится на державность.

Державность – это отождествление себя с Россией, со всем ее национальным богатством, природой, каждым листочком, каплей воды, глотком воздуха.

Сейчас под **державностью** следует понимать характеристики политического, экономического, военного и духовного могущества страны в мире, а также способности оказывать влияние и давление в международных отношениях. Да и само слово «держава» своим происхождением обязано славянскому «***държа***» (владычество, могущество), и в смысловом и стилистическом отношении представляет собой возвышенное обозначение страны и государства со значением **мощи**.

Дело в том, что процесс централизации Российского государства шел при опережающих политических факторах (борьба с внешней угрозой и установление национальной независимости), в силу чего влияние внешней истории России на ее внутреннюю историю было определяющим. Не случайно три общих курса русских истории (М.М. Щербатова, Н.М. Карамзина и С.М. Соловьева) положили в основу своих исторических конструкций рассказ о внешней политике России. Да и В.О. Ключевский в третьем томе «Курса русской истории» отметил могущественное влияние международного положения государства на его внутренний строй. И наоборот. Бывший марксист, а затем видный либеральный экономист и публицист П.Б. Струве в 1908 г. в журнале «Русская мысль» сделал важнейший вывод, что основой и критерием внутренней политики правительств должен служить ответ на вопрос, в какой мере эта политика содействует внешнему могуществу государства. Действительно, практически все российские модернизации подчинялись не столько решению внутренних проблем страны (и уж никак не повышению народного благосостояния),

сколько задачам обороны от внешних врагов, военно-политической экспансии империи и поддержания статуса великой державы.

Общественному сознанию нашей страны свойственна идея обновления и усовершенствования человека во время службы в армии, которая способствует улучшению отдельных сторон личности или даже ее существенной трансформации (армия «школа жизни»). Проведенный военными социологами в 2006-2010 годах анализ показывает: военная служба, по мнению молодых людей в возрасте от 18 до 35 лет, предоставляет возможность испытать себя в трудных условиях, воспитать характер, физически окрепнуть и закалиться, приобрести нужную специальность. Лишь 13,5% опрошенных считает, что служба в армии человеку ничего не дает. Существует связь между отношением к военной службе и степенью развития социальной идентичности личности. Те, кто не намерен проходить армейскую службу, ориентированы на индивидуальные ценности, связанные преимущественно с личной идентичностью. В противовес им, лица не пытающиеся уклониться от военной службы, руководствуются широкими социальными мотивами, отражающими развитую социальную идентичность. Исследователями отмечается, что кризис ценностей в российском обществе, углубив закономерный юношеский кризис идентичности, вызывает кризис жизненного самоопределения молодежи как социальной группы. В период социальной неустойчивости разрушаются «МЫ-концепции», а вместе с ними личностные и социальные идентификации. Эта проблема приобретает особую значимость, когда речь идет о кризисе гражданско-государственной идентичности у молодежи, о неразвитости ее гражданского сознания. По данным всероссийского социологического мониторинга «Социальное развитие молодежи», проведенного Центром социологии молодежи ИСПИ РАН, гордятся своей страной только 33%, не видят оснований для гордости 54% молодых людей. Для современной молодежи гражданство идентифицируется только с формальной принадлежностью к государству.

Социальная идентичность, согласно теории известных западных социальных психологов Г. Тэджфела и Дж. Тернера является главным объяснительным принципом социального поведения им межгруппового взаимодействия в обществе. *В настоящее время молодежь не включает себя в* ***образ государства*** *в своем собственном сознании* и как следствие этого не идентифицирует себя и с защитником Родины. Что приводит к отрицательному восприятию этноса, государства и одного из его атрибутов – Вооруженных Сил.

Анализ социологических исследований приводит к выводу: *молодежью отрицательно воспринимаются не столько сами Вооруженные Силы, сколько перспектива служить в них.* Надо признать, что без сформированного позитивного образа страны, в котором присутствует идея **державности,** граждане современной России не смогут закрепить свою национальную идентичность. Такой образ необходим и для установления и поддержания благоприятных внешних контактов государства.

Согласно социологическим исследованиям проведенным в 2010-2011г.г. на военной кафедре СПб ГУ ИТМО мы можем выделить безусловно положительную тенденцию к снижению количества студентов, мотивом поступления на военную кафедру для которых является попытка уклонения от службы в ВС РФ. В то же время согласились с перспективой пройти военную службу в армии на офицерских должностях не более 8% от обучающихся на военной кафедре СПб ГУ ИТМО. Незначительная часть (2,73%) наиболее подходящим для себя считают прохождение военной службы по призыву сроком 12 месяцев на первичных должностях рядового состава. В то же время для каждого третьего из числа поступивших на военную кафедру, служба в

Вооруженных силах - нежелательная необходимость. А каждый четвертый еще не определил своего отношения к военной службе вообще и в кадрах Вооруженных Сил в частности. Получение офицерской профессии рассматривается скорее как вторая (запасная) специальность, которая позволит проходить военную службу в наиболее «комфортных» условиях, если призыв на военную службу станет реальностью. Конечно, при этом надо учитывать, что не все студенты, поступившие на военную кафедру, стремятся стать именно кадровыми офицерами. Они хотят получить, прежде всего, престижную гражданскую специальность, иначе они поступали бы в военное образовательное учреждение. Но существует и пятая категория обучающихся на военной кафедре. Это те, кто, не желая проходить военную службу, желает поступить на службу в органы (11,4%) где предусмотрена **служба по льготам** *приравненная к военной*, однако не связанная с ее тяготами и лишениями. В то же время среди реально столкнувшихся с этими «тяготами и лишениями» в процессе военных сборов проводимых ежегодно в войсках Западного военного округа уже 53,6% студентов считают эти «трудности» преодолимыми и с большим оптимизмом смотрят на саму службу и предлагаемые условия службы в войсках.

Все это позволяет сделать вывод: элемент державности в системе патриотических ценностей молодежи обучающейся на военной кафедре может и должен стать опорой в воспитании патриотов своего Отечества, позволяет вести работу по пропаганде военной службы в новом ее виде, *в виде рекламы прочно вошедшей в наше время в сознание молодежи.* Причем рекламу военной службы следует проводить во всех ее формах, а не только по контракту. При этом рекламный и пропагандистский материал должен опираться на широкие социальные и средние корпоративные мотивы. Кроме того необходимо показывать молодежи, что служба в армии способствует удовлетворению целого спектра узколичностных мотивов человека. Таких как получение (совершенствование) специальности, испытание и развитие себя, приобщение к современной технике, принадлежность к особой корпорации, составляющей гордость государства и общества (Спецназ, военная разведка, десант проч.). В этом смысле идея «державности» является источником для преодоления кризиса самоиндетификации в сознания современной молодежи, осознания молодыми людьми себя не жителями «ЭТОЙ» страны, а гражданами и частью Великой Державы живущими с ней одной жизнью, разделяющими ее великие и повседневные заботы, готовыми ради нее и на труд и на подвиг.

Литература

1. Орлов И.Б. Державность в современной политической культуре: история и современность. – М. : ГУ-ВШЭ, 2006.

2. Белошев В.А., Рыжков А.В. Элемент «Державности» в системе патриотических ценностей, студентов обучающихся на военной кафедре СПб ГУ ИТМО, Материалы XL научной и учебно-методической конференции. – СПб : СПбГУ ИТМО, 2011.

УДК 355.54

ПРАВОВЫЕ ОСНОВЫ ОСУЩЕСТВЛЕНИЯ ПЕДАГОГИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ГРАЖДАНСКИМ ПЕРСОНАЛОМ ВОЕННЫХ КАФЕДР

Березовский С.А., Красильников Н.И.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Задачей настоящей статьи является исследование особенностей правового регулирования трудовой деятельности гражданским персоналом военных кафедр, осуществляющих педагогическую деятельность в образовательных учреждениях высшего профессионального образования.

Правовые основы осуществления педагогической деятельности гражданским персоналом военной кафедры.

Основным документом, регулирующим трудовые отношения в нашей стране, является трудовой кодекс Российской Федерации (ТК РФ).

Особенности права на осуществление педагогической деятельности и приема на работу педагогических работников регулирует гл. 52 ТК РФ.

В соответствии с п. 1 ст. 20 Федерального закона «О высшем и послевузовском профессиональном образовании» в вузах предусматриваются должности научно-педагогического (профессорско-преподавательский состав, научные работники), инженерно-технического, административно-хозяйственного, производственного, учебно-вспомогательного и иного персонала.

К профессорско-преподавательским должностям относят должности декана факультета, заведующего кафедрой, профессора, доцента, старшего преподавателя, преподавателя, ассистента. К категории «научные работники» относятся граждане, обладающие необходимой квалификацией и профессионально занимающиеся научной и (или) научно-технической деятельностью. Конкретизирует понятие научного работника Положение о порядке замещения должностей научно-педагогических работников в вузе Российской Федерации, утвержденное приказом Министра образования Российской Федерации от 26.11.2002 г. № 4114, устанавливающее, что такими работниками являются лица, занимающие следующие должности: руководитель научно-исследовательского, научного сектора, отдела, лаборатории, другого научного подразделения, главный научный сотрудник, ведущий научный сотрудник, старший научный сотрудник, научный сотрудник, младший научный сотрудник.

К особенностям правового регулирования труда педагогических работников (в том числе и гражданского персонала военной кафедры) относятся некоторые ограничения в приеме на работу лиц, установленные ст. 331 ТК РФ. Так, к педагогической деятельности не допускаются лица:

– лишенные права заниматься педагогической деятельностью в соответствии с вступившим в законную силу приговором суда;

– имеющие или имевшие судимость, подвергающиеся или подвергшиеся уголовному преследованию (за исключением лиц, уголовное преследование в отношении которых прекращено по реабилитирующим обстоятельствам) за преступления против жизни и здоровья,

свободы, чести и достоинства личности (за исключением незаконного помещения в психиатрический стационар, клеветы и оскорбления), половой неприкосновенности и половой свободы личности, против семьи и несовершеннолетних, здоровья населения и общественной нравственности, а также против общественной безопасности;

– имеющие неснятую или непогашенную судимость за умышленные тяжкие и особо тяжкие преступления;

– признанные недееспособными в установленном федеральным законом порядке;

– имеющие заболевания, предусмотренные перечнем, утверждаемым федеральным органом исполнительной власти, осуществляющим функции по выработке государственной политики и нормативно-правовому регулированию в области здравоохранения.

Дополнительно, к преподавательскому составу военной кафедры установлено требование, что замещение педагогических должностей на военной кафедре осуществляется гражданами, пребывающими в запасе ВС РФ и имеющие воинское звание офицера (ст. 48 Постановления правительства РФ от 6.03.2008 г. № 152 «Об обучении граждан Российской Федерации по программе военной подготовки в федеральном государственном образовательном учреждении высшего профессионального образования»).

