ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ

НАУЧНО- ПРАКТИЧЕСКИЙ ЖУРНАЛ

№1 (2) январь-март 2014 г.

Выходит 4 раза в год

Зарегистрировано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций Свидетельство ПИ № ФС77-55950 от 15.11.2013 г.

Учредители и издатели:

ЗАО «Научно-производственное объединение «Эшелон»

Федеральное бюджетное учреждение «Научный центр правовой информации при Министерстве юстиции Российской Федерации»

Отпечатано в РИО НЦПИ при Минюсте России.

Печать цветная цифровая.

Подписано в печать 20.03.2014 г.

Общий тираж 600 экз. Цена свободная.

Адрес: 125438, Москва, Михалковская ул., 65, стр. 1.
E-mail: editor@cyberrus.com Тел. (495)539-2314
Требования, предъявляемые к рукописям, размещены на сайте:
www.cyberrus.com

СОДЕРЖАНИЕ

Подписка на журнал осуществляется в почтовых отделениях по каталогу «Пресса России». Подписной индекс 40707

КОНЦЕПЦИЯ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ

Мы предлагаем вниманию читателей интервью, которое 12 февраля 2014 года дал нашему журналу ***ГАТТАРОВ Руслан Усманович****, Председатель Временной комиссии по развитию информационного общества Совета Федерации Федерального Собрания Российской Федерации*

Руслан Усманович, спасибо, что Вы согласились ответить на наши вопросы.

По Вашей инициативе Временная комиссия по развитию информационного общества представила для всеобщего обсуждения проект[1] Концепции стратегии кибербезопасности Российской Федерации.

Предусматривается ли разработка в нашей стране документов, в которых будут сформулированы понятия границ киберпространства?

Да, и такая разработка уже ведется. Концепцию, вернее, тогда еще Стратегию кибербезопасности мы начали разрабатывать два года назад на площадке Комиссии Совета Федерации по развитию информационного общества. Аудит нормативного регулирования и общей системности усилий, предпринимаемых в направлении обеспечения кибербезопасности, показал нам, что эти усилия фрагментированы, а в регулировании есть крупные пробелы. Проанализировав опыт зарубежных стран, мы пришли к выводу, что и России требуется свой доктринальный документ в этой области. После более чем пяти версий Стратегия стала Концепцией стратегии именно потому, что для прописывания всех уточнений, границ и шагов необходимо включенное участие большого количества государственных органов, прежде всего Совета Безопасности, правоохранительных органов и федеральных министерств. Разумеется, Концепция писалась с участием их представителей, но речь идет о необходимости проработки документа в самих структурах. Мы свою задачу видели, главным образом, в том, чтобы привлечь к теме внимание (и если посмотреть на динамику роста количества принимаемых в России нормативных актов в сфере информационной безопасности, то, возможно, нам удалось в этой части добиться некого успеха), а также сформулировать квинтэссенцию необходимых направлений деятельности для обеспечения кибербезопасности. Будет ли теперь на базе нашего документа разработана Концепция? Верю, что да, поскольку вопрос стоит остро. Возможно, речь даже может идти о коротком горизонте – примерно полутора годах. Но разработку вести будут уже другие ведомства, мы же готовы принимать участие и помочь консультациями. А если появится Концепция, при ней появятся и подзаконные акты, приказы и т.д. с самой что ни на есть подробной конкретикой.

Повлияли ли на работы по разработке Концепции кибербезопасности материалы, опубликованные Эдвардом Сноуденом?

Работы по разработке Стратегии кибербезопасности мы начали более чем за полгода до разоблачений Сноудена. Документы Сноудена, однако, наглядно доказали обоснованность наших опасений и, я думаю, привлекли к нашей работе больше внимания. Должен заметить, что именно поступок Сноудена побудил меня начать плотную работу с транснациональными интернет-корпорациями с тем, чтобы обеспечить соблюдение прав клиентов-россиян на защиту

1 Концепция стратегии кибербезопасности Российской Федерации. См. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

их персональных данных в соответствии с российским законодательством. И, конечно, поступок Сноудена облегчил нашу задачу в части обеспечения прав россиян - транснациональным интернет-корпорациям стало уже невозможно не откликаться на наши требования.

Как, на Ваш взгляд, Концепция будет гармонизирована с документами стран-участников Таможенного союза и других стран ближнего зарубежья?

Концепция выстроена с учетом международных стандартов, норм и опыта в части подготовки подобных документов. Получился качественный и сбалансированный документ. России стоит поторопиться с подготовкой и принятием Концепции, поскольку в мировом рассмотрении мы несколько запаздываем. Однако это относительно стран-лидеров. В целом же законодательное регулирование киберпространства пока находится в стадии активного становления, причем в большинстве стран процесс сейчас находится у начальной точки. Насколько мне известно, из стран Таможенного союза и ближнего зарубежья мы в первых рядах по срокам разработки такого доктринального документа, как Стратегия кибербезопасности. Думаю, мы можем предложить наш опыт соседям, и тогда вопрос гармонизации норм, возможно, и не появится – они будут гармонизированы с самого начала.

Как известно, в Китае политика государства направлена на жесткое регулирование киберпространства. В представленном на обсуждение проекте Концепции сказано, что «регулирование киберпространства исключительно на национальном уровне невозможно в силу его трансграничности». Как бы Вы могли это прокомментировать?

Этот тезис отражает нашу позицию, она заключается в том, что развитие электронных коммуникаций вместе с неизбежными рисками предоставляет и уникальные, широчайшие возможности, и мы считаем неверным их игнорировать, обрывая контакты с другими сегментами интернета, чтобы повысить свою кибербезопасность. Заметьте, я говорю повысить, а не обеспечить. Изоляционистская политика Китая в сфере киберпространства, безусловно, упрощает задачу поддержания кибербезопасности страны в силу его подконтрольности, однако в первую очередь это относится к возможности контролировать действия китайских граждан, а не к неуязвимости против кибератак из-за рубежа. Абсолютной защиты не существует, и все мы имеем дело с рисками.

На Ваш взгляд, насколько возможно международное сотрудничество в области кибербезопасности без взаимного ущемления национальных интересов?

Международное сотрудничество всю свою историю существует поверх ущемления взаимных интересов, но это не мешает ему снимать часть действительно серьезных проблем. Например, сейчас очень остро строит вопрос выработки единых правил игры в части защиты персональных данных граждан при их обработке транснациональными корпорациями. Согласно конструкции международного права такие корпорации, если они не имеют в определенной стране официального представительства, не обязаны соблюдать ее законодательство в сфере защиты персональных данных, что, разумеется, вызывает конфликты. Но для их разрешения на международном уровне нет ни единой площадки, ни уполномоченных органов, ни инструментов арбитража. Между тем в скором времени, я считаю, проблема будет решена именно переговорным путем и недостающие институты будут созданы.

В чем суть деятельности российских «кибероотрядов »?

«Наблюдать, ликвидировать, защищать», я считаю. Смысл их создания в том, чтобы появился инструмент постоянной готовности для реагирования на кибератаки против информационных ресурсов России. Это требует постоянного мониторинга, протоколов действования, жесткой дисциплины. Параллельно, думаю, будет организовано «патрулирование периметра», т.е. проверки защищенности наших киберобъектов.

Какие меры будут применяться для стимулирования российских производителей продукции в области кибербезопасности?

Рассматривается широкий перечень мер поддержки – от создания национальной программной платформы с доверяемой средой разработки и контрактами на госзакупки программного обеспечения (ПО) для государственных органов до введения налоговых льгот. Однако о том, какие

меры будут введены, говорить пока рано. Могу лишь сказать, что понимание проблемы в государственных органах есть.

Вы много усилий приложили в области создания российского электронного правительства. Какие там последние новости?

Процесс движется вперед, но не так быстро, как мог бы. Разумеется, успехи есть. Постепенно выполняются прописанные программы и нормативы. Однако остаются проблемы с едиными стандартами, налаженностью межведомственного взаимодействия, корректной статистикой и публичным мониторингом. На мой взгляд, необходимо создание службы профессионального государственного заказчика, стимулирование спроса на электронные госуслуги со стороны населения – соответствующий законопроект я внес в Государственную Думу еще в 2011 году. Концентрироваться, полагаю, следует на образовании, здравоохранении, ЖКХ и транспорте.

Учитывается ли зарубежный опыт организации защиты информации при разработке российского электронного правительства, в частности, по вопросам защиты персональных данных?

Разумеется. Что касается, например, защиты персональных данных, то разработанный нами при широком привлечении экспертов и представителей ведомств законопроект «О персональных данных» не только полностью соответствует требованиям Конвенции ЕС о защите прав субъектов персональных данных с последними поправками, но и где-то даже опережает мировые нормы – например, в части поддержки развития «облачных сервисов» путем либерализации условий трансграничной передачи данных без падения их защищенности.

Вы в прошлом профессионально занимались спортом. Чем это сейчас помогает Вам в работе? Какие качества и навыки, полученные в те годы, Вы используете?

Да, занимался тяжелой атлетикой, даже выступал за Челябинскую область. Там научился сжимать зубы и делать дело несмотря ни на что. Сейчас, когда выдается время, катаюсь на горных лыжах, иногда играю в хоккей, иногда – в гольф. Спорт помогает вести гармоничную жизнь, отвлекаться от ментальной работы. Помогает поддерживать форму и сбрасывать накопившееся напряжение. Поэтому заниматься им никогда не прекращал.

Какие пожелания Вы хотели бы высказать нашим читателям?

Повышайте свои компетенции в обеспечении кибербезопасности хотя бы на бытовом уровне – обновляйте программное обеспечение, базы антивирусов, не пользуйтесь одной и той же флешкой дома и на работе. Будьте аккуратны со своей личной информацией, не выкладывайте ее в сеть без необходимости – Интернет помнит все. И, разумеется, приглядывайте за детьми. Инструменты родительского контроля сейчас распространены, но используются очень мало. Между тем обеспечение безопасности детской активности в Интернете одними законами не решить, необходимо и участие семьи.

КИБЕРБЕЗОПАСНОСТЬ КАК ОСНОВНОЙ ФАКТОР НАЦИОНАЛЬНОЙ И МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ XXI ВЕКА (Часть 2*)

***Бородакий Юрий Владимирович**, академик РАН, доктор технических наук, профессор*
***Добродеев Александр Юрьевич**, кандидат технических наук, старший научный сотрудник*
Бутусов Игорь Викторович

В статье рассматриваются актуальные проблемы обеспечения международной и национальной кибербезопасности и предлагаются подходы к созданию адекватной современным угрозам системы обеспечения кибербезопасности автоматизированных систем органов военного и государственного управления

***Ключевые слова**: кибербезопасность, информационная безопасность, инфосфера, киберпространство, информационное противоборство*

CYBERSECURITY AS A MAJOR FACTOR OF NATIONAL AND INTERNATIONAL SECURITY IN THE XXI CENTURY (Part 2)

***Yuri Borodakiy**, Member of the RAS, Doctor of Technical Sciences, Professor*
***Alexander Dobrodeyev**, Ph.D., Associate Professor*
Igor Butusov

The actual problems of international and national cybersecurity are considered. The approaches to the development of the cybersecurity system relevant to modern threats to the military and government automated systems are given.

***Keywords**: cybersecurity, cyber security, information security, infosphere, cyberspace, information warfare*

1. СОВРЕМЕННЫЕ ТЕНДЕНЦИИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОРГАНОВ ВОЕННОГО И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

В современных условиях, в целях эффективного отражения угроз кибербезопасности и обеспечения возможности проведения симметричного ответа на вызовы или нанесения упреждающего удара, автоматизированные системы органов военного и государственного управления (АСУ ОВГУ), должны совершенствоваться в направлении повышения степени их автоматизации и компьютеризации, то есть создания и развития АСУ в защищенном исполнении. Насущным требованием времени становится пересмотр принципов построения АСУ ОВГУ с позиций обеспечения кибербезопасности как в мирное, так и в военное время.

По мнению специалистов вооружённых сил США в области кибербезопасности, в техническом плане полная адекватная киберзащита предусматривает построение и использование следующих основных подсистем: подсистемы защиты (Protection Capabilities), обеспечивающей скрытность излучений радиоэлектронных средств, систем и средств связи, компьютерную безопасность (Computer Security) и информационную безопасность (InfoSec); подсистемы обнаружения (Detection Capabilities), обеспечивающей распознавания аномалий в сети за счет применения систем их обнаружения; подсистемы реагирования на изменения технических параметров и обстановки (Reaction Capabilities), обеспечивающей восстановление (в том числе реконфигурацию) и выполнение других процессов информационных операций [2].

По мнению авторов, система киберзащиты, созданная в соответствии с вышеуказанными требованиями, не обеспечивает полной кибербезопасности объекта информатизации, и, в первую очередь, АСУ ОВГУ. Обеспечение кибербезопасности АСУ ОВГУ должно осуществляется единой интеллектуальной системой кибербезопасности, являющейся частью системы информационной безопасности. При этом в основу построения перспективной системы кибербезопасности должно быть положено понятие ***эволюции*** системы, т.е. способность её адаптации через изменение параметров под воздействием

* Первая часть опубликована в №1 за 2013 г.

внешних и внутренних киберугроз (кибератак) и применяемых технологий противодействия им на протяжении своего жизненного цикла [3-11].

Эволюционирующая интеллектуальная система кибербезопасности АСУ ОВГУ должна обеспечить не только обнаружение новых и неизвестных киберугроз и кибератак в ходе мониторинга (разведки) киберпространства, но и анализ выявленных киберугроз (кибератак) и автоматический выбор параметров функционирования АСУ в условиях деструктивных воздействий без ухудшения ее основных характеристик.

В системе кибербезопасности АСУ ОВГУ также должны быть реализованы возможности: автоматического изменения свойств и параметров систем и средств обеспечения кибербезопасности в зависимости от изменения состояния киберпространства (выявления активности потенциальных источников киберугроз, обнаружения кибератак) и результатов проведенных кибератак; автоматической оценки изменения уровня защищенности АСУ от киберугроз при изменении условий функционирования; автоматизированной поддержки принятия решений о противодействии кибератакам и автоматическое воздействие на источники кибератак; автоматизированной поддержки принятия решения о перераспределении ресурсов систем и средств кибербезопасности в случае их функционального поражения в результате кибератак; учета в процессе обеспечения кибербезопасности всех взаимосвязанных, взаимодействующих и изменяющихся во времени факторов, влияющих на уровень кибербезопасности АСУ; снижения нецелевой нагрузки на комплекс средств автоматизации системы кибербезопасности АСУ; прогнозирования, на основе заложенных и накопленных в процессе эксплуатации знаний, факторов, влияющих на уровень защищенности АСУ от всех видов киберугроз.

Определяя задачи борьбы с угрозами кибербезопасности, нельзя отбрасывать разработку и реализацию активных способов и методов обеспечения кибербезопасности. Поэтому в системе кибербезопасности АСУ должны быть предусмотрены возможности проведения упреждающих аппаратно-программных воздействий (упреждающих ударов) и активных атак на выявленные источники кибератак, информационные системы и ресурсы противоборствующей стороны, а так же способность к дезинформации противоборствующей стороны об истинных свойствах и параметрах АСУ и ее системы кибербезопасности.

Важнейшим условием создания системы обеспечения кибербезопасности АСУ ОВГУ является применение аппаратной и программной платформ из состава доверенной программно-аппаратной среды [11]. Доверенность – это строгое, гарантированное соответствие необходимым требованиям в части информационной безопасности, надежности и функциональной устойчивости в условиях современного информационного противоборства при соблюдении определенных условий технологической независимости. Под доверенной программно-аппаратной средой следует понимать совокупность технических и программных средств, организационных мер, обеспечивающих создание, применение и развитие систем специального назначения в защищенном исполнении, отвечающих необходимым требованиям информационной безопасности, надежности и функциональной устойчивости, подтвержденных сертификатами соответствия (заключениями) в соответствующих обязательных системах сертификации Российской Федерации (рис.1). Главный критерий «доверенности» - это соответствие требованиям информационной безопасности в современных условиях информационного противоборства. Доверенность аппаратно-программной среды фактически определяется доверенностью используемых аппаратных (программно-аппаратных) средств и программного обеспечения.

Большой опыт ОАО «Концерн «Системпром» по разработке и сертификации по требованиям безопасности информации (ТБИ) систем и комплексов специального назначения в защищенном исполнении и СЗИ позволяет предложить следующий под-

Рис.1. *Реализация основ обеспечения доверенной программно-аппаратной среды*

ход к оценке доверенности используемого программного обеспечения (ПО) и программно-аппаратных средств в соответствии с определенными критериями, в основу которого закладываются неразрывность понятия «доверенность» с гарантиями и уровнями обеспечения информационной безопасности, т.е. главным критерием доверенности должна выступать информационная безопасность.

При этом, доверенность ПО имеет несколько уровней оценки: статус разработчика; доступность исходных кодов; наличие сертификата соответствия (заключения); возможности разработки, тиражирования и поставки ПО, его технической поддержке (см. таблицу 1).

Создание эффективной системы кибербезопасности АСУ ОВГУ предусматривает полнодостаточную реализацию комплексного подхода в обеспечении информационной безопасности изделий и объектов АСУ, заключающегося в рациональном сочетании следующих составляющих: защита от утечки по техническим каналам и противодействие техническим средствам разведки; применение аппаратно-программных средств защиты информации для создания системы защиты информации от НСД; разработки и реализация комплекса организационно-технических мер (рис.2).

Система кибербезопасности АСУ ОВГУ, по мнению авторов, должна включать в себя взаимосвязанные между собой следующие основные функциональные системы: мониторинга (разведки) киберпространства, комплексной защиты информации, оперативного оповещения о кибератаках (угрозах) и активного противодействия им, в свою очередь состоящих из определенных функциональных подсистем.

Предлагаемая структурная схема системы кибербезопасности АСУ ОВГУ представлена на рисунке 3.

Функционирование всех вышеперечисленных систем и подсистем должно быть регламентировано соответствующими нормативными правовыми актами и руководящими документами.

***Таблица 1.**- Уровни доверенности программного обеспечения*

Уровни доверенности ПО	**Критерии оценки доверенности ПО**				
	Разработчик ПО	**Предоставление исходных кодов**	**Наличие сертификата соответствия (заключения) на ПО по ТБИ**	**Наличие аттестованного производства ПО**	**Тиражирование и поставка продукции ПО**
1 уровень доверенности	Российская компания, обладающая всеми необходимыми лицензионными возможностями	Исходные коды ПО в наличии и предъявляются для проверок соответствия ТБИ	В наличии сертификат соответствия (заключение) на ПО по ТБИ (в части отсутствия НДВ) при строгом соответствии РДВ	Аттестованное в рамках сертификации по ТБИ производство	Осуществляется тиражирование и поставка ПО и обеспечивается техподдержка на всех этапах жизненного цикла
2 уровень доверенности	Зарубежная компания, положительно зарекомендовавшая себя на международном рынке	Исходные коды ПО открыты и свободно предъявляются (предоставляются) в части проверок соответствия ТБИ, либо их наличие в сети Интернет	В наличии сертификата соответствия (заключения) на ПО по ТБИ в части отсутствия НДВ при строгом соответствии РДВ, при обязательном условии, что Заявителем на сертификацию является российская компания, обладающая соответствующими лицензиями ФСБ России и лицензиями на разработку и производство ПО	Аттестованное в рамках сертификации по ТБИ производств	Осуществляется тиражирование и поставка ПО и обеспечивается техподдержка на всех этапах жизненного цикла Тиражирование и поставка продукции ПО обеспечивается Заявителем на сертификацию по ТБИ
3 уровень доверенности	Зарубежная компания, положительно зарекомендовавшая себя на международном рынке	Исходные коды ПО предъявляются (предоставляются) по согласованию с Заявителем на сертификацию	Соответствует 2-му уровню доверенности	Соответствует 2-му уровню доверенности	Соответствует 2-му уровню доверенности
4 уровень доверенности	Зарубежная компания	Исходные коды ПО недоступны для проверок на соответствие ТБИ	Соответствует 3-му уровню доверенности	Соответствует 3-му уровню доверенности	Соответствует 3-му уровню доверенности

Далее рассмотрим более подробно основные функциональные системы и подсистемы, их предназначение и возможны й состав.

Система мониторинга (разведки) киберпространства должна представлять собой совокупность специализированных аппаратно-программных средств, предназначенных для оценки обстановки в киберпространстве, систематического сбора и обработки информации о возможных угрозах кибербезопасности АСУ ОВГУ (источники, характер, содержание, масштаб, время и т.п.), прогнозирования возможных вариантов и технологий реализации кибератак и потенциально опасных объектов, способных осуществлять кибератаки, выявления признаков и фактов кибератак на информационные объекты и выдачи информации о возможном воздействии кибератак на информационную инфраструктуру. Ведение разведки в киберпространстве требует цифрового проникновения в сети и компьютеры потенциального противника и предусматривает использование совершенно новых источников, форм и способов сбора данных и информации, разработки новых разведывательных средств и технологий, тактических и технических приемов. На систему мониторинга и разведки киберпространства должна возлагаться функция обеспечения формирования и ведения базы данных по вскрытым (обнаруженным) различным видам и источникам киберугроз (кибератак), что предусматривает создание и ведение каталога потенциальных угроз кибербезопасности и признаков кибервоздействий на информационные ресурсы АСУ ОВГУ, определение номенклатуры потенциальных угроз кибербезопасности, создание и ведение банка критериев обнаружения кибератак на информационные системы.

Комплексная система защиты информации должна включать в свой состав современные системы защиты информации (СЗИ) и средств контроля их эффективности. В состав системы должны входить:

- система предупреждения и обнаружения компьютерных атак (СПОКА);
- подсистема программно-аппаратных средств защиты от НСД;
- подсистема криптографической защиты информации и шифрования;
- подсистема контроля состояния и функциональной устойчивости.

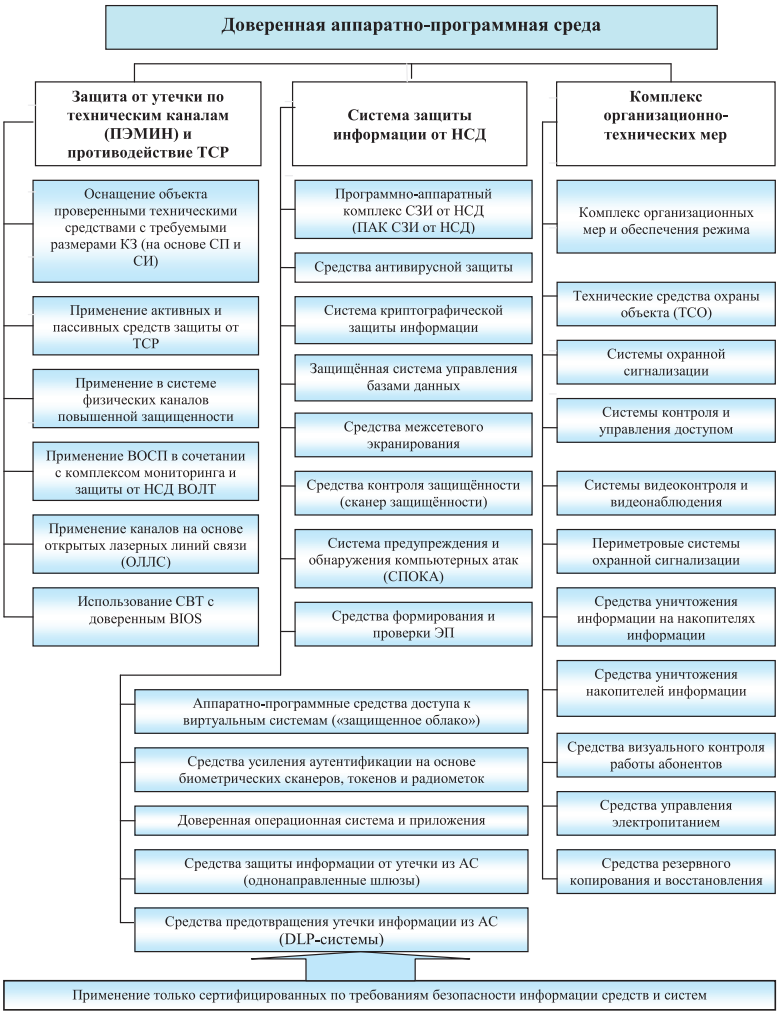


Рис.2. *Реализация комплексного подхода в обеспечении информационной безопасности АСУ ОВГУ*

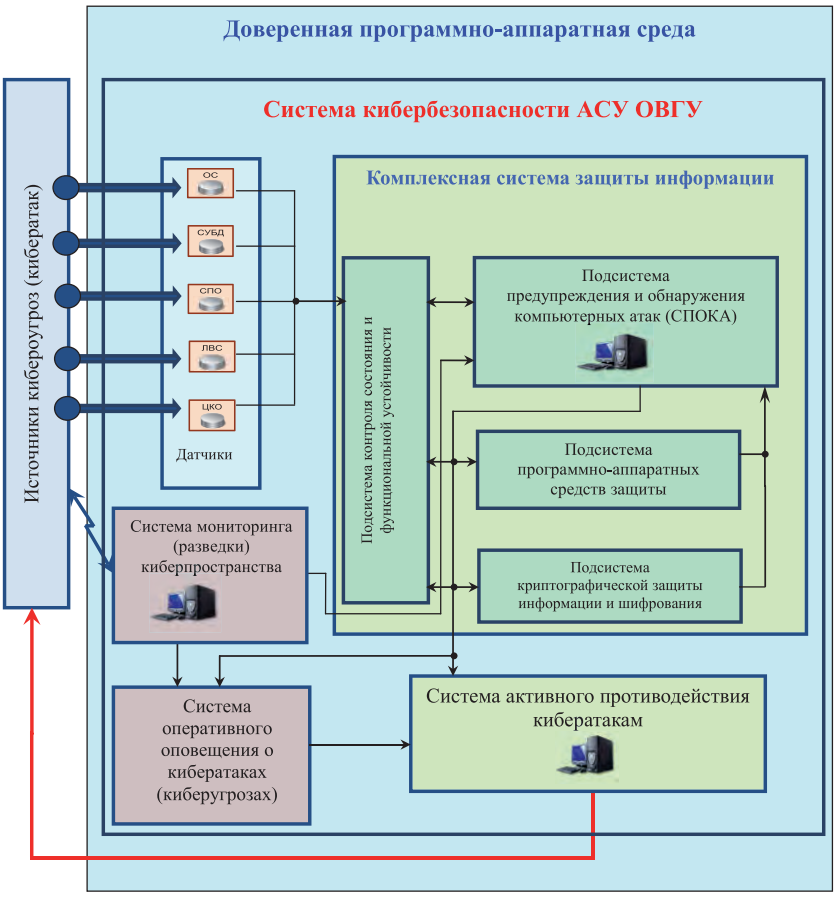


Рис.3. *Структурная схема системы кибербезопасности АСУ ОВГУ*

СПОКА представляет собой совокупность взаимосвязанных программно-аппаратных средств, предназначенных для: прогнозирования сценариев и классификации компьютерных атак; идентификации признаков вторжения и обнаружения компьютерных атак; анализа уязвимостей и технологических циклов управления; контроля технических и программных средств компьютера, информационной системы или сети с целью предупреждения о возможном вторжении; применения методов противодействия компьютерным атакам; оценки и обеспечения функциональной устойчивости функционирования АСУ в условиях кибератак.