Как и для других категорий работников, трудовые договоры на замещение должностей научно-педагогических работников в вузе могут заключаться как на неопределенный срок, так и на срок, определенный сторонами трудового договора.

Заключению трудового договора на замещение должности научно-педагогического работника предшествует избрание по конкурсу на заключение соответствующей должности, заключение с педагогическим работником договора на неопределенный срок предполагает проведение конкурса на замещение его должности 1 раз в 5 лет (ст. 332 ТК РФ).

В целях сохранения непрерывности учебного процесса, допускается заключение трудового договора на замещение должности научно-педагогического работника в высшем учебном заведении без избрания по конкурсу на замещение соответствующей должности при приеме на работу по совместительству или в создаваемые высшие учебные заведения до начала работы ученого совета – на срок не более 1 года, а для замещения временно отсутствующего работника, за которым в соответствии с законом сохраняется место работы, – до выхода этого работнику на работу.

Не проводится конкурса на замещение должностей:

– декана факультета и заведующего кафедрой;

– научно-педагогических работников, занимаемых беременными женщинами;

– научно-педагогических работников, занимаемых по трудовому договору, заключенному на неопределенный срок женщинами, имеющими детей в возрасте до трех лет (ст. 322 ТК РФ).

Конкурсный отбор объявляется ректором (проректором, руководителем филиала) вуза в периодической печати или других средствах массовой информации не менее чем за 2 месяца до его проведения. Устанавливается срок подачи заявления для участия в конкурсном отборе – 1 месяц со дня опубликования объявления о конкурсе. Несвоевременная подача заявления является основанием для отказа в его принятии и соответственно для участия в конкурсе.

Если работник, занимающий должность научно-педагогического работника по трудовому договору, заключенному на неопределенный срок, по результатам конкурса, предусмотренного п. 4.3 ст. 332 ТК РФ, не избран на должность или не изъявил желания участвовать в указанном конкурсе, то трудовой договор с ним прекращается в соответствии с п. 4 ст. 336 ТК РФ (дополнительные основания прекращения трудового договора только для научных и педагогических работников).

При избрании работника по конкурсу на замещение ранее занимаемой им по срочному трудовому договору должности научно-педагогического работника новый трудовой договор может не заключаться. В этом случае действие срочного трудового договора с работником продлевается по соглашению сторон, заключаемому в письменной форме, на определенный срок – не более 5 лет или на неопределенный срок.

Должности декана факультета и заведующего кафедрой являются выборными. Порядок проведения выборов на указанные должности устанавливается уставами высших учебных заведений.

Пункт 88 Типового положения об образовательном учреждении высшего профессионального образования (утверждено Постановлением Правительства Российской Федерации от 14.02.2008 г. № 71) предусматривает, что увольнение педагогических работников по инициативе администрации высшего учебного заведения в связи с сокращением штатов допускается только после окончания учебного года.

В соответствии со ст. 333 ТК РФ для педагогических работников устанавливается сокращенная продолжительность рабочего времени – не более 36 часов в неделю.

Специфичность фиксации и оценки трудовой деятельности педагогических работников закреплена Положением об особенностях режима рабочего времени и времени отдыха педагогических и других работников образовательных учреждений (утверждена приказом Министра образования и науки Российской Федерации от 27.03.2006 г. № 69), которое определяет, что нормируемая часть рабочего времени работников, ведущих преподавательскую работу, определяется в астрономических часах и включает проводимые учебные занятия независимо от их продолжительности и короткие перерывы (перемены) между каждым учебным занятием. При этом количеству часов установленной учебной нагрузки соответствует количество проводимых указанными работниками учебных занятий продолжительностью, не превышающей 45 минут.

Конкретная продолжительность учебных занятий, а также перерывов между ними предусматривается уставом образовательного учреждения.

Режим рабочего времени работников из числа профессорско-преподавательского состава вузов в пределах 36-часовой рабочей недели определяется с учетом выполнения преподавательской работы, а также осуществления:

- научно-исследовательской;
- творческо-исполнительской;
- опытно-конструкторской;
- учебно-методической;
- организационно-методической;

- воспитательной;
- физкультурной;
- спортивно-оздоровительной работы.

Режим выполнения преподавательской работы регулируется расписанием учебных занятий. Основным показателем является учебная нагрузка профессорско-преподавательского состава вузов. Учебная нагрузка для военнослужащих и гражданского персонала, замещающих должности профессорско-преподавательского состава, устанавливается нормативными правовыми актами федеральных органов в зависимости от их квалификации и профиля кафедры в размере до 900 часов в учебном году (п. 29 Типового положения, утвержденного Постановлением Правительства Российской Федерации от 31.01.2009 г. № 82).

Нормы времени для расчета объема учебной работы и основных видов учебно-методической и других работ, выполняемых профессорско-преподавательским составом, устанавливает письмо Министра образования Российской Федерации от 26.06.2003 г. № 14-55-784 ин/15, а также ученый совет вуза.

Ежегодный основной оплачиваемый отпуск педагогических работников вузов является удлиненным и составляет 56 суток.

В соответствии со ст. 335 ТК РФ педагогические работники не реже, чем через каждые 10 лет непрерывной преподавательской работы имеют право на длительный отпуск сроком до 1 года, порядок и условия предоставления которого определяются приказом Министра образования Российской Федерации «Об утверждении Положения о порядке и условиях предоставления педагогическим работникам образовательных учреждений длительного отпуска сроком до 1 года от 7.12.2000 г. № 3570.

Таким образом, к особенностям правового регулирования трудовой деятельности гражданского персонала, замещающего должности педагогических работников военных кафедр относятся регулирование педагогической деятельности нормативными актами Министерства образования и науки Российской Федерации.

Литература

1. Трудовой кодекс Российской Федерации.
2. Федеральный закон «О высшем и послевузовском профессиональном образовании».
3. Положение о порядке замещения должностей научно-педагогических работников в вузе Российской Федерации (приказ Министра образования Российской Федерации от 26.11.2002 г. № 4114).
4. Постановление правительства Российской Федерации от 6.03.2008 г. № 152 «Об обучении граждан Российской Федерации по программе военной подготовки в федеральных государственных образовательных учреждениях высшего профессионального образования».
5. Постановление правительства Российской Федерации от 14.02.2008 г. № 71 «Типовое положение об образовательном учреждении высшего профессионального образования».
6. Положение об особенностях режима рабочего времени и времени отдыха педагогических и других работников образовательных учреждений (приказ Министра образования и науки Российской Федерации от 27.03.2006 г. № 69).

7. Примерные нормы времени для расчета объема учебной работы и основные виды учебно-методической, научно-исследовательской и других работ, выполняемые профессорско-преподавательским составом в образовательных учреждениях высшего и дополнительного профессионального образования (письмо Министра образования Российской Федерации от 26.06.2003 г. № 14-55-784 ин/15).

8. Приказ Министра образования Российской Федерации от 7.12.2000 г. № 3570 «Об утверждении Положения о порядке и условиях предоставления педагогическим работникам образовательных учреждений длительного отпуска сроком до 1 года.

ВЛИЯНИЕ СОВРЕМЕННОГО ИНФОРМАЦИОННОГО ОБЩЕСТВА НА КАЧЕСТВЕННОЕ ОБРАЗОВАНИЕ

Гавриш В.М.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Статья отражает значимость влияния информационного общества на качественное образование. Стремительное развитие новых информационных технологий предъявляет новые требования к образованию. Современный процесс обучения стал неразрывно связан с развитием информационных и коммуникационных технологий, без которых качественное образование становится невозможным. И не учитывать измененния современных реалий нельзя.

УДК 355.54

К ВОПРОСУ О КОМПЛЕКСНОМ ПОДХОДЕ В ПОДГОТОВКЕ СТУДЕНТОВ НА ВОЕННОЙ КАФЕДРЕ

Гончаров А.Д.[1], **Морозов В.В.**[2]

[1)] *Санкт-Петербургский государственный университет информационных технологий, механики и оптики*

[2)] *Михайловская военная артиллерийская академия*

Педагогическая система вуза, являясь основой образовательного процесса подготовки специалиста, системно отражает цель, содержание, принципы, формы, методы и средства деятельности руководящего, преподавательского, научного и административного состава вуза по организации и ведению учебной, методической, воспитательной и научной работы, контролю и оценке уровня подготовленности студентов.

Анализ основных педагогических понятий позволяет сделать следующие выводы. Во-первых, что педагогическая система – это целевая система обучения и воспитания, где решаются конкретные педагогические задачи. Во-вторых, в основе педагогической системы лежат цель, содержание, формы, методы и средства деятельности (организаторской, учебной, методической,

воспитательной), которые обусловливают определенные действия преподавателей и обучающихся по овладению методами и средствами будущей профессиональной деятельности. В-третьих, педагогическая система – это «система-процесс», в которой осуществляется формирование личности будущего специалиста с заданными качествами.

Основными элементами педагогической системы являются:

- обучающие – руководящий и преподавательский состав;
- обучающиеся – студенты вуза;
- цель подготовки специалиста и требования к уровню его подготовленности;
- содержание образования, как определенное количество задач обучения, воспитания и развития будущего специалиста;
- принципы, формы, методы и средства обучения и воспитания студентов, контроля и оценки их подготовленности.

Рассмотрим сущность основных структурных элементов педагогической системы с точки зрения комплексного подхода и принципы их взаимодействия в процессе обучения и воспитания студентов на военной кафедре.

Обучающие – субъекты системы, в функции которых входит планирование, организация, ведение, контроль, оценка учебной, методической, научной и воспитательной работы и обеспечение образовательного процесса. Ответственность, обязанности и права должностных лиц руководящего и преподавательского состава определяются действующим законодательством Российской Федерации, постановлениями правительства РФ и нормативными документами, утверждаемыми ректором вуза. Необходимо особо отметить, что уровень профессионализма преподавателей является решающим условием качества и эффективности образовательного процесса и соответственно результативности педагогической системы.

Обучающиеся – объект системы. Студенты в соответствии с профессиональными образовательными программами в рамках педагогической системы овладевают знаниями, навыками и умениями будущей профессиональной деятельности, приобретают и развивают необходимые личностные качества. Учебная деятельность студентов в ходе образовательного процесса максимально должна приближаться к условиям профессиональной деятельности военного специалиста.

Цель подготовки военного специалиста и требования к уровню его подготовленности определяют основные количественные и качественные показатели и критерии, в соответствии с которыми должен быть организован образовательный процесс и по которым должны оцениваться его результаты. Указанный элемент педагогической системы является системообразующим и предопределяет содержание образования, задачи, формы, методы и средства учебной, методической и научной работы военной кафедры и преподавателей. Уяснение педагогами и студентами цели подготовки специалиста и требований к уровню его подготовленности, на наш взгляд, делает образовательный процесс целенаправленным на конкретные результаты, активным и интенсивным, а учебная деятельность носит творческий характер. Это позволяет коллективу преподавателей военной кафедры избегать шаблона, стереотипов в обучении и в полном объеме реализовать принципы научности и перспективности в подготовке военного специалиста.

Содержание образования составляет основу профессиональных образовательных программ, в соответствии с которыми формируются задачи учебной, методической и научной работы военной кафедры. Ими определяется логика и взаимосвязи учебных дисциплин, на основе чего реализуется комплексный подход в подготовке военного специалиста, выбираются формы и средства учебной деятельности. При этом содержание образования для студентов определяется в соответствии с квалификационными требованиями. Содержание, на наш взгляд, должно быть построено таким образом, чтобы оно отражало достигнутый уровень науки и служило основой теоретической, практической и психологической подготовки студента к будущей профессиональной деятельности.

Принципы, формы, методы и средства обучения и воспитания студентов, контроля, оценки их успеваемости и подготовленности образуют «инструмент» технологии подготовки военного специалиста, а в единстве с формами и методами деятельности руководящего и преподавательского состава по планированию и организации образовательного процесса – педагогическую технологию.

Результатом функционирования каждой педагогической системы подготовки специалиста в вузе является уровень знаний, навыков, умений, сформированности качеств личности студентов.

Следовательно, уровень знаний, навыков и умений студентов, как и любой другой, на наш взгляд должен характеризоваться минимальным количеством показателей, критериев и в то же время отвечать требованиям достаточной объективности. В противном случае контроль и оценка результатов обучения и воспитания, учебной деятельности преподавателей и студентовстановится громоздкой, трудоемкой, а самое главное, не понятной для обучающихся, что не позволяет им своевременно регулировать процесс самообразования.

Кроме того необходимо отметить, что переход вузов к подготовке специалистов по новым профессиональным образовательным программам предполагает не только знание основных принципов организации и ведения образовательного процесса, но и практические умения системного и комплексного решения частных, но взаимосвязанных задач подготовки специалиста – обучения, воспитания и развития.

Всю совокупность принципов создания педагогических систем на наш взгляд можно условно (по признаку вида деятельности) разделить на три группы.

Первая группа объединяет принципы организаторской деятельности руководящего, преподавательского, научного и административного состава вуза, реализация которых приводит к созданию определенной целевой системы подготовки специалиста. Предметным выражением реализации этих принципов является деятельность по проектированию образовательного процесса, а конечным результатом – профессиональная образовательная программа подготовки специалиста в вузе.

Такими основными принципами являются:

– принцип диагностичности цели подготовки (зачем учить), содержания образования (чему учить), уровня подготовленности выпускника вуза (какой уровень квалификации обеспечить) и организации обучения (как учить);

– принцип соответствия квалификационных требований к уровню подготовленности выпускника вуза, бюджету учебного времени, цели подготовки, содержанию образования и возможностям по обеспечению образовательного процесса;

– принцип главного звена и достаточного основания в планировании и организации образовательного процесса;

– принцип рационализма в разделении полномочий (ответственности, обязанностей и прав) должностных лиц при формировании цели, содержания, выборе форм, методов и средств организации и ведения образовательного процесса;

– принцип перспективности в планировании подготовки специалиста;

– принцип оптимальности логики и междисциплинарных связей образовательного процесса.

Вторая группа принципов предопределяет ведение образовательного процесса, то есть, собственно принципы обучения, которые определяют функционирование целевой педагогической системы подготовки специалиста. К ним относятся:

– принцип научности, профессионализма и фундаментальности в подготовке специалиста;
– принцип активности, самостоятельности и сознательности в обучении;
– принцип систематичности, последовательности и наглядности в обучении;
– обучение на требуемом уровне трудностей;
– прочность в овладении знаниями, навыками и умениями военной специальности;
– самообучение, самоконтроль, самооценка и личная ответственность студента за уровень подготовленности;
– коллективизм и индивидуальный подход в подготовке специалиста.

Третья группа принципов охватывает деятельность руководящего и преподавательского состава по непосредственному руководству образовательным процессом в целом и его главными частями – учебной, методической, научной и воспитательной работой.

К ним можно отнести:

– принцип адресности и диагностичности задач учебной, методической, научной и воспитательной работы военной кафедры, преподавателя;

– принцип рациональности в обеспечении образовательного процесса;

– принцип объективности в контроле, оценке и учете уровня успеваемости и подготовленности студентов;

– принцип оперативности в принятии решений и их выполнении по регулированию (корректированию) образовательного процесса.

На практике реализация указанных принципов позволяет прийти к стройной системе управления вузом и к стабильности в организации учебной деятельности, к требуемой результативности процесса подготовки специалиста.

Рассмотренные принципы тесно взаимосвязаны, взаимообусловлены и предполагают определенные формы, методы и средства деятельности по организации и ведению образовательного процесса, то есть педагогическую технологию.

Современная педагогическая технология на наш взгляд должна представлять собой совокупность процессов определения (оптимизации) и реализации в образовательном процессе

подготовки специалиста, цели обучения (для чего учить), содержания обучения (чему учить), форм и методов обучения (как учить).

Структурно педагогическая технология как процесс деятельности руководящего, преподавательского и административного состава военной кафедры включает технологию проектирования образовательного процесса (порядок подготовки и проведения учебных занятий, контроля и оценки успеваемости студентов, контроля и оценки качества занятий, других мероприятий учебной, методической, научной и воспитательной работы).

Предметным выражением единства технологии проектирования образовательного процесса и технологии обучения является структурно-логическая схема подготовки студентов разработанная на кафедре разведки и соответствующая ей система видов учебных занятий. Такая технология реализует логику подготовки специалиста и оптимизирует междисциплинарные связи учебных дисциплин, как по времени, так и по виду и месту проведения занятий.

Педагогическая технология в педагогической системе отражает структуру и динамику учебной деятельности, и ее результаты. Вот почему учебный план подготовки специалиста должен связывать единой целевой установкой комплект учебных программ, чтобы в итоге обучения можно было определить уровни обученности. Такими уровнями являются:

- о чем обучающийся должен иметь представление;
- что обучающийся должен знать и уметь использовать;
- какими навыками и умениями обучающийся должен владеть;
- какой опыт (навык, умение) в какой деятельности обучающийся должен иметь.

Таким образом, рассмотренный подход к формированию целевых установок учебных дисциплин и квалификационных требований на наш взгляд позволяет преподавательскому составу дифференцированно подходить к определению целей занятий (учебных и воспитательных), а руководящему составу максимально объективно осуществлять оценку хода и результатов обучения, прогнозировать уровень подготовленности выпускника, и при необходимости, корректировать образовательный процесс.

Здесь же необходимо отметить, что на современном этапе образовательный процесс необходимо строить на основе традиционных и новых форм, методов и средств активного обучения, содержащий определенное количество учебных задач – моделей, выраженных на языке знаковых средств предметного и социального содержания будущей профессиональной деятельности выпускника на первичных офицерских должностях. В этом случае педагогическая система подготовки специалиста претерпевает существенные изменения. Эти изменения обусловлены следующим.

Во-первых, модель учебной деятельности содержит предметную и социальную составляющие профессиональной деятельности специалиста, а не модель процесса обучения, то есть в модели содержатся ситуации профессионального действия, требующие интеллектуальной или физической деятельности обучающегося. Он воспринимает не готовые алгоритмы, правила, способы, а пытается найти их.

Во-вторых, требования к обучающемуся становятся системообразующими и задают новый принцип построения целевой педагогической системы, как системы, нацеленной на выполнение квалификационных требований.

В-третьих, субъект обучения студент в этой системе занимает деятельную позицию, предметом которой являются профессиональные действия.

В заключении необходимо отметить, комплексное и системное применение рассмотренных методов и особенностей педагогических систем позволяет спроектировать процесс учебной деятельности на основе диагностических и реально достигаемых целей подготовки военного специалиста, оптимизировать содержание образования и соответствующую ему систему видов учебных занятий. Это позволяет успешно решить задачи обучения, воспитания и развития будущего специалиста – военного профессионала.

Литература

1. Закон РФ «Об образовании» от 10 июля 1992 года № 3266-1.

2. Постановление Правительства РФ от 06.03.2008 №152 «Об обучении граждан российской федерации по программе военной подготовки в федеральных государственных образовательных учреждениях высшего профессионального образования».

3. Совместный приказ Министра обороны Российской Федерации и Министерства образования и науки Российской Федерации № 666/249 от 10 июля 2009 г. «Об организации деятельности учебных военных центров, факультетов военного обучения и военных кафедр при федеральных государственных образовательных учреждениях высшего профессионального образования».

УДК 355.54

ОСНОВНЫЕ НАПРАВЛЕНИЯ РАБОТЫ КОЛЛЕКТИВА ПРЕПОДАВАТЕЛЕЙ ВОЕННОЙ КАФЕДРЫ

Громов А.В.[1], **Морозов В.В.**[2]

[1)] *Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики*

[2)] *Михайловская военная артиллерийская академия*

Главной задачей в работе педагога, возглавляющего один из коллективов кафедры, является создание, прежде всего, дружного коллектива преподавателей. Достижение этой цели предусматривает учет старшим коллектива конкретных возможностей каждого преподавателя: его жизненного, служебного и боевого опыта, теоретических и практических знаний и навыков, педагогического опыта, склонностей к этой области деятельности, умственных и физических способностей, особенностей характера и других моментов, характеризующих его, как офицера и человека.

Рассмотрим основные направления работы коллектива.

Первое направление – достижение единства понимания всех главных и второстепенных вопросов по курсу, преподаваемому коллективом. Насколько это важно нет необходимости много говорить: разнобой в трактовке учебных вопросов в большом и малом привел бы к хаосу в

знаниях, запутал обучающихся и естественно недопустим, тем более, что к итоговой аттестации исправить что-либо существенное трудно.

Для достижения такого единства преподаватели коллектива по указанию старшего посещают его лекции. Перед каждым практическим занятием старший коллектива проводит инструкторско-методические совещания, на которых даются единые установки в изложении, рассмотрении по существу вопросов, выносимых на занятие. Эта кропотливая и напряженная работа ведется из года в год не только на инструкторско-методических совещаниях, но и ежедневно. У преподавателей коллектива в ходе подготовки к занятиям появляется множество дополнительных вопросов, которые по разным причинам могли и не рассматриваться ранее, в том числе на инструкторско-методических совещаниях. Возникает, в связи с этим, необходимость индивидуальной работы с преподавателями, быстрой и правильной реакции со стороны старшего коллектива.

Достижение единства понимания и изложения вопросов продолжается и в перерывах между занятиями, когда происходит короткий обмен мнениями между преподавателями, а после проведения соответствующего занятия – во время подведения его итога в коллективе.

Особо следует подчеркнуть значение в решении рассматриваемой задачи качественной разработки учебных материалов.