Подсистема программно-аппаратных средств защиты от НСД должна включать в свой состав, помимо традиционно применяемых систем и средств защиты (идентификации и аутентификации пользователей, средства разграничения доступа, антивирусной защиты, защищенные системы управления базами данных, средства межсетевого экранирования), также средства формирования и проверки электронной подписи; аппаратно-программные средства доступа к виртуальным системам («защищенное облако»); средства усиления аутентификации на основе биометрических сканеров, токенов и радиометок; средства защиты информации от утечки (однонаправленные шлюзы) и средства предотвращения утечки информации из АС (DLP-системы); средства контроля защищенности (сканер защищенности); программно-аппаратные средства защиты информации технологии «тонкий клиент»; средства защиты от спама и др.

Необходимо также безусловное применение технических средств охраны СВТ, обрабатывающих критически важную информацию и комплексов средств защиты от ИТР и РЭБ.

Подсистема криптографической защиты информации и шифрования представляет собой совокупность аппаратных, программных и аппаратно-программных средства, систем и комплексов, предназначенных для защиты информации, циркулирующей в технических средствах, при ее обработке, хранении и передаче по каналам связи, включая шифровальную технику и обеспечивающих криптографическое преобразование информации и управление процессом распределения ключей. Средства криптографии и шифрования должны защищать не только информации внутри сети и каналах связи, ни и внутренние информационные ресурсы технических средств (внутренние и внешние носители информации) и являются самым сильным рубежом защиты в системе обеспечения кибербезопасности.

Подсистема контроля состояния и функциональной устойчивости предназначена для обеспечения непрерывного контроля состояния и функциональной устойчивости АСУ, ее системы защиты с выдачей информации и рекомендаций в систему управления кибербезопасностью с принятием адекватных мер по корректировке работы СЗИ для борьбы с текущими кибератакам и осуществление их своевременной плановой (внеплановой) смены. Подсистема должна включать в себя: средства мониторинга и сбора информации о состоянии функциональной устойчивости и параметрах АСУ ОВГУ и ее СЗИ от НСД; средства анализа и оценки количественных показателей уровня защищенности АСУ и ее СЗИ от НСД; средства подготовки и принятия решений для формирования сигналов управления средств регулирования параметров СЗИ АСУ (подсистему адаптации); средства централизованного перехода к новым настройкам СЗИ и т.п.

Система активного противодействия кибератакам должна включать в себя средства выбора оптимальной стратегии противодействия, средства активного воздействия на процесс совершения атаки, средства планирования и ведения упреждающих атакующих действий, а также средства активного поражения критически важных информационных объектов противоборствующей стороны.

Система оперативного оповещения о кибератаках (киберугрозах) должна представлять собой совокупность взаимосвязанных программно-аппаратных и телекоммуникационных средств, предназначенных для организации своевременного доведения информации в режиме реального времени до соответствующих субъектов управления о возможных (выявленных) кибератаках (угрозах), их сущности и параметрах, попытках НСД к информации и принятых (необходимых) мерах защиты и противодействия.

2. ОСНОВНЫЕ НАУЧНО-ТЕХНИЧЕСКИЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ АСУ ОВГУ И ВОЗМОЖНЫЕ ПУТИ ИХ РЕШЕНИЯ

В современных реалиях система национальной безопасности России пока еще во многом не готова как к созданию и обеспечению эффективного и защищенного киберпространства для нужд государства, так и к эффективному противодействию постоянно возрастающим угрозам в киберпространстве, которые реальны для всех, без исключения, элементов военной и государственной организации страны.

Одной из основных проблем является отсутствие глубокой научной проработки вопросов обеспечения кибербезопасности. Огромное количество руководящих, нормативно-методических и прочих документов в области защиты информации разработаны в прошлом веке и не учитывают возможные современные каналы утечки информации. Критическая ситуация сложилась в области телекоммуникационных систем для нужд государственного управления и передачи информации ограниченного доступа, построенных с использованием современного импортного оборудования. Современные АСУ ОВГУ, как правило, построены на базе ПЭВМ импортного производства или на базе комплектующих импортного производства, что также создает предпосылки к утечке информации и успешной реализации кибератак на них.

Важной особенностью является технологическая отсталость российских компаний ИТ-индустрии от ведущих зарубежных вендоров, что неизбежно ведет к опасности масштабных сбоев аппаратных и программных средств. Количества сертифицированных в системе сертификации Минобороны и ФСБ России средств защиты информации явно недостаточно. И это далеко не полный перечень проблемных вопросов.

Мировой опыт обеспечения кибербезопасности говорит о необходимости создания целостной системы, сочетающей организационные, оперативные и технические меры защиты с использованием современных методов прогнозирования, анализа и моделирования ситуаций. При этом важнейшей составной частью этой системы должна являться задача обеспечения кибербезопасность АСУ ОВГУ. Критичность обеспечения киберзащиты подобных АСУ обусловлена тем, что ущерб от реализации угроз кибербезопасности может привести к нарушению управления государством и его Вооруженными Силами, а следовательно – к снижению национальной безопасности государства.

По мнению авторского коллектива, основными направлениями развития и совершенствования системы кибербезопасности АСУ ОВГУ могут являться:

- формирование на государственном уровне единой научно-технической политики в области кибербезопасности, развитие и совершенствование нормативно-правовой базы и формирование единого понятийного аппарата в области кибербезопасности, законодательный перевод кибероружия и суперкомпьютеров в статус образцов вооружения;

- создание единых реестров программных и аппаратных средств, перспективных АСУ ОВГУ (взаимодействующих АСУ, систем и средств связи), рекомендуемых к разработке или внедрению и выработка требований к ним, создание баз данных, касающихся надежности функционирования АСУ, состояния их защищенности, состояния техниче-

ского оборудования, оценки эффективности действующих и внедряемых мер безопасности, создание хранилища эталонного программного обеспечения, используемого в АСУ ОВГУ;

- создание и функционирование системы постоянного мониторинга киберпространства; организация работы по реализации комплекса мер, направленных на своевременное обнаружение, предупреждение, отражение и нейтрализацию угроз кибербезопасности АСУ ОВГУ, разработка методов и средств своевременного выявления угроз и оценки их опасности для АСУ, прогнозирования возможных крупномасштабных киберконфликтов;

- развитие исследований в области математического моделирования процессов обеспечения кибербезопасности АСУ ОВГУ, направленных на разработку вероятных сценариев развития ситуации и поддержку управленческих решений;

- разработка и реализация комплексной целевой программы, определяющей основные направления и мероприятия по построению систем кибербезопасности АСУ ОВГУ с учетом вновь возникающих угроз (информационное оружие [13,14], кибертерроризм, инсайдеры, электромагнитный терроризм), разработку научно-методических основ создания программно-аппаратных средств выявления кибератак, оценки и обеспечения реального уровня защищенности критически важных информационных систем и устойчивости функционирования в условиях активных кибератак с учетом особенностей их функционирования;

- разработка комплекса мер по созданию и внедрению телекоммуникационного оборудования, устойчивого к кибератакам;

- разработка и внедрение импортозамещающих технологий, материалов, комплектующих и других видов продукции, используемых в АСУ ОВГУ и системах кибербезопасности;

- создание отечественных базовых информационных технологий, включающих в себя необходимый и достаточный для функционирования единого информационного пространства комплекс программных средств;

- разработка и создание средств противодействия информационному оружию, развитие и совершенствование программно-технических методов предотвращения утечек, разрушения, уничтожения, искажения и перехвата информации (в том числе и исключения НСД к ней) и криптографических средств ее защиты при передаче по каналам связи, а также интенсификация разработок собственных систем и средств для проведения адекватных мер при применении противоборствующей стороной информационного оружия;

- использование технологии нейронных сетей при построении систем кибербезопасности АСУ ОВГУ, обладающих способностью к обучению на примерах и обобщению данных, адаптироваться к изменению свойств объекта управления и внешней среды, высокой устойчивостью к повреждениям своих элементов в силу изначально заложенного в нейросетевую архитектуру параллелизма;

- формирование специальных испытательных баз (полигонов) для проведения испытаний (проверок) по оценке функциональной устойчивости АСУ ОВГУ и систем кибербезопасности в реальных изменяющихся условиях функционирования с использованием реальных кибератак и сведений по инцидентам, возникающих (появившихся) на объектах АСУ и оценки эффективности систем кибербезопасности;

- разработка современных СЗИ на основе использования технологий и механизмов СПОКА, в том числе отвлечения удара, создания ложных целей, разработка комплексов (механизмов) активного противодействия кибератакам, а также средств подавления источников кибератак и обеспечения ответного противодействия;

- разработку для АСУ ОВГУ специализированных экономически целесообразных информационных технологий, исключающих или в максимальной степени снижающих на технологическом уровне обмен информацией, подлежащей обязательной защите;

- проведение комплекса мероприятий по развитию систем, средств и методов мониторинга и технической оценки уровня реальной защищенности АСУ ОВГУ в условиях кибератак, создание баз данных, содержащих сведения об устойчивости функционирования, состоянии защищенности, оценки эффективности действующих и внедряемых мер кибербезопасности;

- проведение исследований технологий, способов и методов проведения кибератак на информационно-коммуникационные сети и компьютерные системы, особое внимание обратив на выявление и противодействие внедряемым боевым программным агентам [15], и противодействия им;

- разработка основных положений, определяющих возможность, характер и порядок применения средств кибервоздействий в мирное и военное время, особенно в глобальных сетях иностранных государств и увязку их с нормами международного права;

- создание единого государственного ситуационного центра системы мониторинга, контроля и защиты киберпространства информационно-телекоммуникационной инфраструктуры и межведомственных

ситуационных специализированных центров противодействия кибертерроризму и кибератакам;

- совершенствование системы подготовки и переподготовки кадров в области кибербезопасности на базе профильных образовательных учреждений.

Кибербезопасность в настоящее время приобретает значение новой отрасли в нашем военно-промышленном комплексе, предназначенной в конечной цели обеспечить национальную безопасность нашей страны, и отношение к ее формированию должно носить и иметь не ведомственный, а государственный характер. Своевременное планирование и реализация мероприятий обеспечения кибербезопасности и информационного противоборства на глобальном и региональном уровнях становится одним из приоритетных направлений обеспечения национальной безопасности Российской Федерации и должно оказать существенное влияние на ее укрепление.

Литература

1. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) // Вопросы кибербезопасности. 2013. № 1(1). С.2-9.
2. Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А. Кибервойны - реальная угроза национальной безопасности. М.: Изд-во КРАСАНД, 2011. 96 с.
3. Бородакий Ю.В., Лободинский Ю.Г. Информационные технологии в военном деле (основы теории и практического применения) М.: Горячая линия – Телеком, 2008. 394 с.
4. Бородакий Ю.В., Боговик А.В., Карпов Е.А., Курносов В.И., Лободинский Ю.Г., Масановец В.В., Паращук И.Б. Основы теории управления в системах специального назначения. М.: Изд. Управление делами Президента Российской Федерации, 2008. 400 с.
5. Бородакий Ю.В., Лободинский Ю.Г. Эволюция информационных систем - М.: Горячая линия – Телеком, 2011. 368 с.
6. Научно-технический сборник ФГУП «Концерн «Системпром» / Под общей ред. Ю.В.Бородакия - М.: ФГУП «Концерн «Системпром», 2011. № 1 (1).
7. Научно-технический сборник ФГУП «Концерн «Системпром» / Под общей ред. Ю.В.Бородакия - М.: ФГУП «Концерн «Системпром», 2012. № 1 (2).
8. Научно-технический сборник ФГУП «Концерн «Системпром» / Под общей ред. Ю.В.Бородакия - М.: ФГУП «Концерн «Системпром», 2013. № 1-2 (3).
9. Бородакий Ю.В., Миронов А.Г., Добродеев А.Ю., Болдина М.Н. Проблемы и перспективы создания эволюционирующих интеллектуальных систем защиты информации для современных распределенных информационно-управляющих систем и комплексов специального и общего назначения // Научные проблемы национальной безопасности Российской Федерации. 2012. Вып. 5. С. 328.
10. Бородакий Ю.В., Миронов А.Г., Добродеев А.Ю., Болдина М.Н., Бутусов И.В. Перспективные системы защиты информации должны быть интеллектуальными // Защита информации. INSIDE. 2013. № 2. С. 48-51.
11. Бородакий Ю.В., Добродеев А.Ю., Иванова А.И., Куликов Г.В. Перспективная архитектура интеллектуальной системы обеспечения информационной безопасности распределенной автоматизированной системы // Приложение к журналу «Открытое образование». 2006. С. 141-142.
12. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Доверенная среда-основа гарантированной безопасности // «Information Security/Информационная безопасность». 2013. №2. С. 36-37.
13. Расторгуев С.П. Информационная война. Проблемы и модели (Экзистенциальная математика в информационной войне). М.: Гелиос АРВ, 2006. 240 с.
14. Расторгуев С.П. Информационная война. М: Радио и связь, 1999. 416 с.
15. Медин А., Маринин А. Особенности применения киберсредств в межгосударственных военных и во внутренних конфликтах // Зарубежное военное обозрение. 2013. № 3. С. 11-16.

Referens

1. Borodakiy Yu.V., Dobrodeyev A.Yu., Butusov I.V. Kiberbezopasnost kak osnovnoy faktor natsionalnoy i mezhdunarodnoy bezopasnosti KhKhI veka (Chast 1), Voprosy kiberbezopasnosti (Cybersecurity Issues), 2013, No 1(1), pp. 2-9.
2. Parshin S.A., Gorbachev Yu.E., Kozhanov Yu.A. Kibervoyny - realnaya ugroza natsionalnoy bezopasnosti, Moscow, Izd-vo KRASAND, 2011, 96 p.
3. Borodakiy Yu.V., Lobodinskiy Yu.G. Informatsionnyye tekhnologii v voyennom dele (osnovy teorii i prakticheskogo primeneniya), Moscow, Goryachaya liniya - Telekom, 2008, 394 p.
4. Borodakiy Yu.V., Bogovik A.V., Karpov Ye.A., Kurnosov V.I., Lobodinskiy Yu.G., Masanovets V.V., Parashchuk I.B. Osnovy teorii upravleniya v sistemakh spetsialnogo naznacheniya, Moscow, Izd. Upravleniye delami Prezidenta Rossiyskoy Federatsii, 2008, 400 p.
5. Borodakiy Yu.V., Lobodinskiy Yu.G. Evolyutsiya informatsionnykh system, Moscow, Goryachaya liniya - Telekom, 2011, 368 p.
6. Nauchno-tekhnicheskiy sbornik FGUP «Kontsern «Sistemprom», By ed. Yu.V.Borodakiy, Moscow, FGUP «Kontsern «Sistemprom», 2011, No 1 (1).
7. Nauchno-tekhnicheskiy sbornik FGUP «Kontsern «Sistemprom», By ed. Yu.V.Borodakiy, Moscow, FGUP «Kontsern «Sistemprom», 2012, No 1 (2).
8. Nauchno-tekhnicheskiy sbornik FGUP «Kontsern «Sistemprom», By ed. Yu.V.Borodakiy, Moscow, FGUP «Kontsern «Sistemprom», 2013, No 1-2 (3).
9. Borodakiy Yu.V., Mironov A.G., Dobrodeyev A.Yu., Boldina M.N. Problemy i perspektivy sozdaniya evolyutsioniruyushchikh intellektualnykh sistem zashchity informatsii dlya sovremennykh raspredelennykh informatsionno-upravlyayushchikh sistem i kompleksov spetsialnogo i obshchego naznacheniya, Nauchnyye problemy natsionalnoy bezopasnosti Rossiyskoy Federatsii, 2012, Vyp. 5, p. 328.
10. Borodakiy Yu.V., Mironov A.G., Dobrodeyev A.Yu., Boldina M.N., Butusov I.V. Perspektivnyye sistemy zashchity informatsii dolzhny byt intellektualnymi, Zashchita informatsii. INSIDE, 2013, No 2, pp. 48-51.
11. Borodakiy Yu.V., Dobrodeyev A.Yu., Ivanova A.I., Kulikov G.V. Perspektivnaya arkhitektura intellektualnoy sistemy obespecheniya informatsionnoy bezopasnosti raspredelennoy avtomatizirovannoy sistemy, Prilozheniye k zhurnalu «Otkrytoye obrazovaniye», 2006, pp.141-142.
12. Borodakiy Yu.V., Dobrodeyev A.Yu., Butusov I.V. Doverennaya sreda-osnova garantirovannoy bezopasnosti, «Information Security/Informatsionnaya bezopasnost», 2013, No2, pp. 36-37.
13. Rastorguyev S.P. Informatsionnaya voyna. Problemy i modeli, Ekzistentsialnaya matematika v informatsionnoy voyne, Moscow, Gelios ARV, 2006, 240 p.
14. Rastorguyev S.P. Informatsionnaya voyna, Moscow, Radio i svyaz, 1999, 416 p.
15. Medin A., Marinin A. Osobennosti primeneniya kibersredstv v mezhgosudarstvennykh voyennykh i vo vnutrennikh konfliktakh, Zarubezhnoye voyennoye obozreniye (Foreign Military Review), 2013, No 3, pp. 11-16.

ТЕРМИНОЛОГИЧЕСКИЙ БАЗИС В ОБЛАСТИ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

***Макаренко Сергей Иванович**, кандидат технических наук*
***Чукляев Илья Игоревич**, кандидат технических наук, доцент*

В работе предлагается однозначная и непротиворечивая система терминов и определений, в основу которой положены руководящие документы Вооруженных сил США в области информационного противоборства, дополненные материалом международных стандартов и отечественных публикаций данной предметной области.

***Ключевые слова**: информационная война, информационное пространство, информационные воздействия, информационное оружие.*

THE TERMINOLOGICAL BASIS OF THE INFORMATIONAL CONFLICT` AREA

***Sergey Makarenko**, Ph.D.*
***Ilia Chucklyaev**, Ph.D., Associate Professor*

The single–valued and consistent system of terms based on USA Armed Forces` direct documents in the area of informational conflict, which are complemented by international standards and Russian science publications is offered in this work.

***Keywords**: informational warfare, informational space, informational effect, informational weapon*

Адекватное описание противоборства в информационной сфере потребовало формирования соответствующего терминологического базиса. К сожалению, в настоящее время отечественная терминология в данной области, не утверждена официальными документами, а используемые различными авторами термины и определения являются весьма неоднозначными и зачастую противоречивыми. Вместе с тем, в США и странах НАТО еще с 90-х годов введены руководящие документы определяющие терминологию и, зачастую, именно ей руководствуются исследователи в области информационного противоборства.

В работе предлагается однозначная и непротиворечивая система терминов и определений, в основу которой положены открытые источники: руководящие документы Вооруженных сил (ВС) США в области информационного противоборства [1-10], дополненные материалом международных стандартов [11, 13] и публикаций отечественных специалистов [14-26] данной предметной области.

Информационная война

В качестве основного определения в руководящих документах ВС США сформулировано следующие определения информационной войны.

Информационная война – широкомасштабная информационная борьба с применением способов и средств информационного воздействия на противника в интересах достижения целей воздействующей стороны.

По направленности информационных воздействий информационная война, как правило, подразделяется на два основных вида:

- информационно-психологическую (психологическую) войну;
- информационно-техническую войну.

Эксперты ВС США считают, что информационная война может проводиться во всех сферах общественной жизни – в экономике, политике, военном деле, социальных отношениях, сфере духовной жизни и особенно в идеологии. При этом рядом специалистов США введены определения, расширяющие суть данного понятия относительно изложенных в руководящих документах.

Информационная война - комплексное воздействие на систему государственного и военного управления противостоящей стороны, на ее военно-политическое руководство, которое уже в мирное время приводило бы к принятию благоприятных для стороны-инициатора информационного воздействия решений, а в ходе конфликта полностью парализовало бы функционирование инфраструктуры управления противника.

Информационная война – соперничество и организованные действия (информационные операции) конфликтующих сторон в области информационных потенциалов, проводимые с целью снижения возможностей по использованию имеющегося государственного, военного и боевого потенциала противника и сохранения (повышения) возможностей по использованию собственного потенциала.

Информационный потенциал – совокупность информации, зафиксированной на материальных носителях или в любой другой форме, обеспечивающей ее передачу во времени и пространстве потребителям для решения широкого спектра задач, связанных с деятельностью государственных институтов, военно-промышленного комплекса и ВС, а также силы и средства, используемые для получения, обработки, хранения и представления информации; умонастроения людей, использующих эту информацию и способных запускать и контролировать вещественно-энергетические процессы.

Цель информационной войны – такое воздействие на противника, в результате которого он самостоятельно, без принуждения, принимает благоприятные для атакующей стороны решения.

Объекты ведения информационной войны – информационные системы и сети обмена информацией (включая соответствующие линии передач, обрабатывающие центры и человеческие факторы этих систем), а также информационные технологии, используемые в системах вооружений.

Информационная война состоит из совокупности информационных операций, проводимых в информационном пространстве в интересах достижения информационного превосходства.

В настоящее время, содержательная часть понятия «информационная война» применительно к действиям ВС изменились, и сейчас в руководящих документах США и НАТО в основном используется термин «информационная операция». В тоже время область применения термина «информационная война» сместилась в сферу описаний глобальных противоречий между государствами и стратегического информационного противоборства.

Информационное пространство

Информационное пространство – область ведения информационной войны.

Действия в информационном пространстве разворачиваются в:

- технической сфере;
- психологической сфере.

Техническая сфера – область информационного пространства, в которой создается, обрабатывается и накапливается информация. Кроме того, это область, в которой функционируют системы командования, управления, связи, коммуникаций и разведки.

Психологическая сфера – область информационного пространства, которая объединяет мышление личного состава ВС и мирного населения. То есть это область, в которой формируются намерения командиров, доктрины, тактика, методы противоборства, мораль, понятие сплоченности подразделений, уровень подготовки, опыт, понимание ситуации и общественное мнение.

Ряд экспертов ВС США считает целесообразным исключение участия физических средств поражения в информационных действиях (таких как поражение пунктов управления, разрушение инфраструктуры и др.), так как эти действия находятся в физическом пространстве, которое является традиционной областью войны, и объединяет традиционные сферы противоборства - землю, море, воздух и космическое пространство. То есть то пространство, в котором функционируют системы вооружения, военной техники и системы коммуникаций.

Одним из ключевых понятий, которым оперируют специалисты в области информационного противоборства США, является «информационная обстановка», оно по смысловому контексту созвучно «информационному пространству».

Информационная обстановка – совокупность людей, организаций и систем, собирающих, отрабатывающих, доводящих информацию или действующих на ее основе.

Элементы информационной обстановки – руководители, лица, принимающие решения, люди и организации.

Ресурсы информационной обстановки – материальные средства и системы, используемые для сбора, анализа, применения или доведения информации.

Включая понятия ресурса и элементов, можно сформулировать следующее определение информационной обстановки – это сфера, в которой функционируют люди и автоматизированные системы: ведут наблюдение, ориентируются, принимают решения и действуют на основе информации. С этой точки зрения информационная обстановка является «основной обстановкой принятия решений» на земле, на море, в воздухе, в космосе и информационном пространстве.

По взглядам специалистов США, информационная обстановка состоит из трех измерений.

Физическое измерение – это реальный мир, в котором ведутся военные действия на суше, на море, в воздухе и в космосе. Информационные системы и системы связи, их техническая составляющая находится в этом измерении для того, чтобы эти действия могли бы иметь место.

Информационное измерение – место, где информация создается, обрабатывается, распространяется и хранится. Это измерение связывает реальный физический мир с сознанием человека познавательного измерения в качестве входящего источника и преобразует ее в исходящий результат – решение.

Познавательное измерение существует в сознании лица принимающего решение. Это та область, где человек обрабатывает полученную информацию в соответствии с присущим ему комплексом норм, морали, убеждений, культуры и ценностей. Они действуют в качестве ограничений восприятия лицом, принимающим решения при фильтровании информации и получении сознания значимости и взаимосвязи. Информация оценивается и анализируется, чтобы сформировать решения, которые передаются через информационное измерение в область физического мира.

Каждая из составляющих информационной обстановки может быть подвергнута целевому воздействию и являться объектом, который в определенных обстоятельствах может оказать решающее влияние на исход операции (боевых действий) с учетом концептуальной взаимосвязи на основе цикла принятия решения.

Информационные операции

Информационные операции – действия, предпринимаемые для достижения информационного превосходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой собственной информации и информационных систем и инфраструктуры.

Цель информационных операций – достижение информационного превосходства над противником.

Информационное превосходство – способность собирать, обрабатывать и распределять непрерывный поток информации различного характера, препятствуя противнику делать то же самое.

Информационное превосходство так же может быть определено и через показатели динамики обработки информации.

Информационное превосходство – способность обеспечивать такой темп проведения операции, который превосходит любой возможный темп противника, позволяя доминировать во все время ее проведения, оставаясь непредсказуемым, и действовать, опережая противника в его ответных акциях.

Основные объекты воздействия в ходе информационных операций:

- органы управления государства и его ВС;
- информационно-управляющие системы гражданской инфраструктуры (телекоммуникационные, включая средства массовой информации, транспортные, энергетического комплекса, финансового и промышленного секторов);
- информационно-управляющие элементы военной инфраструктуры (системы связи, разведки, боевого управления, тылового обеспечения, управления оружием);
- линии, каналы связи и передачи данных;
- информация, циркулирующая или хранящаяся в системах управления;
- общество в целом (как гражданское население, так и личный состав ВС), его государственные, экономические и социальные институты;
- средства массовой информации (в первую очередь – электронные);
- руководящий состав и персонал автоматизированных систем управления, участвующий в процессе принятия решений.

В период проведения миротворческих операций объектами воздействия могут быть также военизированные, партизанские и политические организации, религиозные и социальные группы, отдельные лица, открыто или тайно выступающие против присутствия ВС или союзников и препятствующие выполнению ими своей миссии.

Поскольку информационные операции связаны с использованием информации и информационных технологий для воздействия на военные и гражданские системы с целью достижения информационного превосходства над противником, ряд специалистов дают следующее определение информационным операциям.

Информационная операция – это комплекс взаимосвязанных по цели, месту и времени мероприятий и акций, направленных на инициализацию и управление процессами манипулирования информацией, с целью достижения и удержания информационного превосходства путем воздействия на информационные процессы в информационных системах противника.

При этом информационные системы рассматриваются в широком смысле, т.е. не только автоматические и автоматизированные технические системы, но и государство и общество, которые тоже рассматриваются как информационные системы.

Информационные операции есть основа ведения информационной войны. Информационные операции являются самостоятельным видом оперативного обеспечения, который реализует на поле боя концепцию информационной войны.

По целям и задачам информационные операции подразделяются на:

- информационное обеспечение;
- специальные информационные операции;
- информационное противоборство.

По уровню управления, на которое осуществляется воздействие, и масштабу воздействия информационные операции могут быть классифицированы на:

- стратегические операции, проводятся по решению военно-политического руководства страны, являются воздействием на элементы государственного устройства потенциальных противников (политические, военные, экономические и информационные) при одновременной защите своих государственных структур и призваны обеспечить достижение национальных стратегических целей;
- оперативные операции, проводятся для обеспечения успешного хода военной операции или кампании в целом или решения ее главных задач, являются воздействием на линии связи, системы тылового обеспечения и боевого управления ВС противника при одновременной защите аналогичных собственных систем, так и союзников;
- тактические операции, проводятся с целью обеспечения решения тактических военных задач и сосредоточены на воздействии на информацию и информационные системы, такие, как системы связи, боевого управления, разведки и другие, непосредственно обеспечивающие ведение боевых действий соединениями и частями противника при одновременной защите своих систем.

По характеру решаемых задач информационные операции могут быть:

- оборонительными,
- наступательными.