Лекции в коллективе читают доценты и старшие преподаватели.

Они разрабатывают их содержание, оформляют, готовят дидактический материал, если можно так выразиться, работают по принципу – я один. Однако старший курсового коллектива изучает весь материал лекций, дает необходимые советы и указания автору. По согласованию с командованием кафедры подготовленные материалы лекции, если необходимо, выносятся на обсуждение в ходе заседаний кафедры.

Необходимо стремиться, чтобы во всех учебных материалах, разрабатываемых коллективом, была четко и на современном уровне изложена точка зрения во всем основным вопросам. В достижении единства понимания это имеет очень большое значение. Однако учебно-методические материалы (УММ) издаются не на один год, а проводятся два-три года. Каждый год, а иногда и через полгода необходимо вносить изменения. Такова динамика жизни, такова относительная устойчивость материалов, издаваемых по военным вопросам, проверенная многими годами. В этой обстановке нужно стремиться учебные материалы по их содержанию разрабатывать так, чтобы главные, стержневые положения оставались незыблемыми и, вместе с тем, правильными в течение большого срока, значительно превышающего переиздание (УММ). Здесь требуется предвидение коллектива, его ответственность и в первую очередь старшего, который осуществляет контроль за содержанием всех разрабатываемых материалов.

Каждый преподаватель, естественно, должен много работать лично. Контроль занятий, проводимый руководством кафедры и старшим коллектива, дает возможность убедиться насколько преподаватели не только едино понимают, но и излагают на занятиях главные и даже второстепенные вопросы по курсу, преподаваемому коллективом.

Второе направление – достижение высокого методического уровня проведения занятий каждым преподавателем коллектива.

Помощь в решении этой задачи оказывает методическая разработка, подготовленная опытными преподавателями на кафедре. Однако методика проведения каждого занятия закладывается при разработке задачи и отражается в методических разработках. Жизнь идет вперед, накапливается опыт и возникает необходимость всегда перед каждым занятием (за 2-3 дня) провести инструкторско-методическое совещание, на котором, как уже указывалось, рассмотреть вопросы занятия по существу с целью единства их понимания и методику их отработки. При этом старший коллектива должен добиться, чтобы эта методика была единой у всех преподавателей и, вместе с тем, не стиралась индивидуальность преподавателя, его лицо. Поэтому методика должна быть единой по всему занятию, отработке главных вопросов, но не обязательно охватывать все нюансы и оттенки, при которых преподаватель может и должен проявить свое творчество.

На инструкторско-методическом совещании дается также принципиальное распределение времени, отводимого на каждый вопрос, имея в виду, что, в зависимости от уровня подготовки учебного отделения, это время может колебаться в ту или иную сторону в некоторых пределах, но весь комплекс вопросов занятия, безусловно, должен быть отработан в отведенное время.

Если содержание вопросов занятия достаточно хорошо изучено преподавателями по учебным материалам и старший коллектива убедился в этом в ходе индивидуальной работы с преподавателями, тогда на инструкторско-методическом совещании он может сосредоточить все свое внимание только на методике проведения занятия.

Полезно приглашать преподавателей на занятия, проводимые старшим коллектива и другими опытными методистами. Такие посещения дают возможность конкретно, на практике увидеть в ходе занятия воплощение тех установок, в том числе методических, которые были даны на инструкторско-методическом совещании.

Совершенствованию методического мастерства предела нет, поэтому при подведении итогов проведенных занятий в коллективе обязательно надо обменяться опытом и выяснить, что в методике всего занятия и по отдельным вопросам было хорошо и что требует исправления или уточнения. Положительный опыт необходимо сразу фиксировать в методических разработках и личных планах проведения занятия, делая соответствующие записи для последующих занятий.

Выслушав мнения товарищей, старший коллектива должен указать разработчику задачи в какой формулировке и в каких материалах сделать исправления на будущее.

В методике проведения каждого практического занятия обязательно предусматривать выработку у обучаемых одного-двух, иногда нескольких навыков. Это определяется темой занятия и его продолжительностью.

Третье направление – достижение высокого идейно-нравственного уровня преподавания.

Решение этой задачи предусматривает, как разумеющееся, высокие идейно-нравственные качества самого преподавателя, успешное овладение им вопросами в системе командирской подготовки, профессиональную компетентность, методическое мастерство. Дополнительно к этому, в коллективе предусматривается в учебных материалах и во время инструкторско-методических совещаний отражать решения высших государственных лиц и органов, требования приказов Министра обороны и директив начальника Генерального штаба Вооруженных Сил, опыт

Великой Отечественной войны, послевоенных учений, опыт локальных войн и военных конфликтов.

Мы стремимся к тому, чтобы они логично вплетались в ткань любого занятия, воспитывали в студентах преданных защитников Родины, убеждали их в возможности решать сложные задачи по разгрому сильного, хитрого и коварного противника с применением вооружения и боевой техники, приборов, и аппаратуры, которые имеются в вооруженных силах.

Достижению идейно-нравственного воспитания студентов и в целом применение всего комплекса мер по их обучению и воспитанию имеет большое значение знание их индивидуальных качеств – индивидуализация обучения. Такие данные о студентах имеются на основе систематического многократного их социально-психологического обследования и сопровождения методом тестирования и наблюдения в учебно-воспитательном процессе.

Такая работа выполняется группой профессионально-психологического отбора по научно разработанным методикам, опробованным в течение многих лет в нашем учебном заведении. Эти методики признаны и используются также в других вузах РФ. Они получили высокую оценку на научных конференциях психологов и социологов в масштабе страны и СНГ.

Достижению высокого идейно-нравственного преподавания содействует хорошая связь с учебными подразделениями вуза, которую должен поддерживать коллектив преподавателей.

Четвертое направление – подготовка начинающих преподавателей с целью быстрого ввода их в строй действующих. Эта задача является важнейшей, поскольку коллектив без ее решения не сможет эффективно выполнять задачу по обучению и воспитанию студентов.

Начинающий преподаватель (хотя по возрасту он может быть весьма солидным человеком в том числе и с большой войсковой практикой) в максимально короткий срок должен изучить весь курс кафедры, а не только коллектива, в который он включен, овладеть методическим мастерством, подготовиться к выполнению на первых порах хотя бы простейших вопросов в ВНР и НИР.

Период подготовки начинающего преподавателя до выпуска его на самостоятельное проведение занятия, по нашему опыту, не превышает половины года. Выходу на самостоятельное проведение занятия всегда предшествует пробное занятие начинающего преподавателя в коллективе, а затем – неоднократные посещения всем личным составом кафедры открытых занятий начинающего преподавателя. При соответствующей подготовке начинающего преподавателя, с учетом его качеств, не следует слишком растягивать срок ввода его в строй, имея в виду, что под тяжестью ответственности люди быстрее растут. Не стоит скроить также и иллюзий. Пока человек не проведет каждое занятие минимум 5–6 раз он еще не чувствует на нем себя уверенно. Поскольку занятий у коллектива по тематике и числу комплексных задач достаточно много, то о становлении молодого преподавателя можно говорить не ранее, чем через 2-3 года.

Привитие любви к профессии и к обучающимся, к предмету, который преподаватель ведет, к тяжелому и очень кропотливому труду по обучению студентов, чтобы все это делалось от души, страстно и убежденно – важные вопросы, которым в коллективе должно уделяться большое внимание.

Пятое направление – обеспечение качественного выполнения военно-научных и научно-исследовательских задач.

Исполнители ВНР и НИР кафедральных и комплексных (с участием других кафедр, учреждений и заведений) находятся в педагогическом коллективе. Старшему коллектива необходимо регулировать их рабочее время таким образом, что они успешно выполняли учебную и научную работу с высоким качеством. К тому же в ходе выполнения ВНР и НИР возникает, по сути дела ежедневно, множество вопросов у исполнителей, которые разрешаются в рабочем порядке в коллективе и прежде всего с его руководителем. Таким образом, самими обстоятельствами, которые являются объективными, коллектив участвует в выполнении каждой научной работы.

Участие преподавателя в научной работе необходимо – это залог того, что и в учебной работе он будет трудиться успешно. Истина простая и давно известная. Поэтому сочетание учебной и научной деятельности преподавателей в коллективе – одна из важных сторон его жизни и качественной работы, его профессионального роста.

Шестое направление – совершенствование учебно-материальной базы кафедры, рационализаторская и изобретательская работа.

Это направление работы коллектива тесно связано с предыдущими, однако о нем стоит говорить отдельно, поскольку оно материально воплощается в обучающих устройствах, стендах, макетах, конструкциях, приспособлениях и т.п.

На кафедре существует распределение ответственности за оборудование и постоянное обновление классов и аудиторий. Разработка (выбор) идей и подготовка всей документации ведется в коллективах под руководством старшего. Создание образцов – это работа отдела УТ и ТА кафедры при непосредственном участии преподавателя – автора.

В ходе этих работ, попутно, рождаются рационализаторские предложения. Иногда это целенаправленное действие преподавателя.

Седьмое направление – разработка программ, тематических планов, распределение нагрузки между преподавателями на год и по семестрам.

Эта работа, в основном, старшего коллектива. По необходимости он привлекает преподавателей коллектива. Однако такое привлечение главным образом для обсуждения того, что им уже разработано перед представлением командованию кафедры или вынесением на заседание кафедры.

Из краткого рассмотрения основных направлений работы можно сделать вывод, что они охватывают, практически, все сферы его жизни и деятельности, вплоть до административных (отпуска,дисцпиплина и т.п.). Создание благоприятного «климата» в коллективе также одна из важнейших обязанностей старшего коллектива. Только при этих условиях возможно успешное функционирование коллектива, выполнение сложных и многообразных задач, стоящих перед ним.

Литература

1. Закон РФ «Об образовании» от 10 июля 1992 года № 3266-1.

2. Постановление Правительства РФ от 06.03.2008 № 152 «Об обучении граждан российской федерации по программе военной подготовки в федеральных государственных образовательных учреждениях высшего профессионального образования».

3. Совместный приказ Министра обороны Российской Федерации и Министерства образования и науки Российской Федерации № 666/249 от10 июля 2009 г. «Об организации деятельности учебных военных центров, факультетов военного обучения и военных кафедр при федеральных государственных образовательных учреждениях высшего профессионального образования».

УДК 004

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ПОЛЕТОВ ГРАЖДАНСКИХ ВОЗДУШНЫХ СУДОВ ПРИ ИСПОЛЬЗОВАНИИ ПИЛОТАЖНЫХ ТРЕНАЖЕРОВ

Жохов С.В.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В настоящее время для поддержания должного уровня квалификации сотрудников гражданской авиации все шире используются авиационные тренажеры из соображений безопасности и экономических причин.