Оборонительные информационные операции – взаимосвязанные процессы по защите информационной среды, вскрытию признаков нападения, восстановлению боеспособности и организации ответных действий на агрессию (нападение).

Цель оборонительных информационных операций – обеспечение выполнения целевых задач информационными и управляющими системами в условиях ведения информационной войны, а также обеспечение сохранности информационных ресурсов и предотвращения утечки, искажения, утраты или хищения информации в результате несанкционированного доступа к ней со стороны противника.

Оборонительные информационные операции включают мероприятия по обеспечению безопасности собственных информационных ресурсов:

- оперативная маскировка;
- обеспечение физической безопасности информационной инфраструктуры;
- обеспечение безопасности информации и скрытности действий войск (сил);
- вскрытие мероприятий по оперативной маскировке противника;
- контрпропаганда и контрдезинформация;
- контрразведка;
- радиоэлектронная защита;
- специальные информационные операции.

Оборонительные информационные операции должны обеспечивать своевременность и точность передачи данных, гарантированный доступ к ним пользователей в условиях информационного воздействия противника. В ходе их предусматривается проведение мероприятий по восстановлению боеспособности информационных систем.

Наступательные информационные операции представляют собой комплексное проведение по единому замыслу и плану мероприятий по оперативной маскировке, радиоэлектронной борьбе, программно-математическому воздействию на информационно-управляющие системы, физическому уничтожению (или выводу из строя) объектов информационной инфраструктуры.

Цель наступательных информационных операций – достижение и удержание информационного превосходства в ходе информационной войны.

В ходе таких операций принимаются меры, оказывающие воздействие на сознание людей и направленные на срыв процесса принятия решений, а также действия с целью нарушения работы или уничтожения элементов информационной инфраструктуры.

Наступательные информационные операции включают следующие мероприятия по достижению и удержанию информационного превосходства:

- оперативная маскировка;
- психологические операции;
- радиоэлектронная борьба;
- физическое разрушение и уничтожение объектов информационной инфраструктуры;
- программно-математические воздействия и атаки на компьютерные сети противника.

При проведении наступательных информационных операций основными традиционными

методами являются психологические операции и мероприятия по оперативной маскировке, традиционно применявшиеся для оказания влияния на сознание людей в процессе принятия ими решений, а также такие действия, как радиоэлектронное подавление и использование средств физического уничтожения, направленные на нарушение функционирования или уничтожение элементов информационной инфраструктуры. К достаточно новым методам в данном случае можно отнести специальные программно-математические воздействия на компьютерные сети противника и специальные информационные операции.

Оперативная маскировка – мероприятия, проводящиеся под руководством командующих объединенными группировками войск (сил), в интересах оказания воздействий на органы принятия решений противника через его системы сбора, анализа и распределения информации путем предоставления им заведомо ложной информации и скрытия признаков реальной деятельности войск (сил).

Цель оперативной маскировки состоит в том, чтобы запутать, дезинформировать разведывательные органы противника, заставить их делать неправильные выводы и, как следствие, добиться от военного руководства противника неверных действий. Эти мероприятия позволяют также опередить противника в принятии решения.

Оперативная маскировка предполагает применение следующих способов:

- дезинформация – распространение заведомо ложной информации о составе, состоянии, дислокации, боеготовности своих войск, их группировках, характере и способах решения задач, планах, предназначении и состоянии военной техники и объектов;
- имитация – воспроизведение правдоподобных демаскирующих признаков, характерных для реальной деятельности войск (объектов), создание радиоэлектронной обстановки с использованием имитаторов, радиотехнических устройств, ложных сооружений и объектов, макетов военной техники и т. д.;
- демонстративные действия – преднамеренный показ противнику специально выделенными силами и средствами активной деятельности в целях его дезориентации и скрытия истинных намерений организаторов;
- обеспечение скрытности действий – определение признаков, распознаваемых разведывательными системами противника и позволяющих ему на основе их анализа получать особо важную и своевременную информацию; выбор и проведение мероприятий, которые обеспечивали бы скрытие этих признаков и тем самым снижали бы до приемлемого уровня уязвимость союзников от действий разведки противника.

Успех проведения мероприятий по оперативной маскировке в определяющей степени зависит от эффективности разведывательного обеспечения. Разведка в этом случае осуществляет вскрытие объектов противника, в отношении которых замышляются эти действия, оказывает помощь в разработке правдоподобной версии, предлагаемой для дезинформации, выборе наиболее перспективных объектов для реализации дезинформации и оценивает эффективность проведенных мероприятий.

Психологические операции – мероприятия по распространению специально подготовленной информации с целью оказания воздействия на эмоциональное состояние, мотивацию и аргументацию действий, принимаемые решения и поведение отдельных руководителей, организаций, социальных или национальных групп и отдельных личностей противника в благоприятном для государства и их союзников направлении.

Радиоэлектронная борьба подразделяется на:

- радиоэлектронное подавление;
- радиоэлектронную защиту;
- радиоэлектронное обеспечение.

Радиоэлектронное подавление – действия наступательного характера, предпринимаемые с целью дезорганизовать, нейтрализовать или снизить возможности противника по эффективному использованию им радиоэлектронных систем в различных звеньях управления ВС.

Радиоэлектронная защита – такие действия, как защита своих радиоэлектронных средств (РЭС) от помех, создаваемых противником, и осуществление контроля (наблюдения) за работой РЭС союзников, с целью исключения их взаимного влияния друг на друга.

Радиоэлектронное обеспечение представляет собой действия, направленные на обнаружение, идентификацию и определение местоположения РЭС противника, которые могут являться как источниками получения разведданных, так и источниками информационных угроз.

Физическое уничтожение элементов информационной инфраструктуры рассматривается как проводимые в ходе информационной операции действия по применению средств огневого поражения и физического уничтожения с целью вывода из строя ключевых элементов системы управления и связи противника.

Программно-математическое воздействие на компьютерные сети (компьютерные атаки)

определяется как действия с применением аппаратно-программных средств, направленные на использование, искажение, подмену или уничтожение информации, содержащейся в базах данных компьютеров и информационных сетей, а также на снижение эффективности функционирования либо вывод из строя самих компьютеров и компьютерных сетей.

Так же среди наступательных информационных операций в ВС США выделяют борьбу с системами управления как самостоятельный вид боевого обеспечения. При организации информационных операций, действия по борьбе с системами управления централизованно интегрируются в них и становятся их неотъемлемыми элементами.

Борьба с системами управления – деструктивное воздействие на информационные системы противника и циркулирующую в них информацию или уничтожение их. При этом целевыми объектами воздействия являются системы управления и связи противника.

Информационное воздействие

Информационное воздействие (информационное нападение) представляет собой наступательную составляющую информационной войны и реализуется посредством наступательных информационных операций.

Информационное воздействие – основной поражающий фактор информационной войны, представляющий собой воздействие информационным потоком на объект атаки – информационную систему или ее компонент, с целью вызвать в нем в результате приема и обработки данного потока заданные структурные и/или функциональные изменения.

Объект информационного воздействия – множество элементов информационной системы, принадлежащих или способных принадлежать сфере управления, и имеющих потенциальные ресурсы для перепрограммирования на достижение целей, чуждых данной системе, но выгодных противнику.

Объектами воздействия и защиты в ходе информационно-психологической борьбы являются психика личного состава ВС и населения противостоящих сторон, системы формирования общественного мнения и принятия решений.

Объектами воздействия и защиты в ходе информационно-технической войны являются информационно-технические системы (системы связи и управления, телекоммуникационные системы, радиоэлектронные средства, компьютерные сети и т.д.).

Для каждой информационной сферы характерны свои объекты воздействия и средства поражения. Различают следующие **объекты информационного воздействия**:

- одиночные (отдельные узлы связи или компьютерная сеть и др.);
- групповые (например, элементы территориально распределенной информационно-управляющей системы).

Средства воздействия также классифицируют по характеру поражающих свойств:

- высокоточное воздействие (на определенный ресурс в информационно-вычислительной сети);
- комплексное воздействие (вся телекоммуникационная инфраструктура информационно-вычислительной системы).

При этом тип воздействия может быть:

- разрушающим;
- манипулирующим;
- блокирующим.

Степень поражения информационным воздействием – емкость той части объекта информационного воздействия, которая либо уничтожена, либо работает на цели, чуждые собственной системе, но выгодные противнику.

Используемая в настоящее время концепция информационной войны предусматривает следующие информационные воздействия:

- подавление (в военное время) элементов инфраструктуры государственного и военного управления (поражение центров командования и управления);
- электромагнитное воздействие на элементы информационных и телекоммуникационных систем (радиоэлектронная борьба);
- получение разведывательной информации путем перехвата и дешифрования информационных потоков, передаваемых по каналам связи, а также по побочным излучениям и за счет специального внедрения технических средств перехвата информации;
- осуществление несанкционированного доступа к информационным ресурсам (путем использования программно-аппаратных средств, прорыва систем защиты информационных и телекоммуникационных систем противника) с последующим их искажением, уничтожением или хищением, либо нарушение нормального функционирования этих систем;
- формирование и массовое распространение по информационным каналам противника или глобальным сетям дезинформации или тенденциозной информации для воздей-

ствия на оценки, намерения и ориентацию населения и лиц, принимающих решения;
- получение интересующей информации путем перехвата и обработки открытой информации, передаваемой по незащищенным каналам связи, циркулирующей в информационных системах, а также публикуемой в открытой печати и средствах массовой информации.

Информационное оружие

Информационное оружие – совокупность методов и средств информационного воздействия на технику и людей.

При этом данное определение может быть сформулировано более развернуто.

Информационное оружие – это совокупность специально организованной информации и информационных технологий, позволяющая целенаправленно изменять (уничтожать, искажать), копировать, блокировать информацию, преодолевать системы защиты, ограничивать допуск законных пользователей, осуществлять дезинформацию, нарушать функционирование носителей информации, дезорганизовывать работу технических средств, компьютерных систем и информационно-вычислительных сетей, применяемая в ходе информационной борьбы для достижения поставленных целей.

В соответствие с видами информационной борьбы информационное оружие подразделяется на два основных вида:
- информационно-техническое (так же включает в себя **программно-математическое оружие**);
- информационно-психологическое (включает в себя психофизическое оружие).

Главными объектами информационного оружия первого вида является технические средства, второго – люди.

Психофизическое оружие – это совокупность всех возможных методов и средств (технотронных, суггестивных, психотропных, комплексных и др.) скрытого насильственного воздействия на подсознание человека с целью модификации его сознания, поведения и физиологического состояния в нужном для воздействующей стороны направлении. Психофизическое оружие представляет собой разновидность информационно-психологического оружия.

Информационное оружие, по сути, является информационной технологией, включающей в себя:
- анализ способов и механизмов активизации у конкретной системы – противника, заложенных в нее программ самоуничтожения;
- поиск программы самоуничтожения;
- разработка конкретного информационного оружия;
- применение информационного оружия по заданному объекту.

Средства информационного воздействия – средства, используемые в качестве информационного оружия.

Средства специального программно-математического воздействия – некоторая самостоятельная программа (набор инструкций), которая способна выполнить любое подмножество перечисленных ниже функций:
- скрывать признаки своего присутствия в программно-аппаратной среде системы;
- обладать способностью к самокопированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать) код программ в оперативной памяти;
- сохранять фрагменты информации из оперативной памяти в некоторой области внешней памяти прямого доступа (локальной и удаленной);
- искажать, блокировать и/или подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных;
- подавлять информационный обмен в телекоммуникационных сетях, фальсифицировать информацию в каналах управления;
- противодействовать работе тестовых программ и систем защиты информационных ресурсов.

Способы программно-математического воздействия можно подразделить на следующие:
- «логические бомбы» – скрытые управляющие программы, которые по определенному сигналу или в установленное время осуществляют несанкционированный доступ к информации, нарушает управление информационными ресурсами либо дезорганизует работу технических средств;
- компьютерные вирусы, представляющие собой специализированные программные продукты, которые способны воспроизводить «логические бомбы», внедрять их дистанционно в информационные сети противника, и обладают способностью к самокопированию;
- программные продукты типа «троянский конь» – программы, внедрение которых по-

зволяет осуществлять скрытый несанкционированный доступ к информационным ресурсам противника для добывания разведданных или проведения информационного воздействия;
- нейтрализаторы тестовых программ, обеспечивающие сохранение естественных и искусственных недостатков программного обеспечения;
- преднамеренно созданные, скрытые от обычного пользователя интерфейсы для входа в систему.

В соответствии с различными основаниями информационное оружие можно классифицировать следующим образом.

По цели использования информационное оружие подразделяют на:
- обеспечивающее;
- атакующее.

Обеспечивающее информационное оружие – оружие, с помощью которого оказываются информационные воздействия на средства защиты информации атакуемой системы.

В состав обеспечивающего информационного оружия входят:
- средства компьютерной разведки;
- средства преодоления системы защиты.

Успешное применение обеспечивающего информационного оружия позволяет осуществлять деструктивные воздействия на хранимую, обрабатываемую и передаваемую в системе информацию с использованием атакующего информационного оружия.

Атакующее информационное оружие – оружие, с помощью которого осуществляется воздействие на хранимую, обрабатываемую и передаваемую в системе информацию, нарушающее применяемые информационные технологии.

В составе атакующего информационного оружия выделяют четыре основных вида средств информационных воздействий:
- средства нарушения конфиденциальности информации;
- средства нарушения целостности информации;
- средства нарушения доступности информации;
- средства психологических воздействий на абонентов информационной системы.

Применение атакующего информационного оружия направлено на срыв выполнения информационной системой целевых задач.

По способу реализации информационное оружие можно разделить на три класса:
- математическое (алгоритмическое);
- программное;
- аппаратное.

Информационное оружие, относящееся к разным классам, может применяться совместно, а также некоторые виды информационного оружия могут нести в себе черты нескольких классов.

К **алгоритмическому информационному оружию** относится:
- алгоритмы, использующие сочетание санкционированных действий для осуществления несанкционированного доступа к информационным ресурсам;
- алгоритмы применения санкционированного (легального) программного обеспечения и программные средства несанкционированного доступа для осуществления незаконного доступа к информационным ресурсам.

К **программному информационному оружию** относятся программы с потенциально опасными последствиями своей работы для информационных ресурсов системы.

К **аппаратному информационному оружию** относятся средства функционального поражения информационных ресурсов системы, а также аппаратные закладки в интересах нарушения функционирования или несанкционированного доступа к информационным ресурсам.

В целом основные понятия концепции информационного противоборства в том виде, в каком они приняты в ВС США, не являются новыми для российской теории военного искусства. Теоретические основы информационного противоборства достаточно полно раскрыты в российской военной науке через понятия «борьба с системами управления противника», «радиоэлектронная война», «завоевание господства в эфире», «психологическая война», «дезинформация», «военная хитрость» и т. п. Новизна подхода ВС США к теории информационного противоборства заключается в комплексном использовании военно-теоретических разработок по данной тематике, основанных на своих технологических достижениях в области информатики. Данный комплексный подход представлен в настоящей работе и предлагается специалистам для использования в интересах развития отечественной теории информационного противоборства.

Литература

1. Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. - Washington D.C.: The White House, 2009.
2. Informational Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. - Washington D.C.: The White House, 2011.
3. Department of Defense Strategy for Operating in Cyberspace. - Washington D.C.: U.S. Department of Defense, 2011.
4. AFDD 3-12. Cyberspace Operations. USAF, 2010, 60 p.
5. AFDD 3-13. Information Operations. USAF, 2011, 65 p.
6. AFPD 10-7. Information Operations. USAF, 2006, 29 p.
7. DoDD 3600.1. Information Operations. US DoD, 2013, 12 p.
8. Information Operations Primer: Fundamentals of Information Operations. U.S. Army War College, 2011, 204 p.
9. JP 3-13. Information Operations. US Joint Chiefs of Staff, 2012. 69 p.
10. JP 3-13.1. Electronic Warfare. US Joint Chiefs of Staff, 2007. 115 p.
11. Стандарт ISO/IEC 27032:2012. Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности. 2012.
12. Стандарт ITU-T X.1205:2008. Обзор кибербезопасности. 2008. – Женева: МСЭ-Т, 2008. – 162 с. – URL: www.itu.int/ITU-T (дата доступа 20.01.2014)
13. Безопасность в электросвязи и информационных технологиях. Обзор содержания и применения действующих Рекомендаций МСЭ-Т для обеспечения защищенной электросвязи. – Женева: МСЭ-Т, 2009. – 162 с. – URL: www.itu.int/ITU-T (дата доступа 20.01.2014)
14. Гриняев С.Н. Поле битвы - киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны. – М.: Харвест, 2004. – 426 с.
15. Расторгуев С.П. Информационная война. – М: Радио и связь, 1999. – 416 с.
16. Почепцов Г.Г. Информационные войны. – М.: Рефл-бук, К.: Ваклер, 2000. – 576 с.
17. Жуков В. Взгляды военного руководства США на ведение информационной войны // Зарубежное военное обозрение. № 1 2001. - URL: http://pentagonus.ru/publ/22-1-0-175
18. Куннакова Н.Л. Информационная война как объект научного анализа // Альманах современной науки и образования, №6 (61), 2012. – 93-96 с.
19. Антонович П.И., Шаравов И.В., Лойко В.В. Сущность операций в кибернетическом пространстве и их роль в достижении информационного превосходства // Вестник Академии военных наук. № 1 (38). 2012. С. 41-45.
20. Антонович П.И. Изменение взглядов на информационное противоборство на современном этапе // Вестник Академии военных наук. № 1 (34). 2011. С. 43-47.
21. Антонович П.И. О современном понимании термина «кибервойна» // Вестник Академии военных наук. № 2 (35). 2011. С. 89-96.
22. Антонович П.И. О сущности и содержании кибервойны// Военная мысль. № 7. 2011. С. 39-46.
23. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) // Вопросы кибербезопасности. № 1 (1). 2013. С. 2-9.
24. Зубарев И.В., Жидков И.В., Кадушкин И.В. Кибербезопасность автоматизированных систем управления военного назначения // Вопросы кибербезопасности. № 1 (1). 2013. С. 10-16.
25. Макаренко С. И. Проблемы и перспективы применения кибернетического оружия в современной сетецентрической войне // Спецтехника и связь. № 3. 2011. С. 41-47. - URL: http://www.st-s.su/sites/default/files/files/pdf/2011-03/2011-03-makarenko.pdf
26. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М.А. Шолохова, 2009. – 372 с.

References

1. Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. - Washington D.C.: The White House, 2009.
2. Informational Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. - Washington D.C.: The White House, 2011.
3. Department of Defense Strategy for Operating in Cyberspace. - Washington D.C.: U.S. Department of Defense, 2011.
4. AFDD 3-12. Cyberspace Operations. USAF, 2010, 60 p.
5. AFDD 3-13. Information Operations. USAF, 2011, 65 p.
6. AFPD 10-7. Information Operations. USAF, 2006, 29 p.
7. DoDD 3600.1. Information Operations. US DoD, 2013, 12 p.
8. Information Operations Primer: Fundamentals of Information Operations. U.S. Army War College, 2011, 204 p.
9. JP 3-13. Information Operations. US Joint Chiefs of Staff, 2012. 69 p.
10. JP 3-13.1. Electronic Warfare. US Joint Chiefs of Staff, 2007. 115 p.
11. Standart ISO/IEC 27032:2012. Informatsionnye tekhnologii. Metody obespecheniia bezopasnosti. Rukovodiashchie ukazaniia po obespecheniiu kiberbezopasnosti. 2012.
12. Standart ITU-T X.1205:2008. Obzor kiberbezopasnosti. 2008. – Zheneva: MSE-T, 2008. – 162 p. – URL: www.itu.int/ITU-T (data dostupa 20.01.2014).
13. Bezopasnost' v elektrosviazi i informatsionnykh tekhnologiiakh. Obzor soderzhaniia i primeneniia deistvuiushchikh Rekomendatsii MSE-T dlia obespecheniia zashchishchennoi elektrosviazi. – Zheneva: MSE-T, 2009. – 162 p. – URL: www.itu.int/ITU-T (data dostupa 20.01.2014).
14. Griniaev S.N. Pole bitvy - kiberprostranstvo. Teoriia, priemy, sredstva, metody i sistemy vedeniia informatsionnoi voiny. – M.: Kharvest, 2004. – 426 p.
15. Rastorguev S.P. Informatsionnaia voina. – M: Radio i sviaz', 1999. – 416 p.
16. Pocheptsov G.G. Informatsionnye voiny. – M.: Refl-buk, K.: Vakler, 2000. – 576 p.
17. Zhukov V. Vzgliady voennogo rukovodstva SShA na vedenie informatsionnoi voiny. Zarubezhnoe voennoe obozrenie. No 1 2001. - URL: http://pentagonus.ru/publ/22-1-0-175
18. Kunnakova N.L. Informatsionnaia voina kak ob»ekt nauchnogo analiza. Al'manakh sovremennoi nauki i obrazovaniia, No 6 (61), 2012. – pp 93-96.
19. Antonovich P.I., Sharavov I.V., Loiko V.V. Sushchnost' operatsii v kiberneticheskom prostranstve i ikh rol' v dostizhenii informatsionnogo prevoskhodstva. Vestnik Akademii voennykh nauk. No 1 (38). 2012. pp. 41-45.
20. Antonovich P.I. Izmenenie vzgliadov na informatsionnoe protivoborstvo na sovremennom etape. Vestnik Akademii voennykh nauk. No 1 (34). 2011. pp. 43-47.
21. Antonovich P.I. O sovremennom ponimanii termina «kibervoina». Vestnik Akademii voennykh nauk. No 2 (35). 2011. pp. 89-96.
22. Antonovich P.I. O sushchnosti i soderzhanii kibervoiny. Voennaia mysl'. No 7. 2011. pp. 39-46.
23. Borodakii Iu.V., Dobrodeev A.Iu., Butusov I.V. Kiberbezopasnost' kak osnovnoi faktor natsional'noi i mezhdunarodnoi bezopasnosti XXI veka (Chast' 1). Voprosy kiberbezopasnosti. No 1 (1). 2013. pp. 2-9.
24. Zubarev I.V., Zhidkov I.V., Kadushkin I.V. Kiberbezopasnost' avtomatizirovannykh sistem upravleniia voennogo naznacheniia. Voprosy kiberbezopasnosti. No 1 (1). 2013. pp. 10-16.
25. Makarenko S. I. Problemy i perspektivy primeneniia kiberneticheskogo oruzhiia v sovremennoi setetsentricheskoi voine. Spetstekhnika i sviaz'. No 3. 2011. pp. 41-47. - URL: http://www.st-s.su/sites/default/files/files/pdf/2011-03/2011-03-makarenko.pdf.
26. Makarenko S. I. Informatsionnaia bezopasnost': uchebnoe posobie dlia studentov vuzov. – Stavropol': SF MGGU im. M.A. Sholokhova, 2009. – 372 p.

КИБЕРБЕЗОПАСНОСТЬ – ПОДХОДЫ К ОПРЕДЕЛЕНИЮ ПОНЯТИЯ

***Безкоровайный Михаил Михайлович**, кандидат технических наук, доцент*
***Татузов Александр Леонидович**, доктор технических наук, доцент*

Существенный рост инцидентов, возникающих в информационной сфере, привел к необходимости системного анализа источников возникновения угроз. Для этого необходимы согласованные среди специалистов понятия, ключевым из которых является кибербезопасность. Оно трактуется неоднозначно многими экспертами. В статье предлагается подход к рассмотрению понятия киберпространства и кибербезопасности.

***Ключевые слова**: информационная безопасность, кибербезопасность, киберпространство, киберпреступления.*

CYBERSECURITY - APPROACHES TO THE DEFINITION

***Mikhail Bezkorovainy**, Ph.D. , Associate Professor*
***Alexander Tatuzov**, Doctor of Technical Sciences , Associate Professor*

Many experts treat this concept in different ways. The paper proposes an approach to the consideration of cyberspace and cybersequrity.

***Keywords**: information security, cybersecurity , cyberspace , cybercrime .*

В настоящее время наблюдается резкий рост инцидентов в области информационной безопасности, которые имеют широкое распространение и приобретают угрожающий характер. Многие из подобных атак затрагивают широкий круг частных, корпоративных, а также государственных интересов.

Главными тенденциями развития угроз являются следующие:

- рост числа атак, многие из которых ведут к большим потерям;
- возрастание сложности атак, которые могут включать несколько этапов и применять специальные методы защиты от возможных методов противодействия;
- воздействие практически на все электронные (цифровые) устройства, в числе которых в последнее время все большую значимость приобретают мобильные устройства, а они в наибольшей степени подвержены рискам в области информационной безопасности;
- все более частые случаи нападения на информационную инфраструктуру крупных корпораций, важнейших промышленных объектов и даже государственных структур;
- применение наиболее развитыми в области компьютерных технологий странами средств и методов кибернападения на другие государства.

Это подтверждается практически ежедневными сводками новостей, в которых сообщается о новых атаках преступников в информационной сфере.

Число вредоносных объектов, которые обнаруживаются в сети ежегодно, исчисляется миллиардами, их распространение ведется более чем 100 миллионов интернет адресов [1] [2]. Каждый год это число увеличивается на 40% [3]. Атаки в информационном пространстве наносят ущерб, который оценивается в 100 миллиардов долларов [4]. По заявлению начальника Бюро специальных технических мероприятий МВД России Алексея Мошкова каждую секунду 12 человек на Земле становятся жертвами киберпреступников. Только в России удалось предотвратить хищение около 1 миллиарда рублей с банковских счетов граждан [5].

Особую опасность составляют угрозы мобильным устройствам, которые ранее редко подвергались атакам. За один год практически в 30 раз увеличилось количество Android-троянцев [3].

Появились крайне сложные элементы нападения, направленные на ухудшение работы промышленных объектов. Это обнаруженный в 2009 г.,

и наделавший много шума червь Stuxnet, разработки этого года Duqu и Flame, последний из которых имеет очень сложную архитектуру. Стало известно о причастности специалистов американских спецслужб к созданию этих комплексных вредоносных программ. Государственными структурами ведется финансирование нападений в области киберпространства [6].

Зафиксированы многочисленные атаки на крупнейшие банки США. Эти атаки смогли взломать передовые системы защиты и создать угрозы национальной инфраструктуре. Предположительно, нападения чаще всего организуются из Китая [7]. В начале года была проведена серия атак на крупнейшие американские СМИ [8], что заставило правительство США еще раз серьезно задуматься об усилении кибербезопасности в стране [9].

В 2013 г. Лабораторией Касперского была опубликована информация о совершенно новом явлении в области компьютерных атак. Была раскрыта шпионская сеть «Красный Октябрь (Red October)», на протяжении пяти лет занимающаяся хищением государственных секретов. Это сложнейший комплекс вредоносных программ, около 1000 вредоносных файлов, относящихся к 30 различным группам модулей [10]. Аналогичные методы уже активно применяются и для мобильных устройств на платформе Android [11].

В конце 2012 г. американские и китайские государственные структуры публично высказали свои подозрения в создании оборудования с недокументированными возможностями, посредством которых из одного государства были атакованы сети другой страны. Под подозрением оказалась продукция фирм Huawei и ZTE с китайской стороны и Cisco с американской стороны [12].

Заявления Эдварда Сноудена подтверждают активное участие государственных структур развитых стран в сборе информации о гражданах, чиновниках, корпорациях и других, казалось бы, общедоступных сведений, которые можно агрегировать для достижения кумулятивного эффекта и получения закрытой информации. С целью манипулирования общественным мнением масс людей активно применяются специальные методы социальной инженерии, во многом опирающиеся на средства коммуникаций с помощью Интернета.

Таким образом, имеется ряд проблем в сфере информационной безопасности, которые не могут быть полноценно решены традиционными средствами и на которые следует обратить внимание обществу и государственным органам. Масштабные нарушения, затрагивающие все стороны жизни общества, в основе которых лежат новейшие методы осуществления атак на компьютерные сети, а также управление общественным сознанием требуют системного подхода к созданию комплексной системы безопасности, способной противостоять этим угрозам.

Общий анализ проблематики защиты от подобных, вновь возникающих и продолжающих развиваться угроз, можно обозначить понятием кибербезопасность. Вопросы обеспечения кибербезопасности были проанализированы в работе [13] и была показана необходимость принятия масштабных мер со стороны государства по обеспечению безопасности в области информационных и телекоммуникационных технологий (далее – ИКТ). Речь идет о координации усилий в этом направлении государственных органов, бизнеса и общества в целом.

Столь сложная задача должна решаться на основе ясно выработанной позиции, однозначном понимании того, что имеется в виду под кибербезопасностью. В работе [14] рассмотрены подходы к выработке терминологии в этой области.

Очевидно, что кибербезопасность должна быть нацелена на обеспечение защиты в киберпространстве. Поэтому основным для анализа проблем кибербезопасности является понятие киберпространство.

Для понимания его содержания целесообразно основываться на термине кибернетика. Кибернетика (от греч. «искусство управления») – наука об управлении, связи и переработке информации.

Абстрактная кибернетическая система представляет собой множество взаимосвязанных объектов, называемых элементами системы, способных воспринимать, хранить и перерабатывать информацию, а также обмениваться информацией. То есть, к предметной области кибернетики относятся все современные информационные и телекоммуникационные технологии. Важно, что в рамках кибернетического подхода элементы системы рассматриваются как непрерывно взаимодействующие между собой и в качестве важных составляющих элементов в киберпространство включены люди – активные участники информационного обмена и использования информационных ресурсов.

В начале 2014 г. Советом Федерации для публичного обсуждения был предложен проект Концепции Стратегии кибербезопасности Российской Федерации (далее – Концепция). Он призван определить направления усилий государства в отношении новых угроз, возникающих в современном информационном мире [15].

Понятие кибербезопасности очень многогранно и поэтому непросто и трудно формализуемо.

Здесь существует очень много различных представлений и взглядов.

Специалисты по информационной безопасности и просто заинтересованные пользователи, в частности, те, которые оставили комментарии к Концепции, высказывают очень противоречивые взгляды на эту проблематику. Анализ комментариев показывает, что одной из основных проблем разработки подобных документов заключается в трудности понимания термина киберпространство и соотнесенным с ним понятием кибербезопасность.

Киберпространство в проекте Концепции определяется следующим образом:

«Киберпространство – сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)».

В принципе, такое определение в какой-то степени трактует отдельные аспекты этого важного понятия, но отсутствие дальнейших подробных разъяснений приводит к неточному его пониманию. Абсолютное большинство экспертов, которые оставили свои комментарии к проекту Концепции, считают, что в определении речь идет исключительно о технологической составляющей информационного поля, то есть о компьютерной и телекоммуникационной инфраструктуре. Совсем упущен из рассмотрения вопрос о деятельности на основе этой инфраструктуры и любых видах человеческой активности, которая осуществляется посредством технологий. А об этом прямо сказано в определении. Для документа, имеющего столь важное значение это неприемлемо и указывает на необходимость дальнейшей методологической работы по определению кибербезопасности как характеристики киберпространства.

Приведенное в концепции определение во многом перекликается с позицией международного стандарта ИСО/МЭК 27032:2012 Руководящие указания по кибербезопасности (ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity).

Киберпространство – это сложная среда, не существующая ни в какой физической форме, возникающая в результате взаимодействия людей, ПО, интернет сервисов посредством технологических устройств и сетевых связей.

В программной статье по кибербезопасности специалистами Великобритании определяется это понятие как *всякая деятельность в сетевой, цифровой форме*, добавляя после этого, что *сюда же относятся информационное содержание и действия осуществляемые посредством цифровых сетей*. (Klimburg A. et al. National cyber security framework manual //NATO CCD COE Publications (December 2012). – 2012. http://belfercenter.hks.harvard.edu/files/hathaway-klimburg-nato-manual-ch-1.pdf).

При всем многообразии этих определений можно отметить, что при четком указании на связанность киберпространства с ИКТ инфраструктурой, основное внимание обращено не на технологии, а на деятельность людей, которые используют эти технологии.

Важно, что основное содержание киберпространства заключается в деятельности пользователей цифровыми информационными ресурсами и ИКТ инфраструктурой. Киберпространство можно рассматривать как триаду, которая включает в себя три основные составляющие.

Информация в ее цифровом представлении: статическом (файлы, записанные на носители данных) и динамическом (пакеты, потоки, команды, запросы, и т.д. передаваемые по различным сетям, обрабатываемые в автоматизированных системах и представляемые на средствах отображения в графическом или текстовом виде).

Техническая инфраструктура, ИКТ, программное обеспечение, с помощью которых осуществляется реализация основных действий с информацией: сбор, обработка, хранение и передача. К таким средствам относятся инфраструктура Интернет и сетевых взаимосвязей, компьютеры, всевозможные гаджеты и т.п.

Информационное взаимодействие субъектов с использованием информации получаемой (передаваемой) и обрабатываемой посредством технической инфраструктуры. Здесь имеются в виду все виды деятельности пользователей или участников киберпространства, которые они осуществляют с использованием информационных ресурсов, потоки и хранилища которых располагаются на технической инфраструктуре.

Все эти составляющие в совокупности и образуют сущность, которую можно именовать киберпространством. Можно выделить следующие его основные свойства.

Первое. Киберпространство определено на множестве цифровых устройств и систем на их основе, которые оперируют с информацией или во многом с ее помощью. Важно, что имеются в виду не отдельные системы, а их совокупность, когда подобных устройств (систем) достаточно много. То есть, в общем виде существенное уменьшение

числа функционирующих устройств (систем) в киберпространстве или нарушение их нормальной работы является угрозой киберпространству. Но речь идет не просто об отдельных устройствах (системах), а о большом числе таких объектов и способности оперировать ими информацией (обеспечивать сервисы) с заданным качеством, то есть осуществлять действия, которые обычно связываются с информационными технологиями. Отсюда вытекает второе свойство.

Активное оперирование информацией и сохранение этой информацией главных ее свойств: целостности, доступности, конфиденциальности и других, определяемых в современных стандартах. В отличие от информационной безопасности речь идет не об информации вообще, а о той информации, которая циркулирует в киберпространстве и составляет важную часть ее содержания. Таким образом, нарушение работы отдельного компьютера подключенного к киберпространству или утеря информации, которая в нем содержится, или нарушение ее свойств, безусловно важных для пользователя данного компьютера, вряд ли может рассматриваться как угроза кибербезопасности.

Третье. Наличие «добропорядочных» связей, связей, которые составляют основу киберпространства, и без которых рассматривать поле цифровых устройств (систем) в качестве некоторой новой сущности вряд ли имело бы смысл. Здесь имеется в виду способность киберпространства передавать, получать и обрабатывать информацию с сохранением ее существенных для целей применения свойств.

Четвертое. Собственно понятие кибер-. Оно относится к управлению. Управление в данном случае подразумевает не наличие прямолинейных команд, которые непосредственно исполняются всеми агентами (участниками) киберпространства, а формирование и передача таких сигналов, которые способны придать рассматриваемой области киберпространства некий «разумный» характер поведения и устойчивость к возникающим угрозам.

Способы управления оказывают непосредственное воздействие на структуру киберпространства. Здесь важно учитывать управление технической основой киберпространства и чисто физическими связями между отдельными узлами или даже областями киберпространства. Но определяющую роль играет управление участниками киберпространства: пользователями и их группами. Под управлением понимается комплекс усилий, направленный на повышение квалификации участников, стимулирование благоприятных для развития киберпространства действий и подавление или прямое запрещение злонамеренных действий. Управление субъектами киберпространства играет определяющую роль в возникновении, существовании и поддержке основных свойств этого образования.

Указанные свойства, а именно многочисленность элементов, составляющих киберпространство, обилие взаимосвязей между ними, возможность применения специальных техник управления действиями этих элементов, и определяют развитие тех угроз, о которых говорилось выше. Необыкновенно высокая и все нарастающая интенсивность атак происходит от громадных масштабов киберпространства, всевозможных и разнохарактерных связей между ними. Сложные атаки, имеющие комплексную структуру, опираются на возможность различных направлений распространения информации и сигналов. Использование методов социальной инженерии позволяет изыскивать наиболее продуктивные методы организации атак. В киберпространстве могут развиваться все более опасные и сложные угрозы. Они используют особенности его построения для достижения максимального эффекта.

Но те же самые особенности, проистекающие из многочисленных взаимосвязей между участниками киберпространства, могут стать важным фактором в повышении эффективности систем, которые обеспечивают защиту от подобных угроз [16]. Для этого необходимо координировать усилия всех заинтересованных участников, создавать механизмы, способствующие наилучшему распределению их усилий. Нужно правильно определять возникающие и прогнозируемые опасности и обоснованно выбирать рациональные меры защиты.

Кибербезопасность имеет целью решение этих вопросов и обеспечение нормального функционирования киберпространства, защищая его от возникающих угроз эффективным образом.

Важно правильно сформулировать понятие кибербезопасности, чтобы главные цели работы служб и средств защиты киберпространства от возникающих угроз были точно определены. Однако в концепции приведена формулировка, которая не может удовлетворить этим требованиям.

В проекте Концепции говорится следующее:

«кибербезопасность – совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями».

Кибербезопасность не может быть направлена на защиту от максимального числа угроз. Нужно

обеспечить максимально благоприятную среду для работы пользователей и всех систем в киберпространстве.

Указанная в Концепции постановка неявно призывает разрабатывать и выявлять все новые и новые угрозы, создавая новые средства и способы защиты от них.

Доля ресурсов, необходимых для обеспечения защиты, при таком подходе будет неуклонно расти, а устойчивая работа киберпространства может даже ухудшаться.

Поэтому в определении кибербезопасности основной упор и целевая установка должны быть сделаны на сохранение благоприятного состояния киберпространства, а не на число угроз. Если мы смогли защититься от невообразимо большого числа угроз, но работоспособность киберпространства нарушена, то это хуже, чем защититься от двух десятков угроз и при этом сохранить приемлемый уровень работоспособности.

Кибербезопасность так же, как и киберпространство может описываться триадой составляющих ее сущностей определенных на составных частях киберпространства: информационных ресурсах, компьютерной и сетевой архитектурах (инфраструктуре) и способах взаимодействия пользователей.

Кибербезопасность охватывает уже не только информацию как объект защиты, не исключительно технические средства, которые определяют возможности функционирования информации, а защиту способов функционирования новой сущности – киберпространства. Защищается деятельность людей, которая осуществляется с помощью информации, распространяемой посредством технической инфраструктуры ИКТ.

При обеспечении кибербезопасности важно учитывать указанные особенности киберпространства и ее наиболее важный аспект – наличие взаимосвязей между участниками (пользователями), что приводит к возможности возникновения синергетического эффекта.

В проекте Концепции указывается на необходимость проведения научных исследований в области кибербезопасности, в частности, на реализацию научно-технических программ и исследований в соответствии с «Приоритетными направлениями научных исследований в области обеспечения информационной безопасности Российской Федерации», утвержденными Советом Безопасности Российской Федерации. Но это лишь общая постановка, отсылающая к списку из более 100 направлений, среди которых необходимо выделить наиболее значимые с точки зрения кибербезопасности. На этих направлениях стоит сосредоточить основные усилия. Предложения по таким работам приведены в статье [17]. Кроме того, следует дополнить тематику перспективных исследований направлениями, которые вытекают из основных свойств киберпространства.

Необходимо подробно и тщательно исследовать основные свойства киберпространства, динамику его развития в различных масштабах времени от мгновенных до многолетних, методы управления этой динамикой. Важно обосновать подходы к определению показателей кибербезопасности, разработать модели для их оценки, выработать способы обоснования критериев.

Без проведения системного анализа и получения оценок применения тех или иных мер невозможно построить эффективную систему кибербезопасности.

Представляется целесообразным в комплекс исследований в области кибербезопасности включить следующие направления:

1. Выработка единой терминологии киберпространства и кибербезопасности, гармонизированной с существующей терминологией в области информационной безопасности.

2. Разработка комплексной системы показателей, охватывающих все стороны функционирования киберпространства и обеспечения его защиты от возможных угроз.

3. Разработка моделей самого киберпространства и основных факторов, оказывающих влияние на его функционирование. Безусловно, необходима тщательно продуманная модель угроз. Одним из важнейших направлений является создание математических моделей, позволяющих получать численные характеристики информационной безопасности (степени угроз информационной безопасности, анализа информационных рисков, оценки эффективности мер защиты).

4. Создание специальных методов обеспечения устойчивости киберпространства или его областей при воздействии угроз. Здесь несколько возможным тем:

- анализ топологической структуры и выработка рекомендаций по ее изменению, способов и конкретных алгоритмов их реализации;

- новые методы криптографической защиты, основанные не только на чисто вычислительных механизмах реализации стойкости, но и на использовании преимуществ многосвязной архитектуры связей и большого числа добропорядочных пользователей;

- методы информационной безопасности на основе социальных сервисов для противодействия кибер-атакам с применением специальных процедур анализа группового поведения.

5. Интеллектуальные методы обеспечения кибербезопасности:

- методы интеллектуальной идентификации пользователей;

- интеллектуальные методы предотвращения вирусных и других атак;

- интеллектуальные методы выявления атак и проникновений;

- методы ситуационного анализа состояния информационной безопасности;

- новые методы криптографической защиты, основанные на нейросетевых технологиях.

Литература

1. http://www.securelist.com/ru/analysis/208050763/Razvitie_informatsionnykh_ugroz_vo_vtorom_kvartale_2012_goda.
2. Trustwave 2013-Global-Security-Report
3. http://www.symantec.com/security_response/publications/threatreport.jsp
4. 2012 Norton Cybercrime Report (http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf)
5. http://mvd.ru/news/item/1033853
6. http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report/cyber-attacks.aspx
7. http://www.cybersecurity.ru/crypto/171331.html
8. http://www.politico.com/story/2013/02/washington-cybersecurity-china-attacks-87087.html
9. http://www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html
10. http://habrahabr.ru/company/kaspersky/blog/169839/
11. http://www.itsec.ru/newstext.php?news_id=91005
12. http://www.cybersecurity.ru/telecommunication/165487.html
13. Старовойтов А. В. Кибербезопасность как актуальная проблема современности // Информатизация и связь. – 2011. – №. 6. – С. 4-7.
14. Безкоровайный М. М., Лосев С. А., Татузов А. Л. Кибербезопасность в современном мире: термины и содержание // Информатизация и связь. – 2011. – №. 6. – С. 27-32.
15. http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf
16. Безкоровайный М. М., Татузов А. Л. Подходы к математическому моделированию в области кибербезопасности // Информатизация и связь. – 2012. – №. 8. – С. 21-27.
17. Безкоровайный М. М., Татузов А. Л. Информационная безопасность в сфере образования и науки // Информатизация и связь. – 2011. – №. 6. – С. 34-39.

References

1. http://www.securelist.com/ru/analysis/208050763/Razvitie_informatsionnykh_ugroz_vo_vtorom_kvartale_2012_goda.
2. Trustwave 2013-Global-Security-Report
3. http://www.symantec.com/security_response/publications/threatreport.jsp
4. 2012 Norton Cybercrime Report (http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf)
5. http://mvd.ru/news/item/1033853
6. http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report/cyber-attacks.aspx
7. http://www.cybersecurity.ru/crypto/171331.html
8. http://www.politico.com/story/2013/02/washington-cybersecurity-china-attacks-87087.html
9. http://www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html
10. http://habrahabr.ru/company/kaspersky/blog/169839/
11. http://www.itsec.ru/newstext.php?news_id=91005
12. http://www.cybersecurity.ru/telecommunication/165487.html
13. Starovojtov A. V. Kiberbezopasnost' kak aktual'naja problema sovremennosti (Cybersecurity as an actual modern problem) // Informatizacija i svjaz' (Informatization and communication). – 2011. – №. 6. – P. 4-7.
14. Bezkorovajnyj M. M., Losev S.A., TatuzovA.L. Kiberbezopasnost' v sovremennom mire: terminy i soderzhanie (Cybersecurity in the modern world : terms and content) // Informatizacija i svjaz' (Informatization and communication) – 2011. – №. 6. – P. 27-32.
15. http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf
16. Bezkorovajnyj M. M., TatuzovA.L. Podhody k matematicheskomu modelirovaniju v oblasti kiberbezopasnosti (Approaches to mathematical modelling in sphere of cybersecurity) // Informatizacija i svjaz' (Informatization and communication). – 2011. – №. 6. – P. 21-27.
17. Bezkorovajnyj M. M., TatuzovA.L. Informacionnaja bezopasnost' v sfere obrazovanija i nauki (Information security in the sphere of education and science) // Informatizacija i svjaz' (Informatization and communication). – 2011. – №. 6. – P. 34-39.

РУКОВОДЯЩИЕ УКАЗАНИЯ ПО КИБЕРБЕЗОПАСНОСТИ В КОНТЕКСТЕ ISO 27032

***Марков Алексей Сергеевич**, кандидат технических наук, старший научный сотрудник, CISSP,*
***Цирлов Валентин Леонидович**, кандидат технических наук, CISSP*

Рассмотрен новый стандарт по кибербезопасности ISO/IEC 27032. Проведен анализ понятий, тезауруса и онтологии кибербезопасности в сравнении с категориями информационной безопасности. Рассмотрены руководящие принципы и организационно-технические меры кибербезопасности. Дано краткое описание методов повышения готовности. Отмечены вопросы гармонизации стандарта в рамках российской нормативной базы. Отмечены ограничения, недостатки и область применения стандарта в России.

***Ключевые слова**: кибербезопасность, киберпространство, киберугрозы, кибер-риски, стейкхолдеры, ИСО 27032, ГОСТ 27005, ГОСТ 27000, меры кибербезопасности, методы и средства обеспечения безопасности*

GUIDELINES FOR CYBERSECURITY IN THE CONTEXT OF ISO 27032

***Alexey Markov**, Ph.D., Associate Professor , CISSP*
***Valentin Tsirlov**, Ph.D., CISSP*

The new standard ISO/IEC 27032 on cybersecurity is considered. The concepts, ontologies, thesaurus of the cybersecurity in comparison with categories of information security are analyzed. The guidelines, organizational and technical measures of cibersecurity are discussed. A brief description of the methods to improve readiness is presented. The harmonization of standards in the framework of the Russian is shown. The limitations and prospects of the standard in the Russian are noted.

***Keywords**: cybersecurity, cyber security, cyberspace, cyber threats, cyber risks, stakeholders, ISO 27032, ISO 27000, cybersecurity measures, security techniques*

Введение

В рамках обсуждения концептуальных основ кибербезопасности страны остро стоит вопрос совершенствования соответствующего понятийного аппарата. В литературе сложился ряд направлений толкования определения «кибербезопасность», отражающего различные аспекты военной политики, международного права, критических информационных инфраструктур, информационно-коммуникационных технологий и компьютерных сетей [1-10]. При этом наблюдается смешение формулировок, данных в различных концептуальных и нормативных документах. Что касается последних, то наибольшее внимание уделяют цитированию нового международного стандарта ISO/IEC 27032:2012 Information technology - Security techniques - Guidelines for cybersecurity.

Следует указать, в нашей стране уже сложился ряд национальных стандартов 27000-серии, гармонизированный с международной базой. Рассмотрению положений стандарта ISO 27032 и его связи с российской нормативной базой посвящена данная статья.

Структура стандарта по кибербезопасности

Международный стандарт ISO 27032 выполнен в стиле риск-ориентированного подхода, хотя и отличается от национальных стандартов ГОСТ 27001 и ГОСТ 27005, привязанных к 4-процессной модели жизненного цикла [11,12]. Стандарт определяет активы киберпространства и заинтересованные стороны, угрозы, рекомендации и меры по обработке рисков, причем в качестве специфической меры выделены указания по координации действий и обмену информацией (рис.1).

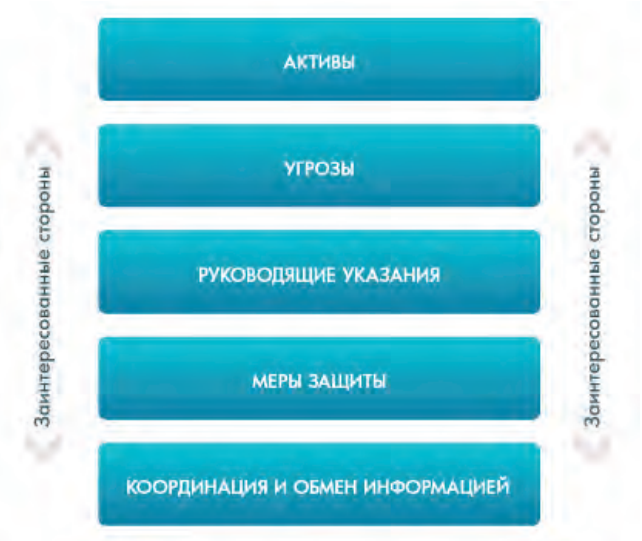


***Рис. 1**. Базовые блоки стандарта ISO 27032:2012*

Основные понятия кибербезопасности

По аналогии с классическим определением информационной безопасности в стандарте под *кибербезопасностью* фактически понимают свойство защищенности активов от угроз конфиденциальности, целостности, доступности, но в некоторых абстрактных рамках – киберпространстве.

Киберпространство формулируется как комплексная виртуальная среда (не имеющая физического воплощения), сформированная в результате действий людей, программ и сервисов в сети Интернет посредством соответствующих сетевых и коммуникационных технологий. Сущностями киберпространства могут быть виртуальные деньги, аватары, облака, виртуальные посольства, виртуальные преступления, виртуальные развлечения и т.д.

Что касается собственно обеспечения кибербезопасности, то в качестве приоритета выделена координация взаимодействия между организациями, формирующими киберпространство, самостоятельные действия которых не обеспечивают эффективную защиту от киберугроз.

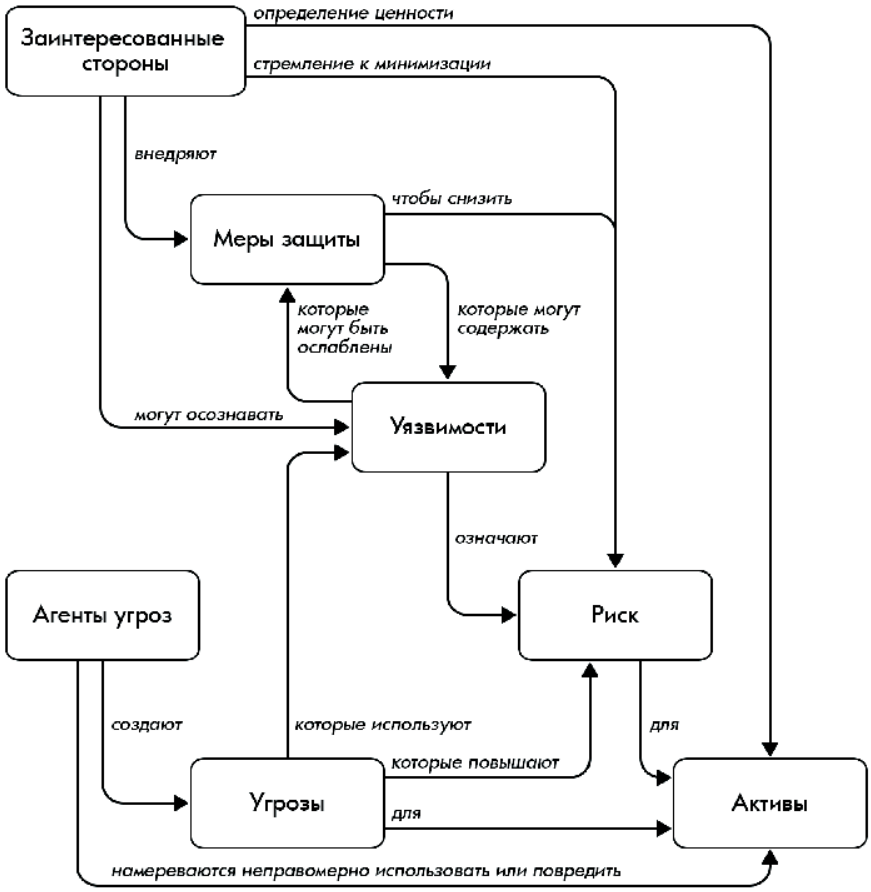
Тезаурус кибербезопасности интегрирован с понятиями информационной безопасности, безопасности приложений, сетевой безопасности, безопасности Интернет, а также безопасности критической информационной инфраструктуры.

Безопасность приложений определяется в отношении программных приложений, а также информационно-программных ресурсов и процессов, участвующих в их жизненном цикле. Безопасность сетей связана с проектированием, внедрением и использованием сетей внутри организации, между организациями, между организациями и пользователями. Безопасность в сети Интернет касается интернет-услуг и соответствующих систем информационно-коммуникационных технологий и сетей. Безопасность критической информационной инфраструктуры характеризует защищенность от соответствующих угроз, в том числе угроз информационной безопасности. Иллюстрация соотношения названных понятий (как ее увидели в международном комитете ISO JTC 1) представлена на рис.2.

По аналогии с понятием «владелец информации» в обеспечении кибербезопасности ключевую роль играют так называемые заинтересованные стороны (stakeholders), определяющие сферу

Источник: ISO 27032:2012

***Рис. 2**. Положение кибербезопасности относительно других сфер безопасности*



Источники: ISO 27032:2012, ISO 15408-1:2009

Рис. 3. *Основные понятия безопасности и характер связей между ними*

защиты своих собственных активов и другие интересы в киберпространстве. В глобальном плане киберпространство не является чьей-либо собственностью: каждый может стать его участником - заинтересованной стороной.

В качестве основных групп заинтересованных сторон выделены следующие:

1. Потребители, которые могут быть физическими лицами либо частными или общественными (государственными) организациями;

2. Провайдеры, основными из которых могут быть провайдеры интернет-доступа и провайдеры интернет-приложений.

Потребитель может стать провайдером путем создания доступных виртуальных продуктов или услуг для других пользователей киберпространства. В стандарте приведены примеры ролей заинтересованных сторон, что удобно при внедрении ролевого метода управления доступом в рамках системы обеспечения кибербезопасности.

Заметим, что стандарт регулирует вопросы безопасности с точки зрения организации, то есть он касается пользователей только в качестве клиентов или сотрудников организации, связанных с последней некоторыми соглашениями.

Как известно, к активам в области безопасности традиционно относят все, что представляет ценность, например, информационные и программные ресурсы. Несмотря на «виртуальный» акцент в определении кибербезопасности, в стандарте активы могут быть как виртуальными так и физическими, например: виртуальный аватар и физическое устройство - usb-идентификатор.

Разделяют две группы активов:

- персональные активы (например, данные личной банковской карты);

- активы организации (например, URL-адрес организации).

Соответственно таксономия киберугроз имеет традиционную схему, которая включает классификации по видам и типам активов, внешним и внутренним признакам, целям, источникам и т.д.