В первую очередь, тренажеры задействованы в процессе обучения, переучивания и отработки действий в чрезвычайных и сложных условиях. Для диспетчерского состава – *тренажер управления воздушным движением*, для летного состава это *пилотажный тренажер*. Наибольшее распространение получили *процедурные (Flight Procedures Training Device)* и *комплексные (Full Flight Simulator)* тренажеры.

Для начальной подготовки используется процедурный тренажер, он дает летчику изучить кабину, средства управления и последовательность действий при выполнении полета, комплексный – для приобретения летных навыков. Современный комплексный тренажер дает ощущения от полета такие же, как и реальный полет на аналогичном воздушном судне, то есть перегрузки, крены, вибрации и тому подобное.

Настоящий доклад посвящен проблемам использования и оснащенности пилотажными тренажерами. На данный момент подавляющее число тренажеров используемых в системе гражданской авиации это устаревшие, выпущенные в 80-ые года, модели не соответствующие современным международным требованиям. Тренажер сегодняшнего дня должен практически на 100% имитировать полет на воздушном судне и, по возможности, должен быть реализован функционал взаимодействия нескольких тренажеров в одном комплексе.

НУЖНЫ ЛИ НАМ УЧЕБНЫЕ ВОЕННЫЕ ЦЕНТРЫ. ПРОБЛЕМЫ ОБУЧЕНИЯ И ВОСПИТАНИЯ СТУДЕНТОВ УВЦ

Лобов Я.В.

Учебные военные центры при федеральных государственных образовательных учреждениях высшего профессионального образования созданы распоряжением Правительства Российской Федерации от 6 марта 2008 г. N 275-р «Об учебных военных центрах (УВЦ), факультетах военного обучения и военных кафедрах при федеральных государственных образовательных учреждениях высшего профессионального образования» и являлись новой формой подготовки граждан для прохождения военной службы по контракту на воинских должностях, подлежащих замещению офицерами. С 2008 года УВЦ открыты в 37 вузах страны, которые являются крупнейшими учебными и научными центрами, имеющими богатый опыт в организации и проведении военной подготовки граждан.

Совместным приказом Министра обороны РФ N 666, Минобрнауки РФ N 249 от 10.07.2009 «Об организации деятельности учебных военных центров, факультетов военного обучения и военных кафедр при федеральных государственных образовательных учреждениях высшего профессионального образования», регулируется деятельность УВЦ.

Профессорско-преподавательский состав УВЦ состоит из военнослужащих, которые направлены не на воинские должности без приостановления им военной службы. Граждане, поступившие и успешно прошедшие обучение по программе военной подготовки в учебном военном центре, признанные годными по состоянию здоровья к военной службе по контракту, должны заключать контракт о прохождении военной службы на 3 года с Министерством обороны. После окончания высшего учебного заведения выпускникам учебного военного центра, заключившим контракт, одновременно с назначением на воинскую должность должно присваивается воинское звание «лейтенант».

Что происходит в Учебных военных центрах на самом деле!? Наборы в УВЦ не производятся с 2010 уже 2 года, и не известно будут ли они в следующем 2010 году. Выпускники УВЦ вместо назначения на воинские должности, подписания контракта, и присвоения звания «лейтенант», контракт не заключают, а зачисляются в запас, с присвоением воинского звания «лейтенант запаса». А ведь это не одна тысяча бюджетных мест по всей стране, на которые федеральный бюджет ежегодно выделяет миллиарды рублей.

УВЦ в основном состоит из военнослужащих пенсионного и пред пенсионного возраста, молодых преподавателей в УВЦ не заманить низким денежным содержанием, по сравнению с преподавателями министерства обороны, она в разы меньше. Из-за отсутствия набора в УВЦ нагрузка профессорско-преподавательский состава значительно уменьшилась. Преподаватели учебной, методической, научной работой не занимаются, находятся в поисках нового места службы, с вероятной возможностью сокращения УВЦ. Что сильно сказалось на морально психологическом состоянии преподавательского состава и студентов УВЦ. Снижается мотивация воинской службы. Студенты поступившие в УВЦ для того, чтобы продолжить по окончании ВУЗа службу в вооруженных сила, не знают что им делать с выбранной специальностью. Студенты УВЦ ищут возможности перехода в военные учебные заведения где им гарантируют военную службу.

В связи с этим, и без того не высокий, уровень преподавания в Учебных военных центрах за последний год сильно упал.

Обеспечение УВЦ современной техникой находится на крайне низком уровне. Даже ведущие вузы не могут обеспечить достойной технической поддержки учебного процесса. Имеющееся оборудование в лучшем случае оставшееся в наследство от военной кафедры устарело, требует срочной замены. Технического персонала УВЦ (инженеров, техников, лаборантов) крайне недостаточно, что связано в первую очередь с низкой оплатой труда. Учебно-материальная база военных образовательных учреждений (институтов, академий) и воинских частей, недоступна для УВЦ, так как нет руководящих документов регламентирующих совместную деятельность военных и гражданских учебных заведений. Имеющееся техническая база военных учебных заведений не используется в учебном процессе Учебными военными центрами. Что касается учебно-методической литературы тут вообще полный завал, с момента образования УВЦ не пришло не одной книгоиздательской продукции, преподаватели используют собственный накопленный потенциал для проведения занятий.

Стажировки и сборы, на основании совместного приказа N 666/249, организованные со студентами УВЦ в воинских частях и учреждениях Министерства обороны, проводятся формально, так как последние не знают что делать со студентами УВЦ. И такие специалисты придут в вооруженные силы на офицерские должности, благо всех выпускников Учебных военных центров 2011 года отправили в запас.

По словам начальника Департамента образования Минобороны Екатерины Приезжевой, с 2011 г. в гражданских вузах страны по гуманитарным, инженерным и техническим профилям будут готовиться около 40% всех офицеров для Вооруженных сил. Вопрос уже решен на высочайшем уровне. На недавней коллегии Минобороны в присутствии президента РФ Дмитрия Медведева глава ведомства Анатолий Сердюков заявил, что назревшая реорганизация военного образования заключается, в частности, в том, что к обучению в военной и гражданской школе будут применяться единые подходы. На сегодняшний день изменений в лучшую сторону не произошло и не намечается. Способны ли УВЦ самостоятельно готовить полноценных специалистов для Вооруженных сил, большой вопрос. Сколько сэкономит государство отказавшись от военных учебных заведений, переложив подготовку офицеров на гражданские ВУЗы, в ущерб обороноспособности страны.

УДК 355.54

ВОСПИТАТЕЛЬНАЯ РАБОТА КАК ЭЛЕМЕНТ СОВЕРШЕНСТВОВАНИЯ ПОДГОТОВКИ НА ВОЕННОЙ КАФЕДРЕ

Рыжков А.В.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Обучение по программе военной подготовки офицеров запаса на военных кафедрах (факультетах военного обучения) при федеральных государственных образовательных

учреждениях высшего профессионального образования является одной форм добровольной подготовки граждан к военной службе.

Обучение производится методом военного дня: аудиторные занятия, самостоятельная работа, а также воспитательная и организационная работа.

С 2008 года одной из основных задач военных кафедр в соответствии с п.1 Положением о факультетах военного обучения (военных кафедрах) при федеральных государственных образовательных учреждениях высшего профессионального образования, утвержденного постановлением правительства РФ от 6 марта 2008 года №152, является и участие в проведении воспитательной работы с молодежью.

Воспитательная работа на сегодняшний день является актуальной, переживающей новое рождение проблемой.

Попытка отказаться от негативного в прошлом привела к появлению негативного в настоящем: уничтожились важные традиции, нарушилась передача опыта между поколениями. Выход из создавшейся ситуации в сфере воспитательной работы в значительной степени связан с необходимостью нового прочтения традиции воспитания, ее включения в современный образовательный процесс.

В настоящее время существуют различные позиции относительно назначения воспитательной работы. В случае традиционного подхода считается, что воспитательная работа должна быть направлена на формирование личности студента в соответствии с требуемым идеалом. В другом случае отстаивается взгляд на студента как на сложившуюся личность, которая не нуждается во внешнем воспитательном воздействии. Одновременно для современной психологии и педагогики все большее значение начинает приобретать понимание воспитательной работы как средства, направленного на создание условий для саморазвития и самовоспитания личности.

В последнее время воспитательной работе стали уделять большее внимания, но современный преподаватель еще не вполне способен обеспечить должного воспитательного воздействия на молодежь. Недостаточное внимание к воспитательной работе со студентами со стороны преподавателей обуславливается рядом причин, в том числе отсутствием должной психолого-педагогической подготовки кураторов к воспитательной работе со студентами, высокой загруженностью преподавателей учебными занятиями.

Необходимость проведения воспитательной работы обусловлена происходящей в настоящее время сменой ценностей и приоритетов у студенческой молодежи. Индивидуальные ценности стали перевешивать общественные, самоценность личности возросла, упал престиж таких ценностей как гражданственность, патриотизм, коллективизм, труд, что может служить отражением изменений в духовном мире молодежи.

Особенности ценностного сознания молодежи определяются возрастной спецификой и характером влияния социального окружения, разнообразными историческими, социально-демографическими национальными факторами, а также воспитательным воздействием со стороны социальных институтов общества, что в конечном итоге обуславливает реальную социальную ситуацию развития для каждой конкретной личности.

Существует проблема возобновления традиций коллективизма, патриотизма. Воспитательная работа, должна быть направлена на развитие гуманной личности с присущим для нее сочетанием выраженной индивидуальности с коллективисткой направленностью, характеризующейся осознанием своего гражданского долга, трудолюбием, ответственностью, профессиональной и гуманитарной культурой, а также культурой взаимодействия с окружающими людьми.

Успешность подготовки студентов во многом определяется реальными условиями их жизнедеятельности, характером возникающих в процессе учебы проблем и возможностями их разрешения со стороны администрации и преподавателей.

Попытка разделения процессов образования и воспитания может создать препятствия достижению конечной цели образования - подготовки профессионально грамотных и гармонично развитых специалистов. Главным направлением воспитательной работы должно является профессионально воспитание через профессию.

Все эти требования могут успешно реализоваться не только через профессиональное обучение и воспитание, но через широкий воспитательный процесс, проводимый во внеучебное время.

Определение воспитательного процесса как внеучебного, является условным. Практически каждая учебная тема несет информационно-значимую воспитательную нагрузку. Воспитание осуществляется при изучении героических страниц истории нашей Родины, особенно военной истории, традиций, обычаев и т.п.

Основными направлениями воспитательной работы должны быть: повышение квалификации преподавательского состава по воспитательной работе; информационное обеспечение, формирование патриотического сознания студентов, развитие профессиональных способностей студентов, духовно-нравственное воспитание студентов, формирование здорового образа жизни, и т.п.