Онтология кибербезопасности представлена на рис.3, который представляет собой адаптацию соответствующей схемы из ISO/IEC 15408-1. Как видно из рисунка, более пристальное внимание в области кибербезопасности уделяется злонамеренным угрозам.

Руководящие указания для заинтересованных сторон

В целях планирования обеспечения кибербезопасности стандарт представляет три руководства:

- рекомендации по оценке и отработке рисков,
- рекомендации по соблюдению требований безопасности пользователями,
- рекомендации по обеспечению кибербезопасности для организаций-провайдеров.

Рекомендации по оценке и обработке рисков опираются на ISO 27005, акцентируя лишь внимание на особенностях кибербезопасности, например, необходимости принятия дополнительной ответственности в отношении заинтересованных лиц в области кибербезопасности в плане отчетности, информированности, учета разных законодательных аспектов, обеспечения согласованности действий потребителей и провайдеров на случай инцидентов и мероприятий по обеспечению безопасности.

Рекомендации для пользователей составляют совокупность норм поведения, определенных провайдером, а именно:

- понимание политики безопасности сайта или приложения,
- понимание рисков безопасности,
- соблюдение политики безопасности персональных данных,
- управление безопасностью личных данных,
- информирование уполномоченных органов о подозрительных явлениях или сообщениях,
- проверка подлинности и понимание политики безопасности торговых площадок (в случае осуществления виртуальной торговой сделки),
- контролирование целостности используемого и разрабатываемого программного обеспечения,
- обеспечение безопасности онлайн-публикаций и блогов,
- соблюдение корпоративной политики информационной безопасности в киберпространстве,
- незамедлительное информирование уполномоченных органов о личных нарушениях безопасности.

Руководящие указания организациям предлагают широкий комплекс мероприятий по управлению информационной безопасностью организацией, а именно:

- внедрение и сертификация системы менеджмента информационной безопасности,
- предоставление безопасных продуктов, прошедших соответствующую оценку,
- тестирование, мониторинг сетей и реагирование,
- техподдержка,
- поддержание уровня собственной осведомленности относительно новейших разработок,
- повышение осведомленности пользователей,
- контроль соблюдения политики безопасности и т.д.

Меры обеспечения кибербезопасности

Конкретные меры обеспечения кибербезопасности могут быть определены по результатам оценки рисков и в рамках планирования действий по повышению безопасности активов. Стандарт представляет ряд базовых мер, направленных на решение задач (табл.1):

- обеспечения безопасности приложений,
- обеспечения безопасности серверов,
- обеспечения безопасности конечных пользователей,
- защиты от атак методами социальной инженерии,
- повышения готовности.

Детального рассмотрения заслуживают мероприятия, касающиеся повышения готовности систем, представленные в отдельном приложении к стандарту:

- мониторинг darknet-сетей,
- «синкхолинг»,
- обратная трассировка.

Напомним, darknet («пустая сеть») – подмножество публичных IP-адресов, которые не используются организацией для реальной работы. Обращение к данному подмножеству адресов, таким образом, возможно лишь в результате ошибок конфигурации или нелигитимных действий, например, в целях первичной разведки путем сканирования. В стандарте описаны три варианта darknet-мониторинга:

- метод по типу «черной дыры» (black hole),
- метод слабого взаимодействия,
- метод сильного взаимодействия.

Синкхолинг (sinkhole-метод, метод «сливной трубы») представляет собой способ перенаправления подозрительного IP-трафика в альтернативное «сливное» устройство (как правило, маршрутизатор) с целью пересылки трафика DDoS-атак, блокировки и анализа бот-сетей и др. Недостатком синкхолинга является то, что атакуемый IP-адрес не может использоваться для связи с легитимными пользователями, пока маршрут не будет удален.

Методы обратной трассировки (traceback) включают методы реконструирования маршрутов атак и обнаружения местоположения узловых центров злоумышленников путем корректировки

Таблица 1

Базовые меры кибербезопасности

Категория безопасности	Мера безопасности
Безопасность приложений	Уведомление пользователей о политике безопасности
	Защита сессий веб-приложений
	Контроль корректности вводимых данных (защита от SQL-инжекций)
	Обеспечение безопасности скриптов (защита от атак межсайтового скриптинга)
	Аудит кода и независимое тестирование программного кода
	Подтверждение подлинности провайдера для потребителей
Безопасность серверов	Безопасное конфигурирование серверов
	Установка системы обновлений безопасности
	Контроль системных журналов
	Защита от вредоносных программ
	Регулярное сканирование контента на наличие вредоносных программ
	Регулярное сканирование уязвимостей сайта и приложений
	Обнаружение попыток взлома
Безопасность конечных пользователей	Использование рекомендованных версий операционных систем
	Использование рекомендованных версий программных приложений
	Использование антивирусных средств
	Настройка веб-браузеров в безопасном режиме
	Блокировка или безопасное выполнение скриптов
	Использование фильтров фишинга
	Использование дополнительных механизмов безопасности веб-браузеров
	Использование персональных межсетевых экранов и систем обнаружения вторжений
	Использование автоматических обновлений доверенных программ
Защита от атак методами социальной инженерии	Разработка и внедрение политик безопасности
	Категорирование и классификация информации
	Обучение и повышение осведомленности пользователей
	Тестирование сотрудников
	Мотивация и стимулирование сотрудников
	Использование технических механизмов контроля
Повышение готовности	Использование ловушек в «пустой» сети
	Перенаправление вредоносного трафика
	Обратная трассировка

маршрутной информации, отслеживания маркированных пакетов, аудита журналов и т.д. Наиболее проблемной является междоменная обратная трассировка по причине необходимости решения вопросов совместимости протоколов и архитектур, технических и организационных вопросов обработки информации конфиденциального характера и др.

Основы обмена информацией и координации

Создание системы обмена информацией и координации обусловлено необходимостью оперативного реагирования на инциденты кибербезопасности, которые зачастую пересекают границы организаций и государств.

В рамках информационного взаимодействия в стандарте выделяются два типа участников:

- организации, предоставляющие информацию;
- организации, получающие информацию.

Участники могут совмещать указанные целевые функции и объединяться в разные цепочки.

Организации, предоставляющие информацию, играют первичную роль и определяют классификацию информации, уровни событий безопасности, формы возможного обмена и т.д. Принимающая сторона в соответствии с принятыми соглашениями проводит мероприятия по защищенной обработке информации.

Реализация системы обмена информацией и координации требует:

***Рис. 4**. Четырехуровневая модель кибербезопасного межорганизационного взаимодействия*

- разработки политики безопасности,
- разработки и внедрения соответствующих методов и процедур,
- определения участвующих групп лиц и организаций,
- разработки и реализации соответствующих технических решений.

Стандарт предлагает варианты интерпретации известных «хороших практик» в области информационной безопасности. Например, политика безопасности должна включать принципы классификации и минимизации информации, ограничения аудитории, протокол координации и др., а процедуры должны содержать методику классификации и категорирования, подписание соглашений о неразглашении, использование заданных стандартов, тестирование и т.д. Работа с персоналом подразумевает информирование, обучение, формирование контактов и т.д.

В качестве основных технических решений отмечаются следующие: принятие стандартов форматов данных, визуализацию данных, использование криптографических механизмов, резервного копирования и других защищенных механизмов информационного обмена, также подчеркивается необходимость тестирования технических средств. Общий порядок организации защищенного информационного взаимодействия предлагается следующий:

1. Идентификация участников информационного обмена, формальная или неформальная;
2 . Определение ролей всех участников информационного обмена;
3. Выбор взаимовыгодных механизмов управления;
4. Классификация и категорирование информации;
5. Разработка политик безопасности;
6. Выбор необходимых методов и процессов для каждой из категорий информации;
7. Определение критериев эффективности, подписание соглашений о неразглашении;
8. Выбор необходимых стандартов и технических решений;
9. Подготовка к работе, установление контактов, обучение участников взаимодействия;
10. Периодическое тестирование;
11. Анализ результатов тестирования с целью оптимизации.

Гармонизация стандарта по кибербезопасности

Положения стандарта ISO 27032 опираются на организационно-технические меры, определенные, главным образом, в стандартах 27000-серии, ссылаются на подходы к оценке безопасности продукции и систем по линии «Общих критериев», а также ссылаются на рекомендации ITU (Международный союз электросвязи)[1].

В нашей стране сложилась представительная нормативная база информационной безопасности, которая может быть полезна при решении задач кибербезопасности. В таблице 2 приведены примеры национальных стандартов, гармонизированных с ISO 27032.

---

1. Рекомендации МСЭ-Т X.1500. Методы обмена информацией о кибербезопасности. МСЭ, 2012. 36 с.; Рекомендации МСЭ-Т X.1205. Обзор кибербезопасности. МСЭ, 2008. 64 с.

Таблица 2.

Национальные стандарты в области информационной безопасности

Обозначение ГОСТ	Наименование
Системы менеджмента информационной безопасности	
ГОСТ Р ИСО/МЭК 27000-2012	ИТ. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология
ГОСТ Р ИСО/МЭК 27001-2006	ИТ. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
ГОСТ Р ИСО/МЭК 27002-2012	ИТ. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности
ГОСТ Р ИСО/МЭК 27003-2012	ИТ. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности
Управление рисками	
ГОСТ Р ИСО/МЭК 27005-2010	ИТ. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности
Оценка безопасности	
ГОСТ Р ИСО/МЭК 15408-2012	ИТ. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий
ГОСТ Р ИСО/МЭК 18045-2013	ИТ. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий
ГОСТ Р ИСО/МЭК ТО 19791-2008	ИТ. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем
Гарантии безопасности	
ГОСТ Р ИСО/МЭК 15026-2002	ИТ. Уровни целостности систем и программных средств
Сетевая безопасность	
ГОСТ Р ИСО/МЭК 27033-1-2011	ИТ. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции
Безопасность приложений	
проект ГОСТ Р (согласно планам ТК 362)	Требования по обеспечению безопасности разработки программного обеспечения
Обеспечение непрерывности бизнеса	
ГОСТ Р ИСО/МЭК 27031-2012	ИТ. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса
ГОСТ Р ИСО/МЭК ТО 18044-2007	ИТ. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности
ГОСТ Р 53647.4-2011	Менеджмент непрерывности бизнеса. Руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности
Проектирование систем безопасности	
ГОСТ Р ИСО/МЭК 21827-2010	ИТ. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса

Заключение

Международный стандарт ISO 27032-2012 дает нам ценные указания и перечень мер по повышению кибербезопасности в Интернет, придерживаясь в целом риск-ориентированного подхода в области информационной безопасности.

Использование рекомендаций стандарта, видимо, поможет организациям-поставщикам интернет-услуг спланировать работы по повышению уровня информационной безопасности ресурсов компьютерных систем, подключенных к сетям общего доступа.

Специфическими особенностями стандарта можно назвать следующие:

- относительная ограниченность области определения стандарта так называемой виртуальной киберсредой,
- решение задач повышения готовности исключительно путем противодействия злонамеренным угрозам,
- обеспечение кибербезопасности возложено на организации-провайдеры,
- обмен информацией и координация действий организаций является приоритетной задачей обеспечения кибербезопасности.

В то же время стандарт дает весьма узкое по-

нимание дефиниции кибербезопасности, существенно отличающееся от понятийного аппарата, например, в области кибервойн и кибероборонны.

Нельзя не отметить, что, на наш взгляд, первая версия стандарта во многом представляет фрагментарную интерпретацию традиционных организационно-технических мер, зачастую мало систематизированных и неполных, что является основной причиной малой распространенности стандарта.

Литература

1. Безкоровайный М.М., Лосев С.А., Татузов А.Л. Кибербезопасность в современном мире: термины и содержание // Информатизация и связь. 2011. № 6. С. 27-33.
2. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) // Вопросы кибербезопасности. 2013. № 1(1). С.2-9.
3. Зубарев И.В., Жидков И.В., Кадушкин И.В. Кибербезопасность автоматизированных систем управления военного назначения // Вопросы кибербезопасности. 2013. № 1(1). С.10-16.
4. Казарин О.В., Тарасов А.А. Современные концепции кибербезопасности ведущих зарубежных государств // Вестник Российского государственного гуманитарного университета. 2013. № 14. С. 58-74.
5. Корченко А.Г., Бурячок В.Л., Гнатюк С.А. Кибернетическая безопасность государства: характерные признаки и проблемные аспекты // Безпека інформації. 2013. Т. 1. № 19. С. 40-44.
6. Старовойтов А.В. Кибербезопасность как актуальная проблема современности // Информатизация и связь. 2011. № 6. С. 4-7.
7. Шеремет И.А. Информационная и кибербезопасность: интервью. Редакция «Эхо Москвы», 2013. URL: http://echo.msk.ru/programs/arsenal/1208183-echo/ (Дата обращения: 23.02.2014).
8. Штитилис Д., Клишаускас В. Особенности правового регулирования кибербезопасности в национальных законах Литвы, России и США: стратегии кибербезопасности // Вопросы российского и международного права, 2013, № 7-8, С. 80-100.
9. Юсупов Р.М., Пальчун Б.П. Безопасность компьютерной инфосферы систем критических приложений // Вооружение. Политика. Конверсия. 1993. №3. С. 23-31.
10. Walls A., Perkins E., Weiss J. Definition: Cybersecurity. Gartner. 2013. ID:G00252816. 4 p.
11. Дорофеев А.В., Шахалов И.Ю. Основы управления информационной безопасностью современной организации // Правовая информатика. 2013. №3. С.4-14.
12. Марков А.С., Цирлов В.Л. Управление рисками - нормативный вакуум информационной безопасности // Открытые системы. СУБД. 2007. № 8. С. 63-67.

References

1. Bezkorovaynyy M.M., Losev S.A., Tatuzov A.L. Kiberbezopasnost v sovremennom mire: terminy i soderzhaniye, Informatizatsiya i svyaz, 2011, No 6, pp. 27-33.
2. Borodakiy Yu.V., Dobrodeyev A.Yu., Butusov I.V. Kiberbezopasnost kak osnovnoy faktor natsionalnoy i mezhdunarodnoy bezopasnosti KhKhI veka (Chast 1), Voprosy kiberbezopasnosti, 2013, No 1(1), pp. 2-9.
3. Zubarev I.V., Zhidkov I.V., Kadushkin I.V. Kiberbezopasnost avtomatizirovannykh sistem upravleniya voyennogo naznacheniya , Voprosy kiberbezopasnosti, 2013, No 1(1), pp. 10-16.
4. Kazarin O.V., Tarasov A.A. Sovremennyye kontseptsii kiberbezopasnosti vedushchikh zarubezhnykh gosudarstv, Vestnik Rossiyskogo gosudarstvennogo gumanitarnogo universiteta, 2013, No 14, pp. 58-74.
5. Korchenko A.G., Buryachok V.L., Gnatyuk S.A. Kiberneticheskaya bezopasnost gosudarstva: kharakternyye priznaki i problemnyye aspekty, Bezpeka informatsii, 2013, Vol. 1, No 19, pp. 40-44.
6. Starovoytov A.V. Kiberbezopasnost kak aktualnaya problema sovremennosti, Informatizatsiya i svyaz. 2011. No 6, pp. 4-7.
7. Sheremet I.A. Informatsionnaya i kiberbezopasnost: intervyu. Redaktsiya "Ekho Moskvy", 2013. URL: http://echo.msk.ru/programs/arsenal/1208183-echo/
8. Stitilis D., Klisauskas V. Osobennosti pravovogo regulirovaniya kiberbezopasnosti v natsionalnykh zakonakh Litvy, Rossii i SShA: strategii kiberbezopasnosti, Voprosy rossiyskogo i mezhdunarodnogo prava (Matters of Russian and International Law), 2013, No 7-8, pp. 80-100.
9. Yusupov R.M., Palchun B.P. Bezopasnost kompyuternoy infosfery sistem kriticheskikh prilozheniy, Vooruzheniye. Politika. Konversiya, 1993, No 3, pp. 23-31.
10. Walls A., Perkins E., Weiss J. Definition: Cybersecurity. Gartner. 2013. ID:G00252816. 4 p.
11. Dorofeyev A.V., Shakhalov I.Yu. Osnovy upravleniya informatsionnoy bezopasnostyu sovremennoy organizatsii, Pravovaya informatika, 2013, No 3, pp.4-14.
12. Markov A.S., Tsirlov V.L. Upravleniye riskami - normativnyy vakuum informatsionnoy bezopasnosti, Otkrytyye sistemy. SUBD (Open Systems Journal), 2007, No 8, pp. 63-67.

МНОГОУРОВНЕВЫЙ ПОДХОД К ОЦЕНКЕ БЕЗОПАСНОСТИ ПРОГРАММНЫХ СРЕДСТВ

Грегори Рибер
Кеннет Малмквист
Алексей Щербаков

Статья посвящена вопросам планирования процесса оценки безопасности программных систем с учетом особенностей присущих информационной среде конкретной организации. Делается анализ процесса оценки безопасности в контексте различных бизнес–факторов, таких как требуемый уровень безопасности, бюджетные ограничения, окупаемость инвестиций и т.д. Дается общая характеристика типов уязвимостей программного обеспечения и описываются основные методы тестирования безопасности программных систем: динамический и статический анализ программного кода. Рассмотрены достоинства и недостатки автоматического и ручного режимов статического анализа. Предлагается пример подхода к планированию процесса оценки безопасности программных систем путем создания набора уровней оценки безопасности, где каждый уровень представляет собой комбинацию нескольких методов анализа программного кода. Статья будет интересна руководителям и специалистам в области безопасности информационных систем осуществляющим разработку, планирование и управление процессом обеспечения безопасности программных средств предприятий и организаций.

***Ключевые слова**: безопаснось программных средств, уязвимость, управление рисками, оценка безопасности, статический анализ, динамический анализ*

MAPPING THE APPLICATION SECURITY TERRAIN

Gregory Reber
Kenneth Malmquist
Alexey Shcherbakov

Enterprise application security requirements, vulnerability types, discovery methodologies, and various application assessment strategies are considered. A multilevel approach to application security assessments is described.

***Keywords**: application security, vulnerability, risk management, security assessment, static analysis, dynamic analysis*

Introduction

Network perimeter security has become more and more effective as products and services have matured. Internet applications are now the target of choice for criminals to obtain restricted information and unwarranted access to companies' protected assets. The number and type of protection measures for these applications is growing. The selection of an appropriate application security risk management solution should take into account the business's diverse requirements and factors. There is no single solution that will fit every company's needs.

Those responsible for the security of their environments need to understand what risks are present in their applications, as each vulnerability has an associated criticality that is based on various factors. Armed with this knowledge, an appropriate risk management strategy can be developed with prioritized action to reduce these threats.

Modern economies are characterized by increasing variety of enterprises of different size, structure, and specialization. Every organization is different to certain extent: it has different business needs, different information systems, and different security requirements. It is quite logical to propose a set of service levels in the realm of application security assessments from which the management could choose the most cost-effective type or level of service that would match the organization's business needs and security requirements.

So what is the required level of application security assessment?

As enterprise application security requirements are considered, it is useful to put them in the same context as various other software attributes that we usually deal with:

- Functionality
- Usability
- Performance
- Reliability
- Security

However, we can't deal with the characteristics of our applications in isolation; we consider them in the context of business requirements and real world business factors including feasibility, funding, return on investment, and opportunity cost.

While better is always desirable, we can't evaluate what is better without understanding the status quo. We need to answer the "better than what?" question. This requires sufficient analysis/assessment to identify a comparative baseline.

For example: A company's web-facing newsletter sign-up page is found to have a Cross-Site Scripting vulnerability. Addressing this risk may require $20,000 in development costs. Is this the best use of funds for this company?

In theoretical terms we want absolute safety. In practical terms we want a "reasonable or better" level of security. The definition of "reasonable" is only meaningful within the context of a specific application and business. The definition may be based upon government (e.g. DoD levels of classification [1]), industry group requirements (PCI DSS [2]), and business domain.

The very act of measuring security, performance, or reliability has an associated variable cost based upon the precision and thoroughness of the analysis, the skills of the analysts, etc.

An application security assessment process is the method of identifying application security vulnerabilities so that the business can make informed risk management decisions that include the evaluation of the financial and opportunity costs associated with mitigating the identified security risks. The thoroughness, depth, and cost of an application security assessment process should reasonably vary with business requirements.

Now that we familiarized ourselves with a high level overview of the application security space let's discuss the different types of security vulnerabilities and discovery methodologies.

What types of security risks should be considered?

A useful starting reference point is the vulnerability taxonomy maintained by OWASP, the Open Web Application Security Project. There, one can find hundreds of articles defining common application security flaws. OWASP also maintains a Top 10 list [3] of the most critical web application vulnerabilities. While the OWASP Top 10 list is a very useful document to increase security awareness, like most lists of this sort, it is neither intended to be comprehensive nor a sufficient definition of application security. AsTech maintains a more wide-ranging catalog of vulnerability classes which we have developed over the past 15 plus years.

There are a number of approaches to assessing application security involving varying combinations of automated and manual analysis from an external (black box) and internal (white box) perspective.

External Web Application Scanning

Dynamic application scanning involves interacting with a running application (essentially using and attacking the application) as a black box to identify points of vulnerability. While the best of breed commercial automated scanning tools can produce some valuable results, they still can't approach the quality and breadth of results that can be identified by a highly skilled ethical hacker.

The strength of application scanning is that because the application is actually attacked, the resulting proof of vulnerability is usually quite concrete and compelling. For example, the results of a successful SQL injection attack might include data or metadata accessed without authorization. If you can see another user's account data or display the structure of the database, it is hard to argue with the existence of the vulnerability.

The weakness of application scanning is that it identifies only a limited range of vulnerabilities and often requires a highly skilled practitioner. Since the application user interface is the attack vector, the approach is ill-suited to examining business component, back-end,

or external service vulnerabilities. For example, if sensitive data such as social security numbers are not being encrypted, or third-party services operate without proper protection, or critical security events such as failed logins are not being adequately logged, these vulnerabilities are likely to go undetected.

Automated Static Analysis

Static analysis involves the review of the application code for vulnerabilities. For most tools, this usually refers to the source code but less frequently refers to the binary code. This would be considered a 'white box' assessment, as nothing is hidden from the analyst. The application code is a much larger and richer analysis target than the user interface addressed by external, or 'black box' application scanning, and therefore a broader range of vulnerabilities can be identified.

The best of breed static analysis tools utilize sophisticated compiler technologies such as data flow analysis, control flow analysis, and pattern recognition to identify security vulnerabilities. The results of automated analysis generally include a high degree of false positives, requiring a highly skilled security engineer to analyze the results with the source code in hand to distinguish between the truly and the falsely reported vulnerabilities.

Each type of application security analysis tool has its strengths and weaknesses. Thorough understanding of these strengths and weaknesses is crucial for implementing a successful application security program using the right tools.

What are the strengths and weaknesses of Static Analysis?

Static analyzers are best at identifying vulnerabilities that can be represented as identifiable patterns. Examples of these risks include:

- A missing entry in an XML configuration file
- The use of a dangerous function, including non-validated user input data in a web page
- Output (Cross-Site Scripting vulnerability)
- Including non-validated input data in the construction of a database query (SQL Injection vulnerability)

Automated Static Analysis

Most static analysis tools can also identify a range of poor programming practices such as the use of uninitialized variables or the lack of error handling.

The main stren gth of automated static analysis is that the analyzers reliably identify candidate issues (which could turn out to be false positives) and can do so in the face of highly complex application structure and control flow that might daunt most humans. For the software expense and the skilled labor required, the results can be quite cost effective.

However, the main limitation of these automated tools is that currently they can only find approximately 50%-80% of the types of security vulnerabilities that should be evaluated in a security assessment to provide a comprehensive view of risks present in an application. With the current state of the technology, automated analyzers are generally not capable of testing algorithms, security policy adherence, and issues that may be derived from the application domain. Examples of these areas include:

- Authentication
- Authorization
- Disclosure of confidential data
- Audit logging
- Cross-Site Request Forgery (CSRF)
- Identifying application 'back-doors'

Manual Static Analysis

Manual static analysis involves a review of the application architecture and source code by highly skilled software security engineers. The resulting analysis is comprehensive and is, overall, the most reliable of the approaches. Thus it has been the method of choice where application security is of paramount concern, such as most financial services organizations.

The strength of manual analysis is the level of depth and thoroughness of the assessment. The full range of security vulnerabilities can most readily be identified with high reliability. Specific attributes of the application domain (credit card numbers, account numbers, classified data, etc.) can be taken into account.

The main drawback of manual analysis is that engineers with the necessary skills and experience – both extensive enterprise application development experience coupled with deep security knowledge – are scarce and in high demand. The time required and the level of effort involved makes this approach more costly than other options.

Vendor Claims

Predictably, vendors of specific technologies or services tend to tout the strengths of their specific approaches and diminish the value of the alternatives. The vendors of automated static analysis tools promote their cost effectiveness and minimize the importance of potentially material coverage gaps, which as we have shown may be significant. Providers of purely manual assessment services tout comprehensive coverage and minimize the impact of cost and schedule.

Of course, there is no 'one size fits all' approach to application security. A sound risk management strategy will make the most appropriate use of any available technology or process.

A multilevel approach

There are many different types of applications in use today, encompassing myriad functionalities and business purposes. Therefore, there can be no 'one size fits all' approach to risk management when contemplating application security. An internally utilized client-server application that tracks office equipment purchases will not have the same security requirements as those of a publicly accessible banking application.

Previously, we described the relative effectiveness of various assessment methodologies at discovering risks.

Now, let's think about the ways to use that knowledge to efficiently identify and plan security assessments for various types of applications taking into account the depth of analysis coverage, the costs, and the residual risk. Among several possible ways to approach this task we chose as an example a method that we will call a multilevel approach to application security assessments. The main idea behind the method is creating a set of levels of security assessment based on the range of "white box" risk discovery options. Each level can be described as a combination of an automated static analysis of the source code and a manual code review. For an added level of verification any of these levels can be further enhanced by adding an external or "black box" vulnerability assessment in the form of a manual or automated dynamic analysis.

1. Comprehensive Assessment – Automated analysis with complete manual analysis

To obtain the most comprehensive results and ensure the lowest residual risk, this level employs automated source code static analysis tools to identify a preliminary set of vulnerabilities and a full manual analysis of the source code for types of vulnerabilities not reliably found through automated tools. This level is most appropriate for commercial applications that have the highest security requirements such as applications involving a high volume or high value financial transactions.

2. Perimeter Assessment – Automated analysis with attack surface manual analysis

To provide breadth of analysis while lowering cost, this level employs automated source code static analysis tools to identify a preliminary set of vulnerabilities. The preceding phase is followed by a manual analysis focused on those areas of the source code that represent the greatest risk for types of vulnerabilities not reliably found through automated tools. Representative areas of focus include the code representing the attack perimeter of the application such as user interfaces and use of external services as well as authentication, authorization, and data protection. Since the manual review is somewhat limited, there is some amount of residual risk with this approach.

3. Perimeter Audit – Automated analysis with attack surface manual audit

To further reduce cost but still provide some breadth of analysis, this level employs automated source code static analysis tools to identify a preliminary set of vulnerabilities and a manual audit of the source code focused on those areas of the source that represent the risk for types of vulnerabilities not reliably found through automated tools. The auditing process samples a portion of the code which is taken to contain representative examples within the range of vulnerabilities present in the application. Since the manual review is even more limited, there is a greater level of residual risk.

4. Automated Assessment – Automated static source analysis audit

To minimize expense while obtaining some reliable level of security assessment, automated static analysis of the application is performed and validated. This provides a reasonable assessment for some of the most frequent critical vulnerabilities such as SQL Injection and Cross-Site Scripting. However it leaves other key areas not addressed by automated analysis unassessed. The level of residual risk is therefore higher still compared to other approaches and thus may not be appropriate for an application that is business critical.

	Level of Risk Identification	Relative Cost	Resulting Residual Risk
Comprehensive Assessment	Highest	Higher	Lowest
Perimeter Assessment	Higher	Moderate	Low
Perimeter Audit	High	Low	Moderate
Automated Assessment	Moderate	Lower	Significant

Conclusions

Every day, more threats and exploits against Internet applications are being discovered. Many applications contain vulnerabilities that haven't been discovered by those responsible for securing these systems, rendering it impossible to implement effective risk management strategies. There are more than a few options available to identify these vulnerabilities, but the decision of which to use in a given business environment can be complicated, since every option has its pros and cons. The multilevel approach presented above can help any organization to identify the right scope of application security assessment within the available budget and ensure the application security needs are met.

AsTech Consulting has been performing application security assessments for top-tier clients since 2001. Our assessment processes combine the skills of some of the industry's best security engineers with the best of class automated analysis tools. We continually modify our processes to take into account the improvements in automated tools, the changes in threats, and industry standards and best practices. Our goal is to deliver the most effective application security process possible, based on each client's unique risk appetite and business objectives.

References

1. DoD Information Security Program: Overview, Classification, and Declassification, DoD Manual 5200.01, Volume 1, p.34. US Department of Defense. 2012.
2. Payment Card Industry (PCI) Data Security Standard, v3.0. PCI Security Standards Council. 2013.
3. OWASP Top 10 – 2013. The Open Web Application Security Project. 2013.

О ПРИЗНАКАХ ПОТЕНЦИАЛЬНО ОПАСНЫХ СОБЫТИЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

***Жидков Игорь Васильевич**, кандидат технических наук, доцент*
Кадушкин Иван Викторович

Статья посвящена вопросам, касающимся проблем безопасности программного обеспечения и созданных на его основе информационных систем. Рассмотрены проблемные вопросы выявления выявлению недекларированных возможностей. Предложена иерархическая классификации нарушений целостности, доступности и целостности. Предложен подход по выявлению потенциально–опасных событий, основанный на сочетании структурного анализа и функционального тестирования.

***Ключевые слова**: сертификация, потенциально опасные события, недекларированные возможности, безопасность программ.*

ABOUT THE SIGNS OF POTENTIALLY DANGEROUS EVENTS IN INFORMATION SYSTEMS

***Igor Zhidkov**, Ph.D., Associate Professor*
Ivan Kadushkin

The issues related to information security systems are discussed. The problem of identify of software security defects is considered. The hierarchical classification of violations of integrity, availability, and integ–rity is proposed. An approach to identify potentially dangerous events based on a combination of structural analysis and functional testing is offered.

***Keywords**: certification, information security defects, undeclared features, software security.*

В настоящее время проблема безопасности программного обеспечения (ПО) и созданных на его основе информационных систем (ИС) стоит как никогда актуально [4,5].

По требованиям безопасности ПО и ИС проверяются с целью контроля функционального соответствия, защиты от несанкционированного доступа, выявления недекларированных возможностей (НДВ), реализующих события, опасные с точки зрения безопасности информации. Проверки могут осуществляться как независимыми представителями заказчика или самого разработчика в процессе разработки и производства ПО, так и экспертами испытательных лабораторий или каких-либо аттестационных комиссий на испытаниях ПО и ИС.

Порядок и требования к проведению сертификационных испытаний описаны в Руководящих документах Гостехкомиссии России (ныне ФСТЭК России) [8].

Рассмотрим более подробно проблему выявления НДВ.

Бытует мнение, что при наличии необходимой документации на ПО (исходных текстов, описания программ, описания применения и др.) на сертификационных или иного рода испытаниях и проверках достигается гарантированное выявление всех НДВ. Однако, это мнение принципиально ошибочное. Дело в том, что изначально вообще неизвестно, внесены НДВ в ПО или нет. В разных испытательных лабораториях при проведении проверок используются принципиально различные технологии, которые по большому счету нельзя признать совершенными из-за научной незавершенности проблемы выявления вредоносных функций ПО. Эти технологии реализуются специалистами неодинакового уровня квалификации, сроки проверки ПО могут оказаться весьма жестко ограниченными, что сказывается на качестве проводимых работ и т.д. Наконец, исходная достоверная документация вообще может не представляться [2,3]. Ситуация в полной мере напоминает «поиск черной кошки в темной комнате». В итоге всегда существует остаточный риск того, что после проверки в ПО сохранятся невыявленные ошибки и функциональные возможности, осуществляющие опасные воздействия на обрабатываемую информацию [9].

В реальности требуемая документация на ПО (в первую очередь, исходные тексты, подробные описания программ и их применения) может отсутствовать в объеме, достаточном для детальной проверки. В этом случае приходится анализировать функциональность и безопасность ПО путем выявления и анализа ПОС в ходе имитации процессов его функционирования.

Таким образом, своевременное выявление и устранение опасных событий на этапе тестирования ПО способно предотвратить или существенно снизить ущерб, возникающий в результате наличия в ПО вредоносного кода.

Одним из основных признаков обеспечения безопасности информации в ИС является сохранение ее целостности, конфиденциальности и доступности.

В ГОСТ РВ 51987-2002 «Информационная технология. Комплекс стандартов на автоматизированные системы. Типовые требования и показатели качества функционирования информационных систем. Общие положения» введены следующие определения [1, 6]:

- целостность информации – состояние информации, при котором обеспечивается достижение целей ее функционального применения;

- конфиденциальность информации – свойство используемой информации быть сохраненной в течение заданного объективного периода конфиденциальности от ознакомления лицами, к ней не допущенными, и/или от несанкционированного считывания техническими средствами;

- доступность информации – это состояние информации, ее носителей и технологий обработки, при котором обеспечивается санкционированный доступ к ней и надежность представления требуемой информации.

Рассмотрим классификационные признаки потенциально-опасных событий (ПОС) при функционировании ПО.

Признаки потенциально опасных событий, связанных с нарушением целостности информации

В соответствии с требованиями руководящими документами Гостехкомиссии России в ИС должна быть обеспечена целостность программных средств, обрабатываемой информации, а также неизменность программной среды.

Основываясь на данном требовании к ИС можно сформулировать типовые способы программного нарушения целостности информации:

1) нарушение целостности информационного ресурса ИС:

- нарушение целостности файлов;

- нарушение целостности записей (полей записей);

- нарушение целостности каталогов и папок.

2) нарушение целостности программного ресурса ИС:

- нарушение целостности программ;

- нарушение размещения программ на внешних носителях информации.

3) нарушение целостности программной среды:

- нарушение целостности активных процессов;

- активизация несанкционированных процессов;

- несанкционированное удаление активных процессов.

Вышеприведенные способы программного нарушения целостности информации базируются на следующем множестве событий, являющихся высшим уровнем детализации классификационных признаков нарушения целостности информации:

- несанкционированная модификация информации;

- несанкционированное уничтожение информации;

- несанкционированное перемещение информации.

Анализ сформированного множества событий нарушения целостности информации позволяет определить характерные последствия при их реализации в ИС:

- отсутствие возможности активизации программного ресурса ИС;

- отсутствие возможности использования информационного ресурса ИС;

- изменение декларируемого алгоритма программ;

- неверное выполнение расчетных задач по причине модификации информационного ресурса;

- изменение штатного алгоритма активного процесса;

- изменение состава необходимых активных процессов;

программные сбои ИС и возникновение исключительных ситуаций в процессах.

Причинно-следственная связь между способами программного нарушения целостности и последствиями реализации ПОС, направленных на нарушение целостности информации иллюстративно представлена на рисунке 1.

Одним из основных требований к проводимым испытаниям ПО является выявление НДВ, реализующих несанкционированные функции нарушения целостности информационного и программного ресурса (ИПР) в ИС.

Выполненный анализ и опыт проведения испытаний ПО позволяет построить иерархическую структуру классификационных признаков нарушения целостности информации, представленную на рисунке 2.

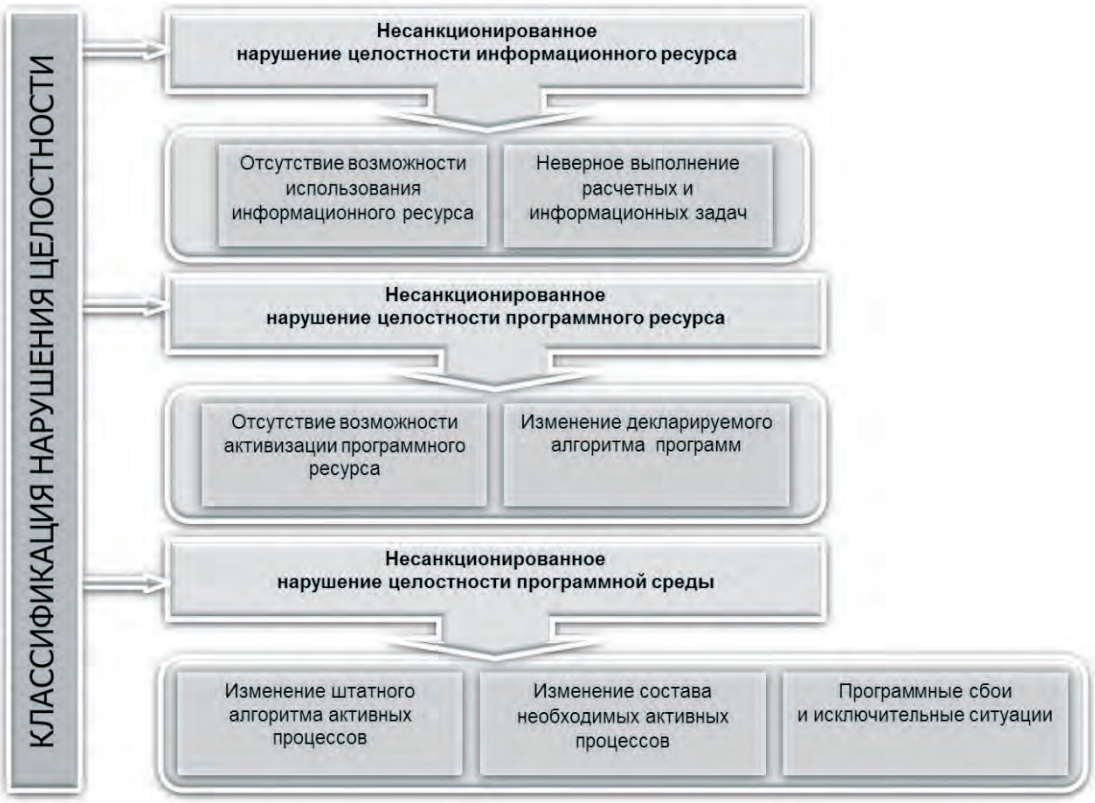


Рис. 1. *Связь между способами и последствиями реализации опасных событий, направленных на нарушение целостности информации*

Рис. 2. *Иерархич еская структура классификационных признаков нарушения целостности ИПР*

Признаки потенциально опасных событий, связанных с нарушением конфиденциальности информации

Нарушение конфиденциальности информации напрямую связано с реализацией угрозы несанкционированного доступа к ИС и является следствием нарушения системы защиты информации.

Угрозы нарушения конфиденциальности, как правило, выступают в форме несанкционированного обращения.

Термин «несанкционированное обращение» означает активные действия, направленные на сбор или хищение ценной информации, закрытой для доступа посторонних лиц.

Опыт эксплуатации показывает, что около 80% попыток НСД к конкретной ИС осуществляют лица, работающие или работавшие с данной системой [7]. Поэтому будем считать, что потенциальный нарушитель имеет достаточно высокую квалификацию и ему известны принципы функционирования ИС.

К типовым способам нарушения конфиденциальности можно отнести:

- уничтожение или вывод из строя ПО с целью вывода из строя СЗИ или системы передачи данных;
- изменение программно-информационного обеспечения с целью нарушения штатных режимов функционирования ИС;
- захват прав доступа авторизованных пользователей;
- использование уязвимостей в ПО и операционных системах или ошибок, допущенных при администрировании;
- использование доверия между хостами (хост – хост) и сетями (сеть – сеть);
- использование средств, реализующих недекларированные возможности – "троянцы", лазейки (дыры), вирусы и т.д.;
- использование ошибок и особенностей сетевых протоколов или инфраструктуры сети;
- перехват информации в ходе сетевых взаимодействий;
- перехват информации из оперативной памяти.

Все приведенные способы нарушения конфиденциальности приводят хотя бы к одному из следующих событий, составляющих первый уровень иерархии классификационных признаков нарушения конфиденциальности:

- несанкционированное копирование защищаемых ИПР (естественный способ нарушения конфиденциальности; копирование может осуществляться на жесткий диск, на отчуждаемый носитель информации, на удаленный объект сети и в оперативную память);
- несанкционированное ознакомление с защищаемыми ИПР (под ознакомлением понимается вывод информации на средства отображения: дисплей, печатающее устройство);
- несанкционированная модификация программных средств защиты ИПР (изменения могут вноситься в файлы, отвечающие за обеспечение работы системы разграничения доступа, в атрибуты защищаемых информационных объектов и в другие данные, определяющие работоспособность системы защиты информации; цель этих манипуляций состоит в нарушении правил разграничения доступа);
- несанкционированное перемещение защищаемых ИПР (перемещение может осуществляться на жесткий диск, на отчуждаемый носитель информации, на удаленный объект сети и в оперативную память; кроме того, перемещение или удаление некоторых объектов, отвечающих за работоспособность системы защиты информации может привести к нарушению принятых правил разграничения доступа).

Анализ способов нарушения конфиденциальности показал, что при правильной настройке системы защиты администратор безопасности может получить множество данных (признаков), указывающих на то, что в защищаемой системе была произведена попытка доступа к конфиденциальной информации. Таким образом, чем большими возможностями обладает система защиты, тем больше возможных признаков нарушения конфиденциальности она может обнаружить. Основой для поиска признаков нарушения конфиденциальности является информация, хранящаяся в системных журналах, журналах администрирования и прочих подобных банках данных.

Множество признаков нарушения конфиденциальности напрямую зависит от множества способов эту конфиденциальность нарушить. В то же время, если реализованная система безопасности не сможет обнаружить известных ей признаков, неизвестная системе атака станет осуществимой, и конфиденциальность будет нарушена.

В ходе анализа способов получения несанкционированного доступа к конфиденциальной информации были выявлены следующие характерные последствия реализации опасных событий, направленных на нарушение конфиденциальности в ИС:

1) Нарушение целостности информационно-программных ресурсов.

Нарушение целостности защищаемых данных – первый признак нарушения конфиденциальности, ведь изменение данных возможно только после получения к ним доступа. Нарушение целост-

ности системы защиты информации сигнализирует о возможном изменении характеристик функционирования системы защиты и, как следствие, о возможном нарушении конфиденциальности.

2) Нарушение доступности информационно-программных ресурсов.

Нарушение доступности, как и нарушение целостности, является прямым указанием на попытки осуществления несанкционированного доступа к защищаемым ресурсам, за исключением тех случаев, когда доступность нарушена вследствие случайных событий, связанных со сбоями в ПО или аппаратуре.

3) Заражение программными вирусами.

Многие программные вирусы, особенно распространенные сейчас так называемые «троянские кони» написаны именно с целью ознакомления с конфиденциальными данными.

4) Несанкционированное обращение к устройствам вывода информации.

Это событие связано с отображением информации на устройства вывода – монитор либо печатающее устройство. Данное событие может быть и не замечено обычным пользователем, особенно при наличии сетевого принтера. В этом случае обнаружение нарушения конфиденциальности производится на основе анализа системных журналов.

5) Манипуляции или неправильное использование файлов с информацией.

Сюда относятся и попытки прямого копирования информации, и вывод ее на внешние носители, и печать, и простое ознакомление путем открытия файлов на чтение. Также возможно копирование файлов, содержащих конфиденциальную информацию, в незащищенные области диска. Информация об этих манипуляциях обычно хранится в журналах аудита.

6) Разработка компьютерных программ для неслужебного использования.

Появление неизвестного исполняемого файла может привести к выполнению запрещенных в ИС действий.

7) Сообщения об ошибках в ходе аутентификации.

Если в течение короткого промежутка времени произошло несколько ошибок при аутентификации, это может свидетельствовать о попытках несанкционированного доступа. Кроме того, авторизованный пользователь может обнаружить

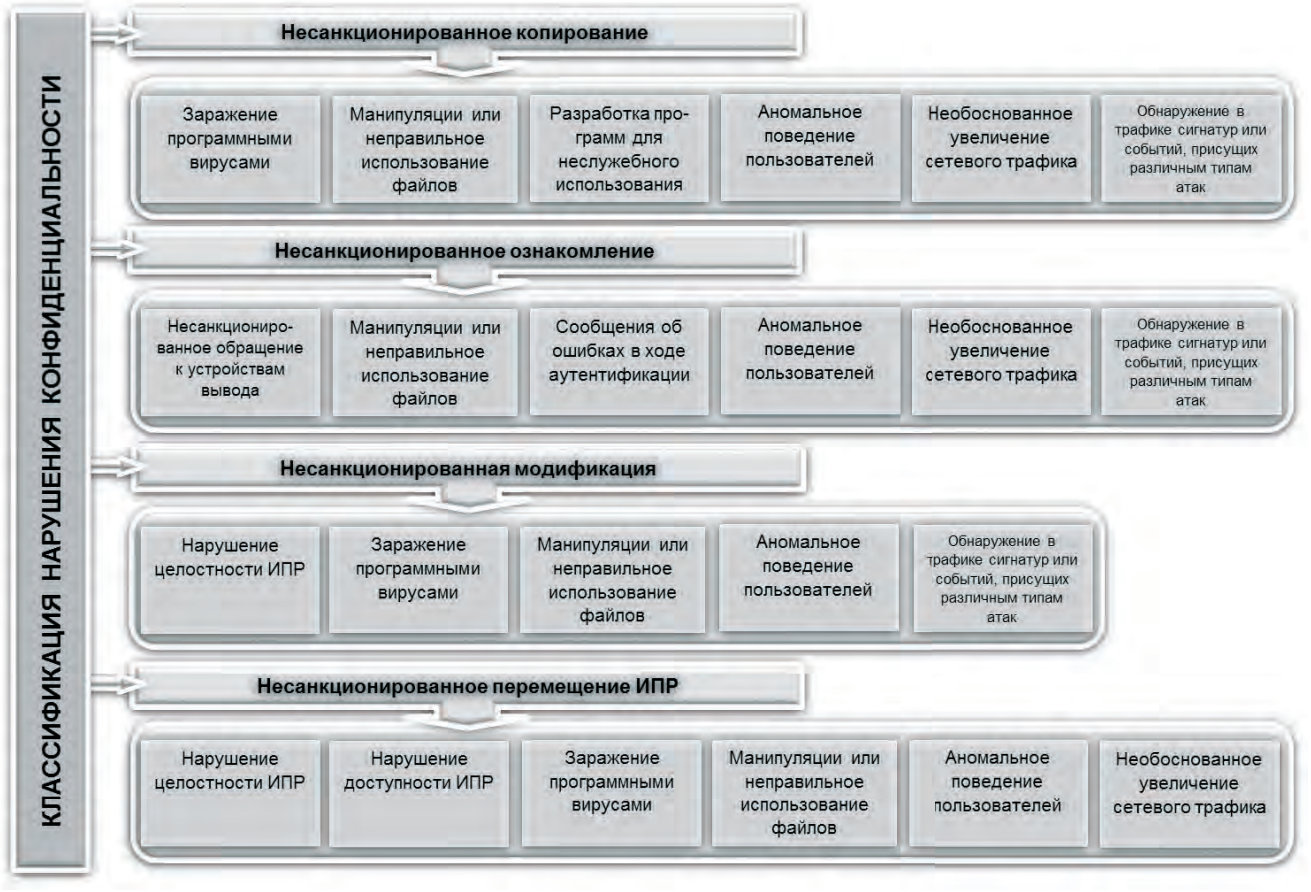


Рис. 3. *Связь между способами и последствиями реализации опасных событий, направленных на нарушение конфиденциальности ИПР*

несанкционированное вхождение в систему от его имени, проанализировав время последнего входа в систему.

8) Аномальное поведение пользователей.

Основной принцип обнаружения аномалий состоит в том, что атаки отличаются от нормального поведения. Скажем, определенную повседневную активность пользователей можно смоделировать достаточно точно. Допустим, конкретный пользователь обычно регистрируется в системе около десяти часов утра, читает электронную почту, выполняет транзакции баз данных, уходит на обед около часа дня, допускает незначительное количество ошибок при доступе к файлам и так далее. Если система отмечает, что тот же самый пользователь зарегистрировался в системе в три часа ночи, начал использовать средства компиляции и отладки и делает большое количество ошибок при доступе к файлам, она должна пометить эту деятельность как подозрительную.

9) Необоснованное увеличение сетевого трафика.

Увеличение исходящего сетевого трафика может свидетельствовать об утечке информации на удаленный объект сети. Увеличение входящего сетевого трафика может свидетельствовать о несанкционированной записи на диск объектов сомнительного содержания, которые могут представлять опасность для функционирования системы защиты информации.

10) Обнаружение во входящем сетевом трафике сигнатур или событий, присущих различным типам атак.

На этом принципе работают программы, реализующие защиту посредством межсетевых экранов.

Связь между способами и последствиями реализации опасных событий, направленных на нарушение конфиденциальности, представлена на рисунке 3.

В ходе испытаний и тестирования ПО по требованиям безопасности информации необходимо дать подтверждение отсутствия в ПО НДВ, реализующих возможности по нарушению конфиденциальности информации. В результате анализа способов, реализующих механизмы нарушения конфиденциальности, предложена иерархическая структура классификационных признаков нарушения конфиденциальности ИПР, изображенная на рисунке 4.

Рис. 4. *Иерархическая структура классификационных признаков нарушения конфиденциальности*

Признаки потенциально опасных событий, связанных с нарушением доступности информации

Для обеспечения гарантированной доступности и сохранности информации как правило применяют многоуровневое резервирование и дублирование каналов передачи данных и внешних носителей информации.

Реакция ответственных служб на нарушения доступности ИПР преследует две главные цели: локализация нарушения и уменьшение наносимого ущерба, и недопущение повторных нарушений.

Планирование восстановительных работ, являясь частным случаем проработки реакции на нарушение доступности, позволяет подготовиться к потенциально опасным событиям, уменьшить ущерб от них и сохранить способность к функционированию критически важных сервисов.

Процесс планирования восстановительных работ можно подразделить на следующие этапы:

- выявление критически важных сервисов, их ранжирование по степени критичности;
- идентификация ресурсов, необходимых для функционирования критически важных сервисов;
- определение перечня потенциально опасных событий;
- разработка плана восстановительных работ;
- подготовка к реализации разработанного плана;
- проверка плана.

И при подготовке мер реагирования на нарушение доступности, и при планировании восстановительных работ необходимо проводить измерения, показывающие, за какое время то или иное действие может быть выполнено на практике. Располагая временной метрикой элементарных действий, можно оценивать продолжительность более сложных мероприятий. Если не удается уложиться в отведенное время, нужно или повысить подготовку персонала, или пересмотреть накладываемые ограничения, или разработать альтернативные, возможно, более дорогостоящие процедуры.

Признаками нарушения доступности информации могут выступать следующие события:

- отсутствие доступа на чтение ресурса;
- отсутствие доступа на запись ресурса;
- отсутствие доступа на исполнение ресурса;
- отсутствие доступа на удаление ресурса;
- отсутствие доступа на перемещение ресурса;
- блокирование определенных функций ПО;
- блокирование вывода информации.

В ходе испытаний на функциональную безопасность ПО необходимо дать подтверждение отсутствия в ПО недекларированных возможностей, реализующих нарушение доступности информации.

В результате анализа признаков нарушения доступности информации можно сформулировать множество ПОС, приводящих к нарушению доступности ИПР. Иллюстративно признаки ПОС, приводящих к нарушению доступности информации представлены на рисунке 5.

Рис. 5. *Признаки ПОС, приводящих к нарушению доступности*

В соответствии с предложенной схемой возникновение каждого из признаков нарушения доступности ИПР является следствием возникновения ПОС, реализацией которых являются системные вызовы операционной системы.

Как видно из предложенных структур, нижним уровнем классификационных признаков ПОС, влияющих на целостность, конфиденциальность и доступность ИПР, являются системные вызовы используемой операционной системы.

В испытательной лаборатории информационных систем и программного обеспечения 3 ЦНИИ МО РФ проведен анализ системных вызовов линек ОС Windows и ОС МСВС. Сформирован перечень потенциально опасных системных вызовов, который используется при проведении сертификационных испытаний по требованиям безопасности информации.

Для выявления описанных ПОС на этапе тестирования и испытаний ПО предлагается совместное использование проверок, как по поиску НДВ, так и на соответствие требованиям по защите от НСД, представленное на рисунке 6.

Заключение

Сложность современных ИС измеряется не столько количеством комплектующих элементов и механических соединений, сколько бесконечным множеством возможных сценариев функционирования подобных систем, семантическим многообразием исходной формализованной информации, подлежащей оперативной обработке в режиме реального времени, и множеством функций программного обеспечения, реализующего эту обработку и подлежащего соответствующим проверкам на испытаниях.

Предлагаемый подход направлен на повышение эффективности выявления ПОС при проведении испытаний ИС на соответствие требованиям безопасности информации.