Воспитательная работа должна проводиться непрерывно и охватывать студентов на всех курсах обучения, с учетом их особенностей и занятости. Обучение - это не только овладение специальностью, оно не должно сводиться только к привитию необходимых для деятельности по специальности знаний, умений и навыков. Оно должно тесно переплетаться с воспитанием профессионального мастерства, строящегося на высоких мотивах, моральных и психологических качествах специалиста, личности студента в целом.

Литература

1. Положение о факультетах военного обучения (военных кафедрах) при федеральных государственных образовательных учреждениях высшего профессионального образования (утвержденное постановлением правительства РФ от 6 марта 2008 года №152).

2. Воспитательная работа в ВС РФ // Учебное пособие. Под редакцией Н.И.Резника. М, 2005.

3. Белошев В.А., Рыжков А.В. Элемент «Державности» в системе патриотических ценностей, студентов обучающихся на военной кафедре СПб ГУ ИТМО // Материалы XL научной и учебно-методической конференции. – СПб : СПбГУ ИТМО, 2011.

4. Панова Е.В., Рыжков А.В. Информационные технологии - инструмент повышения качества обучения и подготовки офицеров запаса на военных кафедрах // Материалы XL научной и учебно-методической конференции. – СПб : СПбГУ ИТМО, 2011.

5. Панова Е.В., Рыжков А.В. Воспитательная работа как неотъемлемая составляющая обучения в высшей школе // Межвузовский сборник научных трудов. – СПб : АртЭго, 2010.

6. Рыжков А.В. «Воспитательная работа в процессе обучения» Научно-технический вестник. – СПб : СПб ГУ ИТМО, 2005.

УДК 355.234:378.6

ВОЕННЫМ КАФЕДРАМ 85 ЛЕТ. УСПЕХИ И ПРОБЛЕМЫ

Супрун А.Ф.

Санкт-Петербургский государственный политехнический университет

Перед тем как рассказать о сегодняшнем дне военной образования при Санкт-Петербургском государственном политехническом университете хотелось бы вспомнить несколько поворотных моментов истории. Так, до 1926 года в военной подготовке студентов царила неразбериха. Руководство вузов имело право ходатайствовать об отсрочке призыва каждого, обратившегося с такой просьбой, студента. Для этого руководство учебного заведения обращалось в военные инстанции с официальными письменными просьбами. А те решали: призывать студента в РККА или нет.

Если ходатайство по поводу какого-нибудь студента в военкомат не поступало, его призывали на службу. Такие ходатайства необходимо было представлять ежегодно.

С лета 1926 года студенты, имевшие отсрочку, освобождались от допризывной подготовки.

20 августа того же года ЦИК и СНК СССР (по ходатайству профессорско-преподавательского состава ВУЗа) приняли постановление об организации высшей военной подготовки студентов вузов. Тогда же, в августе, был подписан приказ Реввоенсовета СССР N 565 и во исполнение этого документа приказ штаба Ленинградского военного округа N 326, в соответствии с которыми, в Ленинградском политехническом институте начались занятия студентов по военной подготовке.

Таким образом, октябрь 1926 года – это дата рождения военной кафедры, хотя само понятие «военная кафедра» появилось гораздо позже. Оглядываясь на историю военного образования Союза ССР, а затем России может показаться, что это образование сложилось в стройную систему за период семидесятипятилетнего существования. Однако на протяжении этого периода военное образование при политехническом имело и свои взлеты и свои трудности. Чаще всего это было связано с определенными историческими событиями имевшими место в стране.

И все же прослеживается главная идея военного образования это бережное отношение государства к интеллектуальному потенциалу страны и его использование как в гражданской сфере так и в военной.

Подготовка патриотов страны и специалистов для ЗРВ ВВС и СВ России – задача нынешней военной структуры университета. Ежегодно университет выпускает около тысячи специалистов

запаса для армии страны. В перспективе возможна и подготовка кадрового состава для вооруженных сил государства. Эти вопросы находятся в стадии исследования.

Демократизация процесса образования отразилась и на военном обучении. В первую очередь следует отметить, что студенты 90-ых добились отмены формы обязательного обучения военному делу. Сейчас военная подготовка – строго добровольное дело студента вуза дневной формы обучения. Другое завоевание демократических реформ в образовании – это возможность обучения девушек по инженерным специальностям.

Проблемы нынешнего военного обучения порождены тем, что направления подготовки инженерной школы резко изменились, а направленность в военной подготовке студентов как офицеров запаса не менялись и остались прежними. Разве может быть полноценным специалистом ЗРВ студент, не имеющий базовой инженерной подготовки?

Здесь просматриваются несколько путей решения проблемы. Первый это пересмотр специальностей с целью максимального сближения военной специальности и гражданской. Понятно, что в этом случае качество подготовки – колоссальное. Второй путь это проведение дополнительной подготовки гуманитариев вне сетки часов военной подготовки по разработанным программам с привлечением как военных, так и гражданских специалистов. И третий путь решения проблемы это избирательный подход к отбору факультетов и кандидатов на обучение. В этом случае студенты ряда факультетов могут быть поставлены в неравное положение по отношению к своим собратьям по вузу.

В заключении хотелось бы еще раз отметить, что введенная в 1926 году система военного образования при гражданских вузах стала и остается быть в высокой степени гибкой и экономичной для нашего государства особенно в настоящее время, что позволяет тратить незначительные денежные средства, а получать образованных в военном отношении специалистов для кадровой и срочной службы.

Государственный и только государственный подход к стоящей сегодня проблеме реформирования системы военного образования сможет дать значительные плоды для решения вопроса формирования офицерского корпуса обновленных ВС РФ.

ПРИЕМЫ СОВЕРШЕНСТВОВАНИЯ ОЦЕНКИ КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММ ВОЕННОЙ ПОДГОТОВКИ

Хромов И.Н.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

На военной кафедре Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики в процессе военной подготовки большое внимание уделяется аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям осваиваемой ими образовательной программы. Для ее проведения на кафедре разработана **информационная профессионально-ориентированная**

обучающая среда, которая представляет собой комплекс оценочных средств и реализует ряд методических приемов.

Как показывает опыт, применение в образовательном процессе информационно-ориентированной обучающей среды позволяет максимально приблизить условия аттестации обучающихся к условиям их будущей профессиональной деятельности.

УДК 51-7

ПРАКТИКА ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ПРОГНОЗИРОВАНИЯ – “FUTURE” В ПРОЦЕССЕ ОБУЧЕНИЯ СТУДЕНТОВ КАФЕДРЫ МИПИУ

Шабаев Р.И.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Рассматриваются вопросы, касающиеся программного обеспечения в решении задач моделирования и прогнозирования угроз информационной безопасности, связанные с особенностями специализации и подготовки бакалавров и магистров на кафедре МиПИУ СПб НИУ ИТМО.

Ключевые слова: информационная безопасность (ИБ), информационные угрозы (ИУ), моделирование, прогнозирование, программный комплекс, 2012 год, катастрофа.

Особенность учебного плана подготовки студентов кафедры МИПИУ по специальности 090900 «Информационная безопасность» – специализация, основой которой является *математическое моделирование и прогнозирование информационных угроз*. Объектами будущей профессиональной деятельности студентов, помимо решения задач правового и организационно-технического обеспечения информационной безопасности, должно быть и решение задач прогнозирования. В этих целях разработан ряд программных комплексов (Future, SinusMaker), позволяющих качественно решать задачи моделирования и прогнозирования угроз информационной безопасности.

Информационная безопасность, понимаемая как *состояние защищенности национальных интересов в сфере* информации, информационной инфраструктуры, а также субъектов, осуществляющих сбор, формирование, распространение и использование информации, является важной составной частью национальной безопасности государства. Поэтому вопросы обеспечения ИБ не могут быть решены успешно в отрыве от решения прогнозных задач. В данном контексте следует отметить, что в последние несколько лет вокруг проблемы 2012 года развернута настоящая информационная война, выражающаяся, прежде всего, в апокалипсических сценариях дальнейшего развития мировых событий. Поэтому ответ на вопрос, в какой степени возможно усиление опасных природных и техногенных процессов, обострение в социально-политической сфере, представляется весьма важным.

1. Теоретические и практические основы программного моделирования и прогнозирования информационных угроз.

В Доктрине ИБ подчеркнуто: «Государство в процессе реализации своих функций по обеспечению информационной безопасности Российской Федерации: проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности Российской Федерации, разрабатывает меры по ее обеспечению; организует работу… по реализации комплекса мер, направленных на *предотвращение, отражение и нейтрализацию* угроз информационной безопасности Российской Федерации». В структуру обеспечения ИБ входит сам объект безопасности, определение (прогнозирование) угроз объекту ИБ и принятие конкретных мер по их предотвращению. Доктрина также определяет, что объектами безопасности и прогнозирования являются *человек, общество и государство*.

Разработанная на кафедре модель обеспечения информационной безопасности (рис. 1), имеет четкую методическую направленность, поскольку раскрывает место и роль специализации кафедры в деле решения задач обеспечения информационной безопасности.

Рисунок 1. Модель обеспечения информационной безопасности

Данная модель раскрывает основные сферы и объекты моделирования и прогнозирования и служит базой для определения основных направлений приложения сил профессорско-преподавательского состава кафедры. Таким образом, в рамках изучения дисциплин специализации, проблема выявления, анализа и прогнозирования угроз информационной безопасности (информационных угроз) становится ключевой.

Разрабатываемый и апробированный в течение 7 лет программный продукт, называемый в последней версии – «**Future**», позволяет решать ряд задач в области прогнозирования информационных угроз.

Из назначения и целей выводятся и возможности программы FUTURE:

– мониторинг объектов повышенной опасности;
– прогнозирование чрезвычайных ситуаций;
– выявление угроз политической и экономической стабильности государства.

2. Практика использования программного комплекса для прогнозирования «FUTURE» в процессе обучения студентов кафедры МИПИУ.