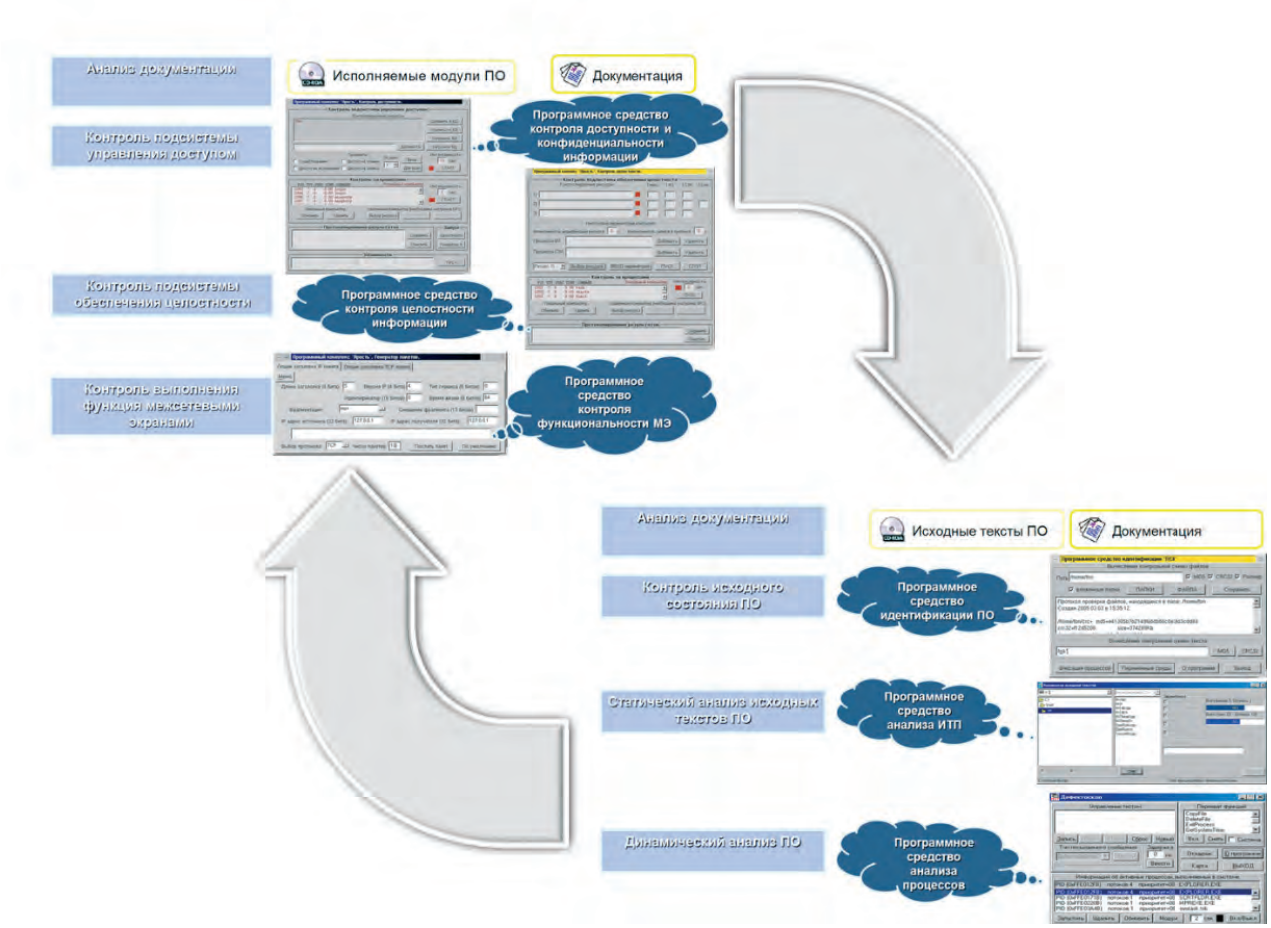


Рис. 6. *Порядок выявления потенциально-опасных событий на этапе тестирования и испытаний ПО*

Литература

1. Бойко А.А., Гриценко С.А., Храмов В.Ю. Система показателей качества баз данных автоматизированных систем. // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2010. № 01. С. 39-45.
2. Жидков И.В., Львов В.М., Федорец О.Н. Применение программно-инструментальных средств автоматизированного тестирования в процессе сертификационных испытаний // Информационное противодействие угрозам терроризма. 2008. № 10. С. 170-176.
3. Жидков И.В., Федорец О.Н. Проблема создания безопасного программного обеспечения и предложения по ее решению // Доклады Томского государственного университета систем управления и радиоэлектроники. 2008. Т. 2. № 1. С. 32-33.
4. Зубарев И.В., Жидков И.В., Кадушкин И.В. Кибербезопасность автоматизированных систем управления военного назначения // Вопросы кибербезопасности. 2013. № 1 (1). С.10-16.
5. Зубарев И.В. Сертификация как направление повышения безопасности информационных систем и программного обеспечения // Известия Южного федерального университета. Технические науки. 2003. Т. 33. № 4. С. 48-53.
6. Костогрызов А.И., Зубарев И.Ю., Родионов В.Н. и др. Методическое руководство по оценке качества функционирования информационных систем (в контексте стандарта ГОСТ РВ 51987). М.: Изд-во 3 ЦНИИ, 2004, 352 с.
7. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность / Справочник. – М.: Новый юрист, 1998. С. 48-57.
8. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. М.: Радио и связь, 2012. 192 с.
9. Diomidis Spinellis. Code Quality: The Open Source Perspective. - Addison Wesley, 2006. 569 p.

References

1. Boyko A.A., Gritsenko S.A., Khramov V.Yu. Sistema pokazateley kachestva baz dannykh avtomatizirovannykh sistem, Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriya: Sistemnyy analiz i informatsionnyye tekhnologii, 2010, No 01, pp. 39-45.
2. Zhidkov I.V., Lvov V.M., Fedorets O.N. Primeneniye programmno-instrumentalnykh sredstv avtomatizirovannogo testirovaniya v protsesse sertifikatsionnykh ispytaniy, Informatsionnoye protivodeystviye ugrozam terrorizma, 2008, No 10, pp. 170-176.
3. Zhidkov I.V., Fedorets O.N. Problema sozdaniya bezopasnogo programmnogo obespecheniya i predlozheniya po yeye resheniyu, Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki, 2008, Vol. 2, No 1, pp. 32-33.
4. Zubarev I.V., Zhidkov I.V., Kadushkin I.V. Kiberbezopasnost avtomatizirovannykh sistem upravleniya voyennogo naznacheniya, Voprosy kiberbezopasnosti (Cybersecurity Issues), 2013, No 1(1), pp.10-16.
5. Zubarev I.V. Sertifikatsiya kak napravleniye povysheniya bezopasnosti informatsionnykh sistem i programmnogo obespecheniya, Izvestiya Yuzhnogo federalnogo universiteta. Tekhnicheskiye nauki, 2003, Vol. 33. No 4, pp. 48-53.
6. Kostogryzov A.I., Zubarev I.Yu., Rodionov V.N. and etc. Metodicheskoye rukovodstvo po otsenke kachestva funktsionirovaniya informatsionnykh sistem (v kontekste standarta GOST 51987), Moscow, 2004, 352 p.
7. Kurushin V.D., Minayev V.A. Kompyuternyye prestupleniya i informatsionnaya bezopasnost / Spravochnik, Moscow, Novyy yurist, 1998, pp. 48-57.
8. Markov A.S., Tsirlov V.L., Barabanov A.V. Metody otsenki nesootvetstviya sredstv zashchity informatsii, Moscow, Radio i svyaz, 2012. 192 p.
9. Diomidis Spinellis. Code Quality: The Open Source Perspective. Addison Wesley, 2006, 569 p.

ПРИМЕР ИСПОЛЬЗОВАНИЯ ТЕОРЕТИКО-ИГРОВОГО ПОДХОДА В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

***Калашников Андрей Олегович**, доктор технических наук*

В работе рассматривается пример использования теоретико–игрового подхода при решении задач обеспечения кибернетической безопасности информационных систем с использованием «ложных» информационных объектов.

***Ключевые слова**: антагонистическая игра, кибербезопасность, «ложный» информационный объект*

EXAMPLE OF USING OF GAME-THEORETIC APPROACH IN PROBLEMS OF ENSURING CYBER SECURITY OF INFORMATION SYSTEMS

***Andrey Kalashnikov**, Doctor of Technical Sciences*

In this paper we consider an example of using game–theoretic approach for solving the tasks of ensuring cyber security information systems, using false information objects.

***Keywords**: zero–sum game, cyber security, false information object*

1. Введение

Приоритетной целью государственной политики на современном этапе является переход на инновационный путь развития. Данный переход характеризуется интенсивным внедрением и использованием передовых информационных технологий в сферах экономики и финансов, промышленности и энергетики, транспорта и связи, государственного управления и национальной безопасности, науки и культуры, образования и здравоохранения и многих других.

Однако, широкое и повсеместное использование информационных технологий немыслимо без повышенного внимания к проблемам их собственной безопасности [1]. Это внимание проявляется не только в развитии и совершенствовании традиционных методов и средств защиты информации, но и в появлении новых подходов к обеспечению кибербезопасности информационных технологий и систем. Одним из примеров подобного подхода может служить постепенное внедрение методов активной защиты, включающей, в том числе методы дезинформации потенциального нарушителя, введения его в заблуждение. Частым случаем такого подхода может служить метод защиты «истинных» информационных объектов, находящихся в системе, путем создания защитником «ложных» информационных объектов. Данный подход не является чем-то принципиально новым, поскольку давно используется в военных и специальных операциях, однако в сфере информационных технологий данный метод только начинает обретать популярность, подтверждением чему служат последние редакции документов отечественных регуляторов (смотри, например [2]).

Необходимо отметить, однако, что использование подобного подхода требует обязательного учета возможных стратегий потенциального нарушителя, собственных стратегий защитника, а так же ясного понимания возникающих при реализации тех и других стратегий угроз и рисков. Иными словами, защитнику необходимо уметь принимать эффективные решения в условиях конфликтного взаимодействия с потенциальным нарушителем. В тоже время, представляется достаточно очевидным, что добиться требуемой эффективности при принятии решений без использования определенного математического аппарата будет достаточно затруднительно. Учитывая изначальную конфликтность взаимодействия защитника и нарушителя представляется целесообразным рассмотреть возможность использования для указанных целей аппарат теории игр.

Ниже будет рассмотрен один из примеров использования теоретико-игрового подхода для решения задач обеспечения кибернетической безопасности информационных систем с использованием «ложных» информационных объектов.

2. Постановка задачи

Рассмотрим формальную постановку задачи. Пусть $O=\{o_1,...,o_N\}$ – множество «истинных» информационных объектов. Обозначим $a_i>0$ – ценность «истинного» информационного объекта $o_i \in O$.

Предположим, что Игрок I (защитник) имеет возможность создать $m_i \geq 0$ «ложных» копий информационного объекта $o_i \in O$. Будем считать, что для любого «истинного» информационного объекта $o_i \in O$ стоимость создания одной его «ложной» копии одинакова и равна $c \geq 0$.

Обозначим

$$\mathfrak{M} = \{(m_1,...,m_N) \mid m_i \geq 0, \sum_{i=1}^{N} m_i = m, m = 1,...,M\}$$

– множество векторов вида $(m_1,...,m_N)$, где, для всех $i=1,...,N$, $m_i \geq 0$ – целые неотрицательные числа, которые характеризуют распределение «ложных» копий на множестве «истинных» информационных объектов. Будем рассматривать вектор $(m_1,...,m_N) \in \mathfrak{M}$ в качестве чистой стратегии, а множество $\mathfrak{M}$ в качестве множества всех чистых стратегий Игрока I.

Фактически, можно считать, что выбирая стратегию $(m_1,...,m_N) \in \mathfrak{M}$, Игрок I трансформирует множество $O=\{o_1,...,o_N\}$ во множество

$$O(m_1,...,m_N) = \{\underbrace{o_1,...,o_1}_{m_1+1}, \underbrace{o_2,...o_2}_{m_2+1},..., \underbrace{o_N,...,o_N}_{m_N+1}\},$$

в котором объект типа $o_i \in O$ присутствует m_i+1 раз. Будем также полагать, что никто кроме Игрока I не в состоянии отличить «истинный» информационный объект от «ложного».

Предположим, далее, что Игрок II (атакующий) имеет возможность атаковать $k_i \geq 0$ информационных объектов типа $o_i \in O$. Будем считать, что для любого «истинного» или «ложного» информационного объекта из множества $O(m_1,...,m_N)$ стоимость успешной атаки на него одинакова и равна $d \geq 0$.

Обозначим

$$\mathfrak{K} = \{(k_1,...,k_N) \mid k_i \geq 0, \sum_{i=1}^{N} k_i = k, k = 1,...,K\}$$

– множество векторов вида $(k_1,...,k_N)$, где, для всех $i=1,...,N$, $k_i \geq 0$ – целые неотрицательные числа, которые характеризуют распределение количества успешных атак Игрока II на множестве «истинных» и «ложных» информационных объектов $O(m_1,...,m_N)$. Будем рассматривать вектор $(k_1,...,k_N) \in \mathfrak{K}$ в качестве чистой стратегии, а множество $\mathfrak{K}$ в качестве множества всех чистых стратегий Игрока II.

Назовем пару векторов $((m_1,...,m_N), (k_1,...,k_N))$ – ситуацией игры, а функцию $H((m_1,...,m_N),(k_1,...,k_N))$ – стоимостью игры в ситуации $((m_1,...,m_N),(k_1,...,k_N))$. Обозначим $h(m_i,k_i)$ для всех $i=1,...,N$:

$$(1) \quad h(m_i,k_i) = \begin{cases} \frac{k_i}{m_i+1}(a_i+cm_i) - dk_i, \text{если } k_i < m_i+1 \\ (a_i+cm_i) - dk_i, \text{если } k_i \geq m_i+1 \end{cases}.$$

Рассмотрим выражение (1) более подробно. Учитывая ранее сделанное замечание о неразличимости «истинных» и «ложных» информационных объектов будем предполагать, что Игрок II выбирает объекты для атаки типа $o_i \in O$ случайным и равновероятным образом. Тогда, если $k_i < m_i+1$, то выражение $\frac{k_i}{m_i+1}(a_i+cm_i)$ представляет собой математическое ожидание ущерба Игрока I с учетом его затрат на создание «ложных» информационных объектов типа $o_i \in O$. Если же $k_i \geq m_i+1$ (то есть Игрок II успешно атакует все «истинные» и «ложные» информационные объекты типа $o_i \in O$), то ущерб Игрока I составит (a_i+cm_i). В свою очередь, выражение dk_i представляет собой затраты Игрока II на проведение k_i успешных атак.

Учитывая выражение (1), определим стоимость игры H в ситуации $((m_1,...,m_N),(k_1,...,k_N))$ следующим образом:

$$(2) \quad H(m_1,...,m_N)(k_1,...,k_N) = \sum_{i=1}^{N} h(m_i,k_i).$$

Будем считать, что в ситуации $((m_1,...,m_N), (k_1,...,k_N))$ выигрыш Игрока I равен $H_I((m_1,...,m_N),(k_1,...,k_N)) = -H((m_1,...,m_N),(k_1,...,k_N))$, а выигрыш Игрока II равен $H_{II}((m_1,...,m_N),(k_1,...,k_N)) = H((m_1,...,m_N),(k_1,...,k_N))$.

Поскольку значения M и K предполагаются конечными, то множества $\mathfrak{M}$ и $\mathfrak{K}$, так же конечны. Естественно предполагать, что в указанных выше условиях, Игрок I будет стремиться минимизировать, а Игрок II максимизировать свои выигрыши. Тогда имеем конечномерную антагонистическую матричную игру, решение которой в смешанных стратегиях может быть найдено с использованием известных методов линейного программирования [3].

Обозначим рассмотренную выше игру Γ_1. Очевидно, что игра Γ_1 однозначно задается кортежем:

$$\Gamma_1 = \langle (I, II), N, M, K, (a_1,...,a_N), c, d, H(\cdot) \rangle \quad (3)$$

Выражение (3) фактически является аналогом традиционного представления игры Γ_1 в нормальной форме, где указываются множества игроков, их стратегий и выигрышей в различных ситуациях игры.

3. Анализ задачи

В рамках анализа приведенной выше задачи представляется целесообразным отметить следующие ее особенности.

Значения M и K задают для игроков I и II максимально возможные количества создаваемых «ложных» информационных объектов и успешных атак соответственно. В этом случае, максимальные затраты Игрока I будут равны $C = c \cdot M$, а Игрока II – $D = d \cdot K$. Тогда, множество стратегий Игрока I можно представить в виде:

$$\mathfrak{M} = \{(m_1,...,m_N) \mid m_i \geq 0, \sum_{i=1}^{N} (c \cdot m_i) \leq C\},$$

а Игрока II, в виде:

$$\mathfrak{K} = \{(k_1,...,k_N) \mid k_i \geq 0, \sum_{i=1}^{N} (d \cdot k_i) \leq D\}.$$

Это дает возможность представить игру Γ_1 в альтернативной форме в виде кортежа:

$$\langle (I, II), N, (a_1,...,a_N), c, C, d, D, H(\cdot) \rangle.$$

Обозначим полученную игру Γ_2. Очевидно, что игры Γ_1 и Γ_2 эквивалентны и их нормальные формы совпадают. Выбор того или иного конкретного вида описания игры определяется исключительно удобством формулировок, зависящих от исходной постановки задачи.

Не смотря на то, что решение игры (3) существует (возможно, в смешанных стратегиях), его нахождение может вызвать определенные трудности, которые, прежде всего, связаны с размерностью задачи. Действительно, обозначим $|\mathfrak{M}|$ – мощность множества $\mathfrak{M}$, иными словами – количество чистых стратегий Игрока I. Обозначим $\mathfrak{M}(m)$ – подмножество множества $\mathfrak{M}$, такое что

$$\mathfrak{M}(m) = \{(m_1,...,m_N) \mid m_i \geq 0, \sum_{i=1}^{N} m_i = m\},$$

где $m \in \{1,...,M\}$ и $|\mathfrak{M}(m)|$ – мощность указанного подмножества. Очевидно, что $\mathfrak{M} = \mathfrak{M}(1) \cup ... \cup \mathfrak{M}(M)$.

В соответствии с [4] имеем:

$$|\mathfrak{M}(m)| = \sum_{m_1+...+m_N=m} \frac{m!}{m_1!...m_N!} = N^m,$$

тогда мощность множества $\mathfrak{M}$, или, иными словами, количество чистых стратегий Игрока I, будет равна: $|\mathfrak{M}| = \sum_{m=1}^{M} N^m$.

Аналогично, количество чистых стратегий Игрока II будет равно: $|\mathfrak{K}| = \sum_{k=1}^{K} N^k$. В этом случае общее количество ситуаций игры может быть оценено величиной $|\mathfrak{M}| \times |\mathfrak{K}|$. Очевидно, что уже при достаточно скромных значениях N, M и K размерность задачи линейного программирования для поиска решения игры Γ_1 становится чрезвычайно большой.

Большая размерность игры Γ_1, определяется, в первую очередь, тем фактом, что выбор игроками своих стратегий предполагается одновременным и независимым. Если отказаться от этого предположения, то размерность игры, в определенных случаях, может быть снижена.

Рассмотрим, например, следующую игру: сначала Игрок I выбирает свою стратегию из множества $\mathfrak{M}$, а затем, Игрок II, зная выбор Игрока I, осуществляет выбор своей стратегии из множества $\mathfrak{K}$. Выигрыши и проигрыши в данной игре задаются функцией H, определяемой выражениями (1) и (2). Обозначим полученную игру Γ_3. Несложно показать, что размерность игры Γ_3 равна N^{M+K} и, соответственно, меньше размерности игры Γ_1. Может показаться, что в игре Γ_3 Игрок I находится в гораздо менее выгодных условиях, чем Игрок II. В общем случае это действительно так, однако в определенных случаях, как это показано ниже, у Игрока I может существовать оптимальная стратегия, не зависящая от действий Игрока II. Размерность игры Γ_3 при этом становится приблизительно равной N^K.

Возможен и иной путь снижения размерности игры Γ_1. Если, например, стоимость создания «ложного» информационного объекта удовлетворяет соотношению: $c - a_i \leq 0$, для всех $i = 1,...,N$, то, как нетрудно показать, функция $h(m_i, k_i)$ из выражения (1) будет монотонно невозрастающей по m_i. Аналогично, если стоимость успешной атаки удовлетворяет соотношению:

$\frac{1}{m_i + 1}(a_i + cm_i) - d \geq 0$, для всех $i = 1,...,N$, то функция $h(m_i, k_i)$, при дополнительном условии: $k_i < m_i + 1$, будет монотонно неубывающей функцией по k_i. Тогда, в условиях игры Γ_1 Игроку I имеет смысл ограничить область поиска свои оптимальные стратегии только множеством $\mathfrak{M}(M)$, а Игроку II – множеством $\mathfrak{K}(K)$. Обозначим подобную игру $\Gamma_1(M,K)$. Несложно показать, что размерность игры $\Gamma_1(M,K)$, как и размерность игры Γ_3, равна N^{M+K} и, соответственно, так же меньше размерности игры Γ_1.

Игра Γ_1, так же может быть обобщена следующим образом. Предположим, что стоимость

создания «ложного» информационного объекта $o_i \in O$ равна $c_i \geq 0$, а стоимость успешной атаки на него – $d_i \geq 0$ для всех $i = 1,...,N$. Тогда выражение (1) примет вид:

(4)
$$h(m_i,k_i) = \begin{cases} \dfrac{k_i}{m_i+1}(a_i + c_i m_i) - d_i k_i, \text{если } k_i < m_i + 1 \\ (a_i + c_i m_i) - d_i k_i, \text{если } k_i \geq m_i + 1 \end{cases}.$$

Учитывая выражения (4) и (2), можно определить стоимость игры H в ситуации $((m_1,...,m_N),(k_1,...,k_N))$.

Обозначим рассмотренную выше игру Γ_4. Игра Γ_4 однозначно задается кортежем:

(5)
$$\Gamma_4 = \langle (I, II), N, M, K, (a_1,...,a_N), (c_i,...,c_N), (d_i,...,d_N), H(\cdot) \rangle$$

Очевидно, что возможности по дальнейшему обобщению игры Γ_1 выражением (5) не исчерпываются.

4. Пример решения задачи

Пусть в условиях игры Γ_1 имеем: $M=1$ и $K=1$. То есть, Игрок I имеет возможность создать лишь один «ложный» информационный объект, а Игрок II имеет возможность успешно атаковать один из $N+1$ информационных объектов. Будем так же считать, что для значений $a_i > 0$ и $c \geq 0$ выполнено следующее соотношение:

(6) $$a_1 > a_2 > ... > a_N > c \geq 0.$$

Последнее неравенство в выражении (6) отражает предположение, что стоимость создания «ложного» объекта меньше ценности любого «истинного» информационного объекта из множества $O = \{o_1,...,o_N\}$. В этих условиях имеем:

$\frac{1}{2}(a_i + c) < a_i$ для любого $i = 1,...,N$.

Чистой стратегией Игрока I, в таком случае, можно считать порядковый номер i информационного объекта $o_i \in O$, для которого создается «ложный» объект, а чистой стратегией Игрока II, соответственно, порядковый номер j информационного объекта, на который совершается атака. В этом случае пара (i,j) будет являться ситуацией игры, а функция $H(i,j)$– стоимость игры будет иметь вид:

(7) $$H(i,j) = \begin{cases} \dfrac{1}{2}(a_i + c) - d, \text{если } i = j \\ a_j - d, \text{если } i \neq j \end{cases}, i,j = 1,...,N.$$

Несложно показать, что без ограничения общности можно полагать, что стоимость успешной атаки Игрока II $d = 0$, тогда выражение (7) примет вид:

(8) $$H(i,j) = \begin{cases} \dfrac{1}{2}(a_i + c), \text{если } i = j \\ a_j, \text{если } i \neq j \end{cases}, i,j = 1,...,N.$$

В ситуации (i,j) выигрыш Игрока II составит $H_{II}(i,j)=H(i,j)$, а проигрыш Игрока I $H_I(i,j)=-H(i,j)$. Обозначим i^* и j^* чистые оптимальные стратегии Игроков I и II, соответственно.

Игрок I будет стремиться минимизировать свой проигрыш, тогда, если он выбирает любую стратегию $i \neq 1$, то, поскольку Игрок II будет стремиться максимизировать свой выигрыш, то он выберет стратегию $j = 1$, обеспечивая себе максимально возможный выигрыш и, соответственно, максимально возможный проигрыш Игроку I, что, разумеется, не может того устроить. Следовательно, не зависимо от действий Игрока II, оптимальной стратегией Игрока I будет стратегия $i^* = 1$.

В свою очередь, Игрок II будет стремиться максимизировать свой выигрыш, тогда, поскольку оптимальной стратегией Игрока I будет стратегия $i^*=1$, то, как легко показать, оптимальной стратегией Игрока II будет стратегия $j^*=1$, если $\frac{1}{2}(a_1 + c) > a_2$ или стратегия $j^*=2$, если

$$\frac{1}{2}(a_1 + c) \leq a_2.$$

Приведенное выше решение для игры $\Gamma_1(1,1)$ представляет собой в известной степени «вырожденный» случай. Тем не менее, это решение иллюстрирует подход, которого может придерживаться Игрок I при формировании своей оптимальной стратегии и в более общем случае. В своих дальнейших рассуждениях будем опираться на результаты, изложенные в [5], не приводя при этом строгих доказательств.

Рассмотрим игру $\Gamma_1(M,K)$. Предположим, для простоты, что выполнено соотношение (6), причем $c=0$ и $d=0$. Чистая стратегия Игрока I : $(m_1,...,m_N) \in \mathfrak{M}$(M), чистая стратегия Игрока II: $(k_1,...,k_N) \in \mathfrak{K}$(K). Тогда в ситуации игры $((m_1,...,m_N),(k_1,...,k_N))$ для всех $i=1,...,N$:

(9) $$h(m_i,k_i) = \begin{cases} \dfrac{k_i}{m_i+1} a_i, \text{если } k_i < m_i + 1 \\ a_i, \text{если } k_i \geq m_i + 1 \end{cases}.$$

Предположим, что существует стратегия $(m_1^*,...,m_N^*) \in \mathfrak{M}(M)$ такая, что:

(10) $$\frac{a_1}{m_1^*+1} = \frac{a_2}{m_2^*+1} = ... = \frac{a_N}{m_N^*+1} = a,$$

тогда, как несложно показать, стратегия

$(m_1^*,...,m_N^*)$ будет оптимальной стратегией Игрока I. Действительно, пусть $(k_1,...,k_N) \in \mathfrak{K}(K)$ некоторая стратегия Игрока II, тогда его выигрыш (соответственно, проигрыш Игрока I) с учетом (9) будет равен:

(11) $$H((m_1^*,...,m_N^*),(k_i,...,k_N)) = \sum_{i=1}^{N} h(m_i^*,k_i) = aK\ .$$

Выберем произвольную пару индексов i_1 и i_2 таких, что $1 \le i_1 < ... < i_2 \le N$ и построим, если это возможно, стратегию $(m_1^0,...,m_N^0) \in \mathfrak{M}(M)$ так, что для всех $i = 1,...,N$:

(12) $$m_i^0 = \begin{cases} m_i^*, если\ i \ne i_1, i \ne i_2 \\ m_i^* - 1, если\ i = i_1 \\ m_i^* + 1, если\ i = i_2 \end{cases}\ .$$

Тогда имеем:

$$\Delta H = H((m_1^0,...,m_N^0),(k_i,...,k_N)) - H((m_1^*,...,m_N^*),(k_i,...,k_N)) = \sum_{i=1}^{N}(h(m_i^0,k_i) - h(m_i^*,k_i)) =$$

$$= (h(m_{i_1}^* - 1,k_{i_1}) - h(m_{i_1}^*,k_{i_1})) + (h(m_{i_2}^* + 1,k_{i_2}) - h(m_{i_2}^*,k_{i_2})) = (\frac{k_{i_1}}{m_{i_1}^*} - \frac{k_{i_1}}{m_{i_1}^* + 1})a_{i_1} + (\frac{k_{i_2}}{m_{i_2}^* + 2} - \frac{k_{i_2}}{m_{i_2}^* + 1})a_{i_2} =$$

$$= (\frac{k_{i_1}m_{i_1}^* a_{i_1} + k_{i_1}a_{i_1} - k_{i_1}m_{i_1}^* a_{i_1}}{m_{i_1}^*(m_{i_1}^* + 1)} + \frac{k_{i_2}m_{i_2}^* a_{i_2} + k_{i_2}a_{i_2} - k_{i_2}m_{i_2}^* a_{i_2} - 2k_{i_2}a_{i_2}}{(m_{i_2}^* + 2)(m_{i_2}^* + 1)}) = (\frac{k_{i_1}a}{m_{i_1}^*} - \frac{k_{i_2}a}{(m_{i_2}^* + 2)})\ .$$

Из (6) и (10) следует, что $m_{i_1} \ge m_{i_2} + 1$, тогда: $\Delta H > (\frac{k_{i_1}a}{(m_{i_2}^* + 1)} - \frac{k_{i_2}a}{(m_{i_2}^* + 1)}) = \frac{a}{(m_{i_2}^* + 1)}(k_{i_1} - k_{i_2})$.