Изменение, а точнее сокращение общего количества часов на обучение бакалавра по программе специализации: программное моделирование и прогнозирование информационных угроз», не позволяет сделать акцент на конкретном изучении космических циклов, анализе их выраженности. Поэтому крайне затруднено использование адресного метода прогнозирования объектов исследования, особенно – поиск и нахождение точек бифуркации, циклических точек перехода в новое качество. Ориентировочно программа осуществляет следующий алгоритм действий:

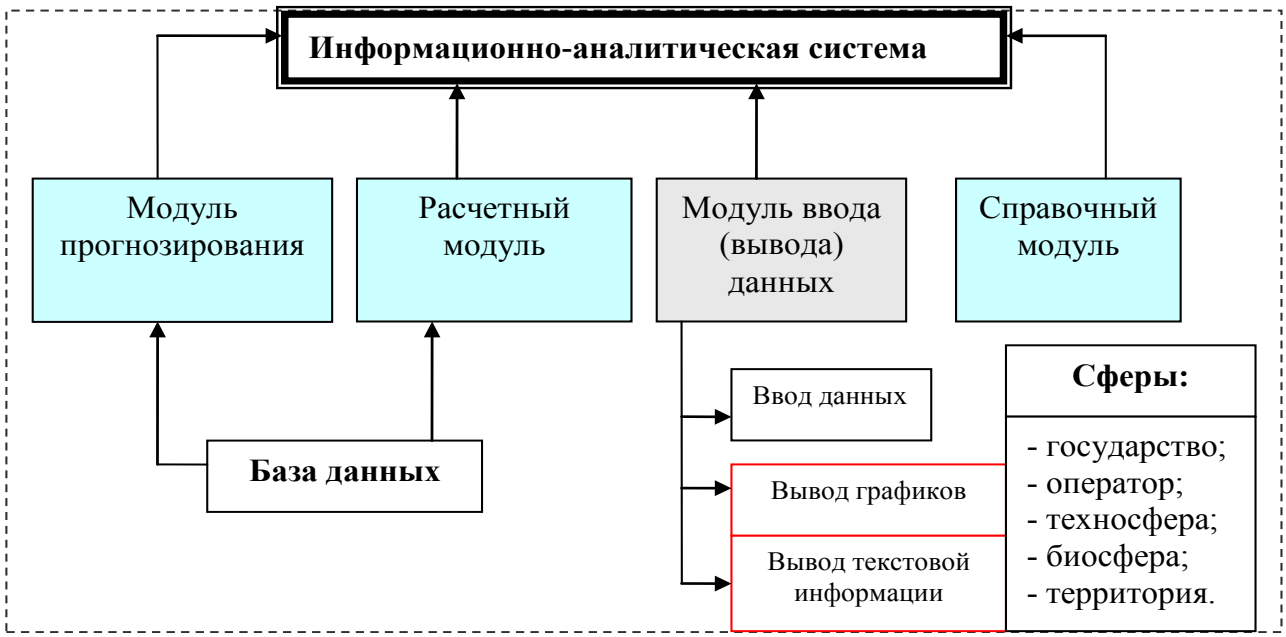


Рисунок 2. Общая структура программы

Таким образом, основным итоговым документом являются оперативный или краткосрочный прогноз-график по видам информационных угроз, основанный на ретроспективном изучении базы данных. Программа также позволяет изменять индексную шкалу посредством введения результатов программного нахождения процентной выраженности космических циклов.

3. Пример использования возможностей программного комплекса для моделирования угроз 2012 года.

В последние десятилетия наблюдаются существенные изменения в некоторых геофизических и космических параметрах. Насколько тесно эти изменения могут быть связаны с природными катаклизмами и, как следствие, представлять опасность для стабильного развития, в частности, проблема дрейфа геомагнитных полюсов Земли?

На рис. 3 показан график, отражающий движение северного геомагнитного полюса. Как видно из графика, к концу 90-х годов по сравнению с 1980-м годом скорость дрейфа северного

геомагнитного полюса увеличилась почти в пять раз. Этот факт может свидетельствовать о существенных изменениях в энергетических процессах в ядре Земли, формирующих геомагнитное поле нашей планеты. Безусловно, наблюдаемое явление может отражать начало очередного цикла резкой активизации эндогенной (внутренней) активности Земли. Учитывая, что процесс движения северного магнитного полюса сопровождается снижением напряженности магнитного поля Земли, можно предположить, что это должно повлиять на глобальные климатические изменения.

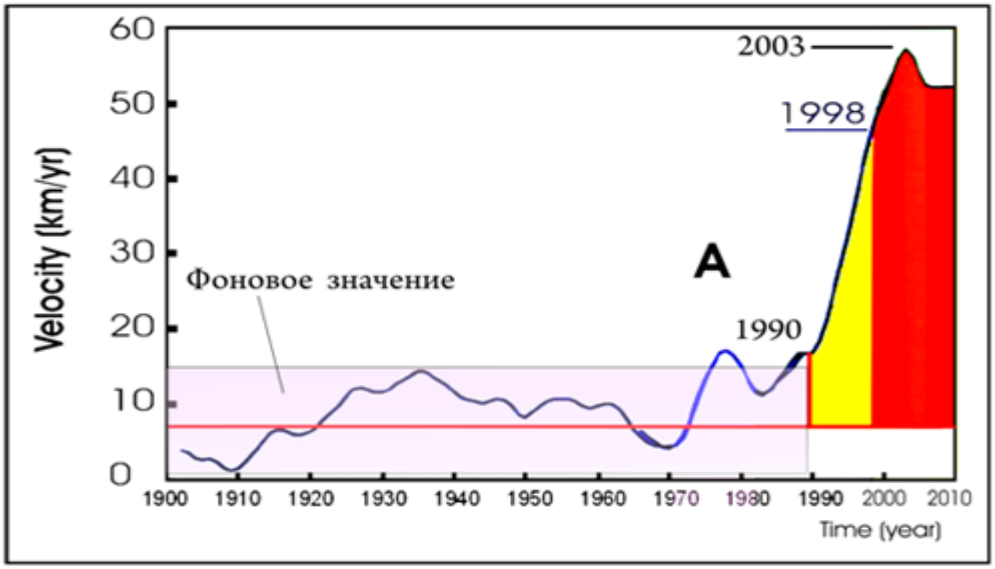


Рисунок 3. График скорости движения северного геомагнитного полюса (http://geochange.org/Pdf/Will_the_Magnetic_North_Pole.pdf)

На рис. 4 приведены результаты исследований сейсмической активности Земли за период с 1976 по 2009 гг. (см. http://www.ru.geochange-report.org), показывающие корреляцию с изменениями в космических параметрах (см. рис. 3). Ожидаемая активность природных катаклизмов в 2012-15 гг. может иметь очень серьезные негативные последствия для стабильного развития цивилизации и привести к огромным жертвам и разрушениям. Экономические последствия для стран, подверженных природным катаклизмам, могут быть катастрофическими.

В ряде исследований последних лет [1] можно выделить следующие результаты:

– основные факторы влияния на катастрофические процессы – гелиогеофизический, космический (колебания земной оси) и лунный;

– лунные циклы могут являться методом расчета времени активизации катастроф и ЧС различного характера;

– *методологически* – частотно-временные закономерности возникновения ЧС, катастроф и опасных процессов различного характера – это результат и следствие взаимодействия внешних (энергетическая накачка) и внутренних (распределение энергии и временная активизация подсистем) квазициклических процессов;

– *математическим* условием возникновения катастрофы являются *экстремумы* выбранных для анализа потенциальных функций, которые могут быть характеристикой изменения выбранного для анализа фактора или параметра, причем любой физической природы;

– к дополнительным, в качестве факторов, обусловливающих катастрофические процессы, отнесены сейсмический, техногенный и человеческий.

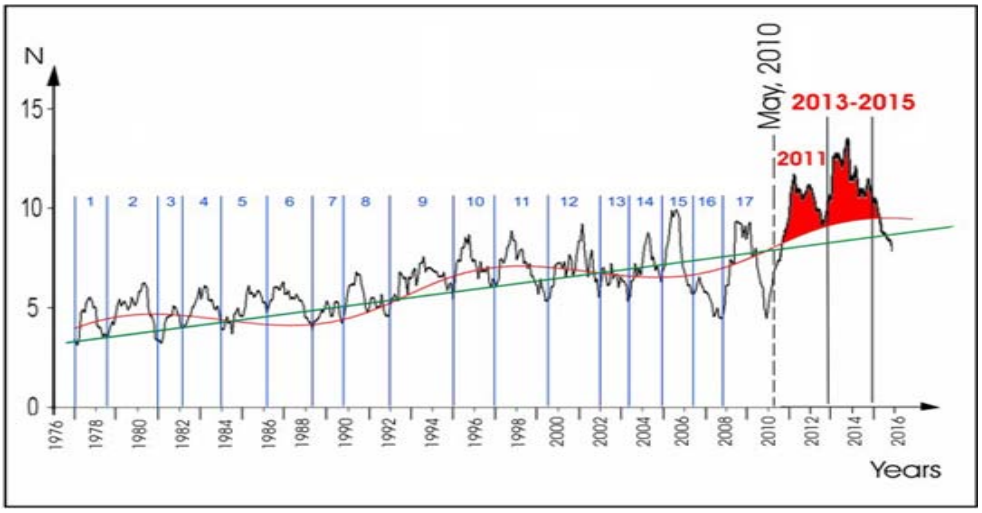


Рисунок 4. График ежемесячного числа землетрясений с M > 6,5 с 1976 г. по 2010 г. с прогнозом до 2016 года на основе выделения синусоидального тренда

Катастрофа есть результат резкого качественного изменения свойств системы в ходе плавного количественного изменении параметров, от которых она зависит. Наиболее вероятно, что катастрофа любого рода возникает не сразу, а имеет продолжительный подготовительный период. Катастрофа происходит только тогда, когда система становится чрезмерно чувствительной к любым, даже минимальным, изменениям внешних факторов. В целом, анализируя имеющиеся разработки в области взаимосвязей космических и земных процессов [1, 3, 5] и др., можно сделать вывод: катастрофа любой системы (природной, техногенной, социальной) есть результат корреляции синхронизированных экстремальных изменений космических (внешних) и внутрисистемных процессов.

На рис. 5 отображен резонансный алгоритм информационной связи внешних (космических) условий с внутрисистемными техногенными и природными процессами.

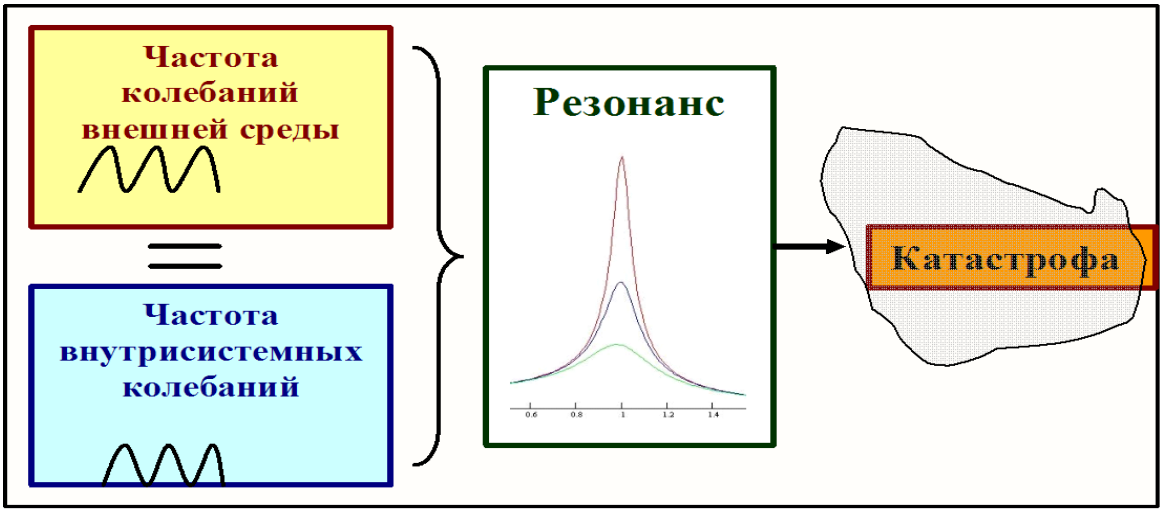


Рисунок 5. Алгоритм информационного резонанса в системах

Как известно, временные ряды состоят из двух элементов:

– периода времени, за который или по состоянию на который приводятся числовые значения (период упреждения);

– числовых значений того или иного показателя, называемых уровнями ряда.

Какие показатели динамического ряда использовать? Учитывая специфику модели прогнозирования, в качестве ведущего параметра целесообразно брать циклическую составляющую. В таком случае, величины, характеризующие цикл, и станут и прогностическим интервалом времени наступления события.

Графическая модель угроз составляется на основе использования Программного комплекса для прогнозирования информационных угроз, разработанный силами Научного общества студентов кафедры Мониторинга и прогнозирования информационных угроз СПб НИУ ИТМО, и, используемый в учебном процессе по предмету специализации. Номер государственной регистрации в реестре программа для ЭВМ – № 2011611038 от 28 января 2011 года.

Внутренние условия функционирования Российской федерации в социально-политической и экономической сферах [4] в 2012 году можно увидеть из графика на рис. 6. График построен на основе уравнения 4-х фазовых гармонических колебаний ведущих циклов развития страны – 36, 72 и 144 – летних [4]. Ближайшая потенциальная точка бифуркации по частоте и фазам колебаний – 2016 год. Следовательно, можно сделать вывод, что с точки зрения внутренних условий развития системы, катастрофических явлений в динамике 2012 года в социально-политической сфере не наблюдается. Специфика будущих внутренних угроз (с 2013 года) – начало утраты динамизма, способное породить возникновение крупных оппозиционных партий.

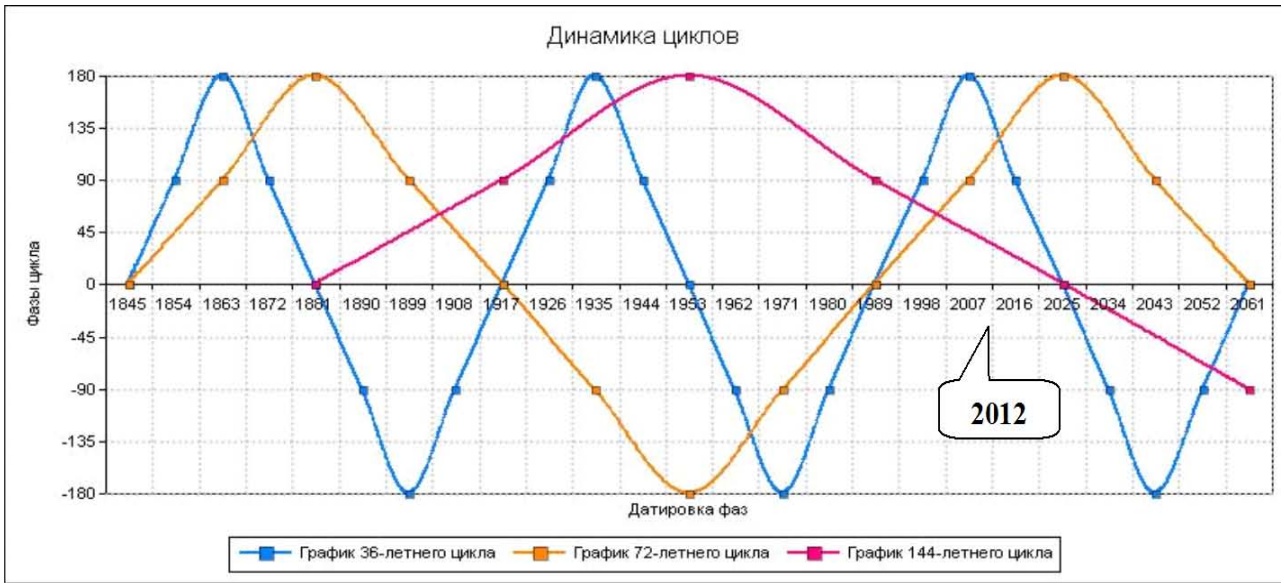


Рисунок 6. Динамика фазово-циклического развития РФ

В графике на рис. 7 реализована идея информационной взаимосвязи космогенных и природно-техногенных катаклизмов. Как видно из графика, наиболее взрывоопасными периодами являются январь-февраль, **июнь-август** и декабрь 2012 года. Период с 6 июня по 10 июля (18 августа) следует рассматривать именно с точки зрения формирования долговременных напряжений и ситуаций, способных реализоваться не только в указанный период, но и в ближайшей перспективе – через 1–1,5 года.

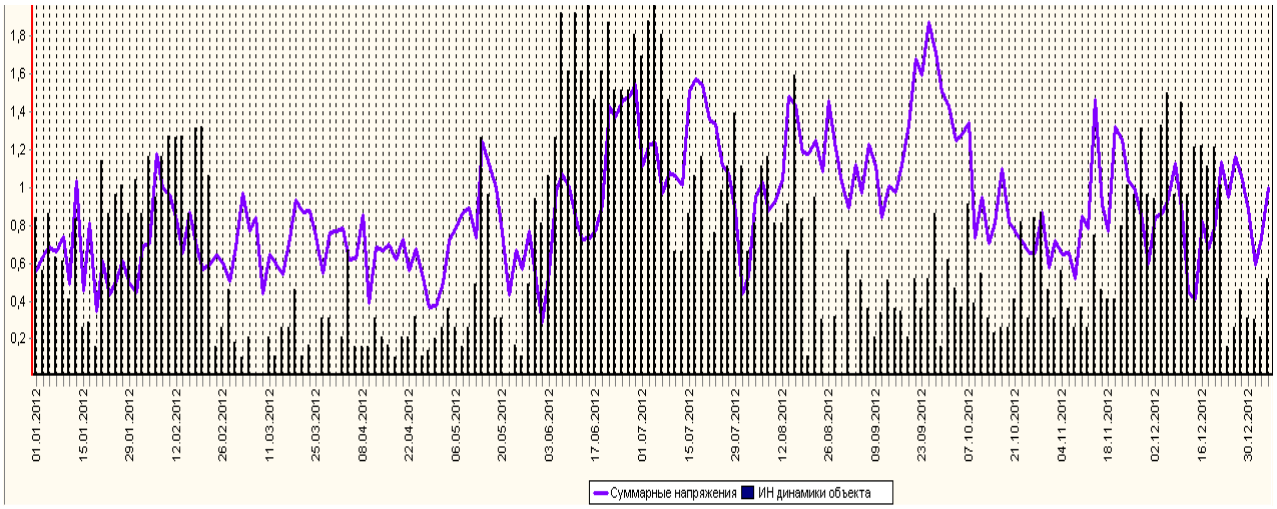


Рисунок 7. Динамика угроз информационной безопасности России в техногенной и природной сферах в 2012 году

В данном контексте, следующие даты могут стать детонаторами (точками возбужнения) долговременных напряжений: 14.01, 14–15.02, 27.05**, 6–12.06**, **29–30.06**, **18–20.07**, 15.08, 27.11.2012.

Главные контуры угроз:

– ухудшение экологической обстановки в связи с возможными авариями на нефтепроводах, АЭС, наводнениями и извержениями вулканов;

– вероятность мировых крупных эпидемий, имеющих непосредственное отношение к РФ;

– усиление терроризма, особенно в компьютерной и ядерной сферах.

Особую озабоченность вызывают нарастание экологических проблем и обострение военной напряженности.

В основе моделирования особенностей внешних угроз положена идея обострения международной обстановки в период перехода в фазу поддержания в 36-летнем цикле развития. Хотя хронологически точкой воспламенения могут явиться 2013–2014 гг., однако в исследуемый период начинают фокусироваться главные проблемные факторы будущих угроз.

Заключение:

1) Моделирование информационных угроз представляет собой важнейшее направление обеспечения информационной безопасности, как составной части обеспечения национальной безопасности государства.

2) Разработанная модель обеспечения информационной безопасности позволяет более эффективно решать задачи подготовки специалиста по математическому моделированию и прогнозированию информационных угроз.

3) Начало второго десятилетия 21 века отмечено периодически повторяющимся неблагоприятным сочетанием экстремальных условий гелиогеофизических и космических факторов.

4) Главной угрозой информационной безопасности РФ в 2012 году являются не социально-политические, а природно-техногенные процессы и общемировые тенденции.

Литература

1. Байда С.Е.. Проблема 2012 года. Оценка реальных угроз. Журнал «Проблемы анализа риска». – 2011. – №1.

2. Жигулин Г. П.. Проблемы информационной безопасности России первой четверти 21 века. Материалы XVI Всероссийской научно-методической конференции «Телематика’2009».

3. Немировский В.Г., Кудрявцева В.И. Универсумный подход к прогнозированию социальных систем. – Красноярск, Минск : Изд-во КрасГУ, изд-во БГУ, 2004. – 172 с.

4. Шноль С.Э. Космофизические факторы в случайных процессах. – 2009. – 388 с.

5. Концепция национальной безопасности Российской Федерации от 17.12.1997 г.

6. Доктрина информационной безопасности РФ от 9 сентября 2000 г.

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики».

Перед студентами, закончившими кафедру мониторинга и прогнозирования информационных угроз (МиПИУ), открываются хорошие перспективы. Высокий уровень подготовки в области информационной безопасности, прикладной математики, информатики, программирования, воинское звание лейтенант по запасу определяют востребованность выпускников как на рынке труда государственных и коммерческих организаций, так и на службе в силовых министерствах и ведомствах РФ.

КАФЕДРА МОНИТОРИНГА И ПРОГНОЗИРОВАНИЯ ИНФОРМАЦИОННЫХ УГРОЗ

Проблема комплексного обеспечения информационной безопасности и совершенствование образовательных технологий подготовки специалистов силовых структур

Межвузовский сборник трудов
II Всероссийской научно-технической конференции ИКВО НИУ ИТМО

Под редакцией Жигулина Г.П., Будько М.Б.

Редакционно-издательский отдел НИУ ИТМО

Зав. РИО Н.Ф. Гусарова

Лицензия ИД № 00408 от 05.11.1999

Подписано к печати 16.04.2012

Заказ № 2444

Тираж 100 экз.

Отпечатано на ризографе

Редакционно-издательский отдел
Санкт-Петербургского национального
исследовательского университета
информационных технологий,
механики и оптики
197101, Санкт-Петербург, Кронверкский пр., д. 49