Откуда $\Delta H > 0$, если существует некоторая стратегия $(k_1,...,k_N) \in \mathfrak{K}(K)$ Игрока II, такая, что $k_{i_1} > k_{i_2}$. Очевидно, что такая стратегия существует.

Построим теперь, если это возможно, стратегию $(m_1^1,...,m_N^1) \in \mathfrak{M}(M)$ так, что для всех $i = 1,...,N$:

(13) $$m_i^1 = \begin{cases} m_i^*, если\ i \ne i_1, i \ne i_2 \\ m_i^* + 1, если\ i = i_1 \\ m_i^* - 1, если\ i = i_2 \end{cases}\ .$$

Тогда имеем:

$$\Delta H = H((m_1^1,...,m_N^1),(k_i,...,k_N)) - H((m_1^*,...,m_N^*),(k_i,...,k_N)) = \sum_{i=1}^{N}(h(m_i^1,k_i) - h(m_i^*,k_i)) =$$

$$= (h(m_{i_1}^* + 1,k_{i_1}) - h(m_{i_1}^*,k_{i_1})) + (h(m_{i_2}^* - 1,k_{i_2}) - h(m_{i_2}^*,k_{i_2})) = (\frac{k_{i_1}}{m_{i_1}^* + 2} - \frac{k_{i_1}}{m_{i_1}^* + 1})a_{i_1} + (\frac{k_{i_2}}{m_{i_2}^*} - \frac{k_{i_2}}{m_{i_2}^* + 1})a_{i_2} =$$

$$= (\frac{k_{i_1}m_{i_1}^* a_{i_1} + k_{i_1}a_{i_1} - k_{i_1}m_{i_1}^* a_{i_1} - 2k_{i_1}a_{i_1}}{(m_{i_1}^* + 2)(m_{i_1}^* + 1)} + \frac{k_{i_2}m_{i_2}^* a_{i_2} + k_{i_2}a_{i_2} - k_{i_2}m_{i_2}^* a_{i_2}}{m_{i_2}^*(m_{i_2}^* + 1)}) = (-\frac{k_{i_1}a}{(m_{i_1}^* + 2)} + \frac{k_{i_2}a}{m_{i_2}^*})\ .$$

Из (6) и (10) следует, что $m_{i_1} \ge m_{i_2} + 1$, тогда: $\Delta H > (\frac{k_{i_2}a}{(m_{i_1}^* + 1)} - \frac{k_{i_1}a}{(m_{i_1}^* + 1)}) = \frac{a}{(m_{i_1}^* + 1)}(k_{i_2} - k_{i_1})$.

Из (6) и (10) следует, что $m_{i_1} \ge m_{i_2} + 1$, тогда: $\Delta H > (\frac{k_{i_2}a}{(m_{i_1}^* + 1)} - \frac{k_{i_1}a}{(m_{i_1}^* + 1)}) = \frac{a}{(m_{i_1}^* + 1)}(k_{i_2} - k_{i_1})$.

Откуда $\Delta H > 0$, если существует некоторая стратегия $(k_1,...,k_N) \in \mathfrak{K}(K)$ Игрока II, такая, что $k_{i_1} < k_{i_2}$. Очевидно, что такая стратегия так же существует.

Таким образом, показано, что даже при минимально возможном в условиях игры $\Gamma_1(M,K)$ отступлении Игрока I от своей оптимальной стратегии $(m_1^*,...,m_N^*) \in \mathfrak{M}$(M) у Игрока II появляется возможность

увеличить свой выигрыш. Приведенные выше рассуждения не являются, конечно, строгим доказательством данного факта, но показывают путь, на котором указанное доказательство может быть получено.

5. Заключение

В работе был рассмотрен пример использования теоретико-игрового подхода для решения задач обеспечения кибернетической безопасности информационных систем с использованием «ложных» информационных объектов. Был сформулированы ряд теоретико-игровых задач, в том числе, в форме антагонистических матричных игр и рассмотрены пути их решения. Большинство рассмотренных задач носило постановочный характер, что оставляет широкий простор для будущих исследований.

Литература

1. Калашников А.О. Модели и методы организационного управления информационными рисками корпораций. М.: Эгвес, 2011. – 312 с.
2. Приказ ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-tekhnicheskaya-zashchita-informatsii/dokumenty/prikazy/703-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n -17).
3. Протасов И.Д. Теория игр и исследование операций: Учебное пособие. – М.: Гелиос АРВ, 2003. – 368 с.
4. Сачков В.Н. Введение в комбинаторные методы дискретной математики. М.: Наука. Главная редакция физико-математической литературы., 1982. – 384 с.
5. Калашников А.О. Арбитражная модель ресурсного обеспечения информационной безопасности организационных систем// Управление большими системами. – 2006. – № 14. – С. 91 – 105.

References

1. Kalashnikov A.O. Modeli i metodi organizacionnogo upravleniya informatsionnimi riskami korporatsii. M.: Egves, 2011. – 312 s.
2. Prikaz FSTEK Rossii ot 11.02.2013 №17 «Ob utverjdenii Trebovanii o zashchite informatsii ne sostavlyayushei gosudarstvennuyu tainu soderjasheisya v gosudarstvennih informatsionnih sistemah» (fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-tekhnicheskaya-zashchita-informatsii/ dokumenty/prikazy/703-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17).
3. Protasov I.D. Teoriya igr I issledovanie operatsii: Uchebnoe posobie. – M.: Gelios ARV, 2003. – 368 s.
4. Sachkov V.N. Vvedenie v kombinatornie metodi diskretnoi matematiki. M.: Nauka. Glavnaya radaktsiya fiziko-matematicheskoi literature., 1982. – 384 s.
5. Kalashnikov A.O. Arbitrajnaya model resursnogo obespecheniya informatsionnoi bezopasnosti organizatsionnih sistem // Upravlenie bolshimi sistemami. – 2006. – № 14. – S. 91 – 105.

МЕТОДИЧЕСКИЙ ПОДХОД К ОЦЕНИВАНИЮ ЭФФЕКТИВНОСТИ ЛОЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Язов Юрий Константинович, *доктор технических наук, профессор*
Сердечный Алексей Леонидович
Шаров Иван Александрович

В настоящее время при защите информационных систем актуальным становится применение «стратегии обмана» и отвлечения нарушителя на ложные ресурсы. Вместе с тем при использовании ложных информационных систем важно знать, насколько эффективно можно обмануть с ее помощью нарушителя при ограничении на потребление ресурсов. В данной статье предложен возможный методический подход к оцениванию эффективности ложных информационных систем и сделаны выводы о направлениях дальнейшего развития методического обеспечения оценивания их эффективности.

Ключевые слова: *ложная информационная система (ЛИС), уязвимость программного обеспечения, несанкционированный доступ (НСД), эффективность защиты*

METHODICAL APPROACH FOR ESTIMATION OF EFFICIENCY OF HONEYPOT SYSTEM

Yuri Yazov, *Doctor of Technical Sciences, Professor*
Alexey Serdechnyy
Ivan Sharov

Nowadays becomes very actual application of «deception strategies» and intruder distraction at false resources in aspect of information systems protecting. In addition to that it's important to know when using honeynets, how efficiently it could deceive the intruder with restriction of low resources consumption. In the current article possible method of evaluation of efficiency of honeypot systems is suggested and conclusion about line of further development of methodogical support of estimate of efficiency is made.

Keywords: *honeynet, software vulnerability, unauthorized access, effectiveness of protection*

При защите информационных систем (ИС) большое внимание уделяется вопросам обнаружения и нейтрализации уязвимостей входящего в их состав программного обеспечения (ПО). В настоящее время все основные способы решения данной задачи основываются на применении «стратегии запрета». Для этого в ручном или автоматизированном режиме проводится поиск уязвимостей ПО ИС, информация о которых имеется в открытых или закрытых базах данных. После обнаружения уязвимость нейтрализуется либо за счет обновления ПО, либо за счет использования средств защиты информации, таких как межсетевые экраны, системы обнаружения вторжений, средства антивирусной защиты и т.д., которые делают невозможным эксплуатацию данной уязвимости для реализации НСД.

Однако, как показывает практика, такая стратегия оказывается неэффективной против уязвимостей «нулевого дня». Это связано с тем, что между выпуском ПО и появлением информации об уязвимости, а тем более устранением ее разработчиками, в большинстве случаев проходит большое количество времени, в течение которого система оказывается уязвимой для НСД. Несмотря на то, что правильно настроенные средства защиты информации делают эксплуатацию некоторых из таких уязвимостей невозможной, всегда остается вероятность наличия не устраненных уязвимостей, а также уязвимостей в ПО самих средств защиты.

В связи с этим в настоящее время актуальным становится применение «стратегии обмана» или

отвлечения нарушителя на ложный информационный ресурс. Необходимость применения средств, реализующих такую стратегию и называемых ложными информационными системами (ЛИС), отмечается и в одном из последних утвержденных нормативных правовых актов «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [1]. Как показали исследования [2], реализуя с помощью ЛИС «стратегию обмана» нарушителя и отвлекая его на ложный информационный ресурс, можно не только не позволить злоумышленнику получить несанкционированный доступ (НСД) к защищаемой информации, но и найти неизвестные ранее уязвимости ПО.

Развитию практики применения ЛИС способствует все большее внедрение технологии виртуализации, появление программных средств виртуализации, таких как VMware ESX/ESXi, Microsoft Hyper-V, Citrix Xen Server и др., позволяющих создать виртуальную инфраструктуру и управлять ею.

Вместе с тем при использовании ЛИС важно знать, насколько эффективно можно обмануть с ее помощью нарушителя и при этом не создать сложностей для функционирования защищаемой ИС, поскольку значительный вычислительный ресурс может оказаться задействованным на обеспечение функционирование ЛИС. С учетом изложенного под эффективностью ЛИС здесь и далее понимается степень достижения цели отвлечения нарушителя от защищаемого информационного ресурса при условии, что ЛИС не влияет существенным образом на функционирование защищаемой ИС.

До настоящего времени методическое обеспечение оценивания эффективности ЛИС, в том числе построенных с использованием средств виртуализации, не разрабатывалось. При этом следует отметить, что в таких системах крайне важно учитывать ограничения на потребление вычислительных ресурсов, поскольку такие ограничения существенно влияют на количество эмулируемых ложных объектов, а, следовательно, и на эффективность защиты.

В данной статье предлагается возможный подход к такому оцениванию, основанный на вероятностной оценке возможности выполнения одновременно двух условий:

срыва НСД к защищаемой информации за счет использования ЛИС;

отсутствия превышения затрат вычислительных ресурсов информационной системы установленного (недопустимого) уровня.

Срыв НСД достигается за счет того, что нарушитель или инициированный им процесс доступа (например, с использованием вредоносной программы) переориентируется на ложные, созданные в виртуальной среде объекты - эмулируемые с помощью виртуальных машин (ВМ) компьютеры в составе компьютерной сети, подключенной к сети общего пользования.

Вероятность НСД ($P_D^{(i)}(t)$) при условии выполнения указанного ограничения на используемый вычислительный ресурс R в общем случае зависит от времени и может быть оценена следующим образом:

$$P_D^{(I)}(t) = \begin{cases} P_{(НСД)}(I,t), \text{если } R \le R_{lim}, \\ 0, \text{в противном случае}, \end{cases} \quad (1)$$

где $P_{(НСД)}(I,t)$ - вероятность того, что за время t нарушитель сумеет получить НСД к I объектам (компьютерам) в составе информационной системы;

R_{lim} - допустимый уровень затрат вычислительных ресурсов R информационной системы.

Эффективность ЛИС как средства защиты по аналогии с [3] рассчитывается с использованием разностного показателя:

$$\eta_{\Delta}(t) = P_D^{(I)}(t) - P_{D(ЛИС)}^{(I)}(t), \quad (2)$$

или относительно-разностного показателя:

$$\eta(t) = \frac{P_D^{(I)}(t) - P_{D(ЛИС)}^{(I)}(t)}{P_D^{(I)}(t)} = 1 - \frac{P_{D(ЛИС)}^{(I)}(t)}{P_D^{(I)}(t)}, P_{D(ЛИС)}^{(I)}(t) > 0, \quad (3)$$

где $P_D^{(I)}(t)$ - вероятность того, что в условиях отсутствия ЛИС за время t нарушитель сумеет получить НСД к I объектам (компьютерам) в составе ИС;

$P_{D(ЛИС)}^{(I)}(t)$ - вероятность того, что в условиях функционирования ЛИС за время t нарушитель сумеет получить НСД к I объектам (компьютерам) в составе ИС.

Следует отметить, что если вероятность НСД в условиях отсутствия ЛИС близка к единице, то значения показателей эффективности совпадают и определяются только значением вероятности $P_{D(ЛИС)}^{(I)}(t)$:

$$\eta(t) = 1 - P_{D(ЛИС)}^{(I)}(t). \quad (4)$$

Рассмотрим подход к оценке этой вероятности. При реализации НСД нарушитель или вре-

доносная программа осуществляет случайный поиск компьютера, являющегося целью атаки, и распознавание его с отнесением к целевому объекту (то есть к компьютеру с защищаемой информацией). При этом поиск может начинаться с любого элемента информационной системы, имеющей IP-адрес или с ложного элемента в составе ЛИС, формируемого ВМ. Пусть в составе информационной системы имеется N_{Tr} истинных объектов, ЛИС формирует N_F ложных объектов, а для анализа каждого объекта на предмет отнесения его к целевому тратится в среднем время $\bar{\tau}_a$. Тогда за время t нарушитель сможет реализовать k шагов, на каждом из которых будут анализироваться попавшиеся ему истинные или ложные объекты:

$$k = \left[\frac{t}{\bar{\tau}_a}\right], \quad (5)$$

где знак $[\,]$ означает выделение целой части дроби.

Вероятность того, что нарушитель за k шагов сумеет получить доступ к i целевым объектам в условиях применения ЛИС, а также примерно равной исходной вероятности доступа к объектам $P_{НСД}$ на каждом шаге, определяется следующим образом:

$$P^{(i)}_{D(ЛИС)}(k) = P^{i}_{НСД} \cdot \prod_{j=0}^{i-1} \frac{N_{Tr} - j}{N_{Tr} + N_F - j} \cdot \cdot \left(1 + \sum_{m=1}^{k-i} C^{m}_{i+m-1} \prod_{j=1}^{m} \frac{N_F - j + 1}{N_{Tr} + N_F - j - i + 1}\right), \quad (6)$$

где C^{m}_{i+m-1} – количество сочетаний из $i + m - 1$ по m.

Кроме того, учитывая (1), при расчете показателя эффективности ЛИС необходимо оценивать ограничение на потребление ЛИС вычислительных ресурсов защищаемой информационной системы. К вычислительным ресурсам в данном случае относятся [4]: объём свободной оперативной памяти, необходимой для работы истинных виртуальных машин *для каждого* сервера виртуализации[1]; резерв свободного процессорного времени, необходимый для надёжной работы *каждого* сервера виртуализации; доля зарезервированного объема трафика, который может передаваться в информационной системе. Ни один из указанных ресурсов не должен превысить допустимый уровень (как правило, резерв свободного процессорного времени должен быть не менее 25%, а доля зарезервированного объема трафика – 50%).

Рассмотрим пример, когда нарушитель осуществляет выбор целевого объекта, в информационной системе, состоящей из 15 объектов, среди которых серверы виртуализации, рабочие станции пользователей, файловые серверы, ложные ВМ и т.п. ($N_{Tr} = 15$). Из них 5 объектов являются ложными ($N_F = 5$), а 3 – целевыми. Анализ объектов осуществляется методом сканирования сетевыми пакетами, в ходе которого определяется тип операционной системы объекта и состав сетевых служб. Продолжительность такого сканирования составляет 30 секунд ($\bar{\tau}_a = 30$), таким образом, для того, чтобы проанализировать все 15 объектов нарушитель должен затратить 7,5 секунд. Предположим, что $P_{НСД} = 0,8$,. Кроме того, в информационной системе работает система предотвращения вторжений, позволяющая в течении 2 секунд выявить и нейтрализовать действия нарушителя ($t = 120, k = 4$).

В информационной системе присутствует два одинаковых сервера виртуализации со следующими характеристиками: 32 ГБ оперативной памяти, пропускная способность канала связи – 1 ГБ/сек, 4 ТБ памяти на жестком диске, процессор – Intel Xeon E7. Расход вычислительных ресурсов сервера виртуализации на работу ВМ (как целевых, так и ложных) представлен в таблице 1.

[1] Сервер виртуализации представляет собой высокопроизводительный компьютер с установленным гипервизором первого типа, обеспечивающий работу виртуальных машин

Таблица 1 *– Расход вычислительных ресурсов сервера виртуализации*

Объект	Процессорное время	Загруженность канала связи	Оперативная память	Память на жестком диске
Целевая ВМ	0,7%	0,001%	2 ГБ	42 ГБ
Ложная ВМ	0,75%	0,00005%	512 МБ	21 ГБ
Гипервизор	0,5%	0,0005%	256 МБ	0,5 ГБ

Условие $R \le R_{lim}$ выполняется, когда на каждом сервере виртуализации свободно не менее 8 ГБ оперативной памяти, на жестком диске – не менее 40 ГБ, канал связи загружен не более чем на 50%, а процессор – на 75%. Данное условие верно, если количество ложных ВМ на одном сервере виртуализации не превышает 15 (количество ложных ВМ в данном случае ограничено дефицитом свободной оперативной памяти). С учётом приведенных данных эффективность ЛИС рассчитывается следующим образом:

$$\eta = 1 - \left(0{,}729 \cdot \prod_{j=0}^{2} \frac{15-j}{20-j} \cdot \left(1 + C_3^3 \prod_{j=1}^{1} \frac{6-j}{11-j}\right)\right) = 0{,}271. \quad (7)$$

На рисунках 1 – 4 показаны зависимости вероятности доступа к целевым объектам от количества ложных объектов, исходной вероятности доступа, определяемой в условиях отсутствия ЛИС, количества целевых объектов в защищаемой ИС и времени.

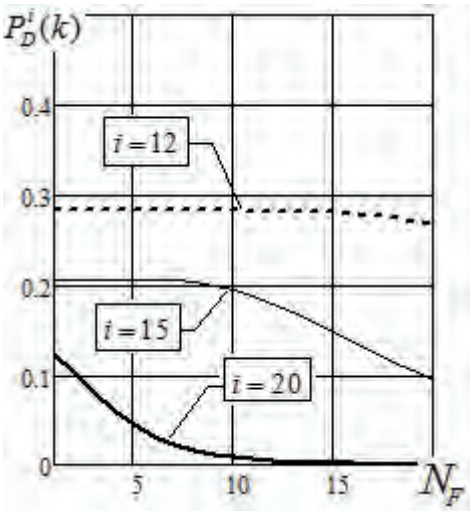


Рис. 1. *Зависимость вероятности несанкционированного доступа за 20 шагов к целевым объектам от количества эмулируемых ложных объектов при исходной вероятности доступа, равной 0.9, и количестве истинных объектов - 50*

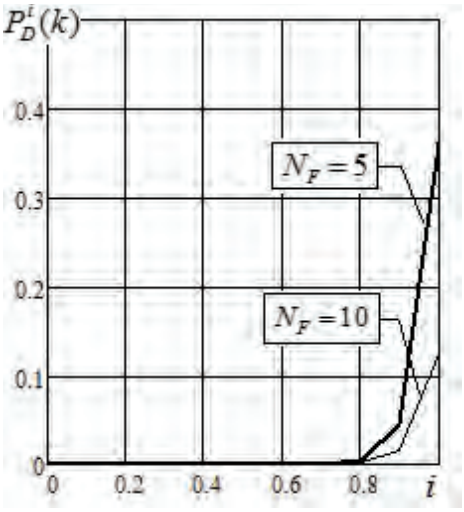


Рис. 2. *Зависимость вероятности несанкционированного доступа к 20 целевым объектам от исходной вероятности доступа к ним в отсутствии ЛИС при исходной вероятности доступа, равной 0.9, если информационная система состоит из 50 истинных объектов*

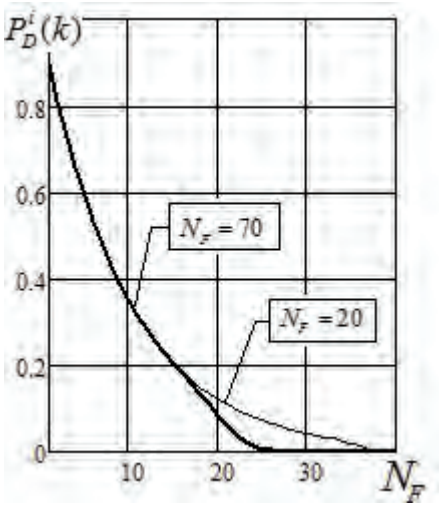


Рис. 3. *Зависимость вероятности несанкционированного доступа за 20 шагов к целевым объектам от количества эмулируемых ложных объектов при исходной вероятности доступа, равной 0.9, и количестве истинных объектов - 50*

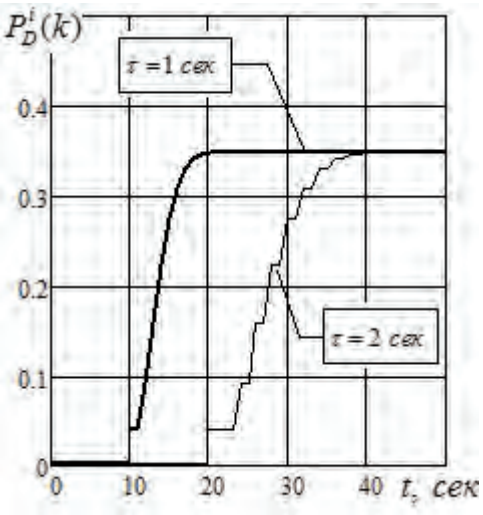


Рис. 4. *Зависимость вероятности несанкционированного доступа к 10 целевым объектам от времени при исходной вероятности доступа, равной 0.9 и 20 ложных объектов, если информационная система состоит из 50 истинных объектов*

Анализ полученных результатов показал, что после достижения определенного количества эмулируемых ложных объектов рост эффективности ЛИС становится несущественным. Это позволяет выбирать целесообразное количество эмулируемых ложных объектов в зависимости от заданных условий.

Однако полученные соотношения и зависимости позволяют оценивать эффективность ЛИС и влияние на нее существенных параметров и характеристик таких средств защиты при условии, что ложные объекты, эмулируемые ЛИС, абсолютно идентичны истинным (целевым) объектам. Если это условие не выполняется, то необходимо оценивать вероятность распознавания ложных объектов и дискредитации таким образом самой ЛИС.

Кроме того, изложенный подход к оценке эффективности ЛИС правомерен в основном для статических ЛИС, состав и параметры которых не меняются в процессе защиты. В реальных ИС состав функционирующих объектов постоянно меняется: часть компьютеров включается или выключается, создаются новые или закрываются действующие виртуальные каналы взаимодействия, изменяется состав программного обеспечения в сети, наконец, изменяется состав защищаемых информационных ресурсов. В этих условиях возникают демаскирующие признаки, по которым нарушитель может распознать наличие ложных объектов и это должно учитываться при оценке эффективности ЛИС.

Все это обусловливает необходимость создания специализированного методического обеспечения оценивания эффективности ЛИС, учитывающего как возможности распознавания ложных и истинных объектов, так и динамику функционирования самой защищаемой ИС и динамических ЛИС, меняющих свой состав и характеристики по аналогии с реальными ИС. Такое обеспечение должно базироваться не только на аналитических методах оценки, но и включать в себя имитационные модели, позволяющие верифицировать аналитические алгоритмы, обосновывать состав демаскирующих признаков ложных объектов, создаваемых в виртуальной среде, и истинных объектов в составе ИС, определять допустимый уровень затрат вычислительных ресурсов ИС на функционирование ЛИС, определять временные характеристики доступа нарушителя или инициируемого им процесса как к целевым, так и к ложным объектам и т.д.

С учетом изложенного на рисунке 5 показаны состав и структура первоочередного методического обеспечения, которое, на наш взгляд, необ-

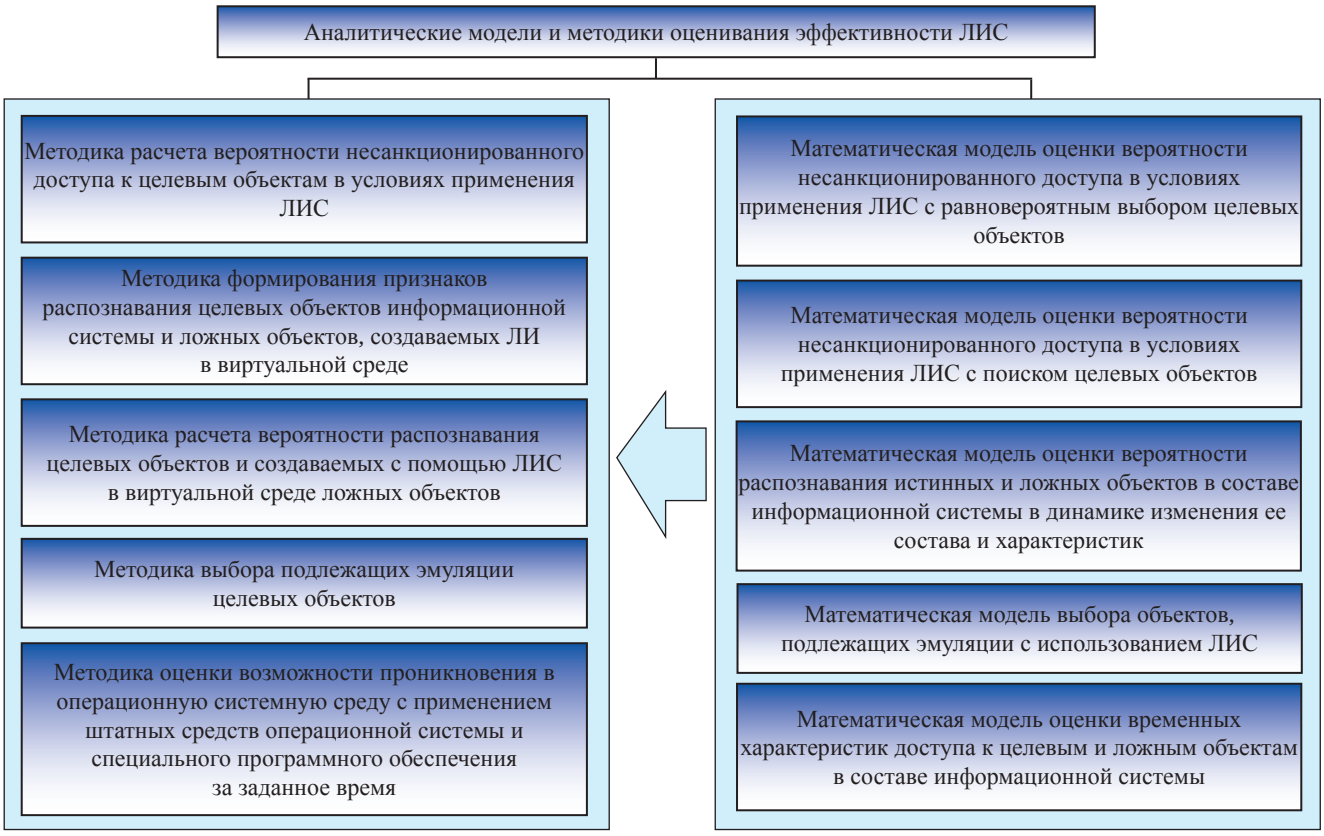


***Рис. 5.** – Состав и структура методического обеспечения оценивания эффективности ложных информационных систем*

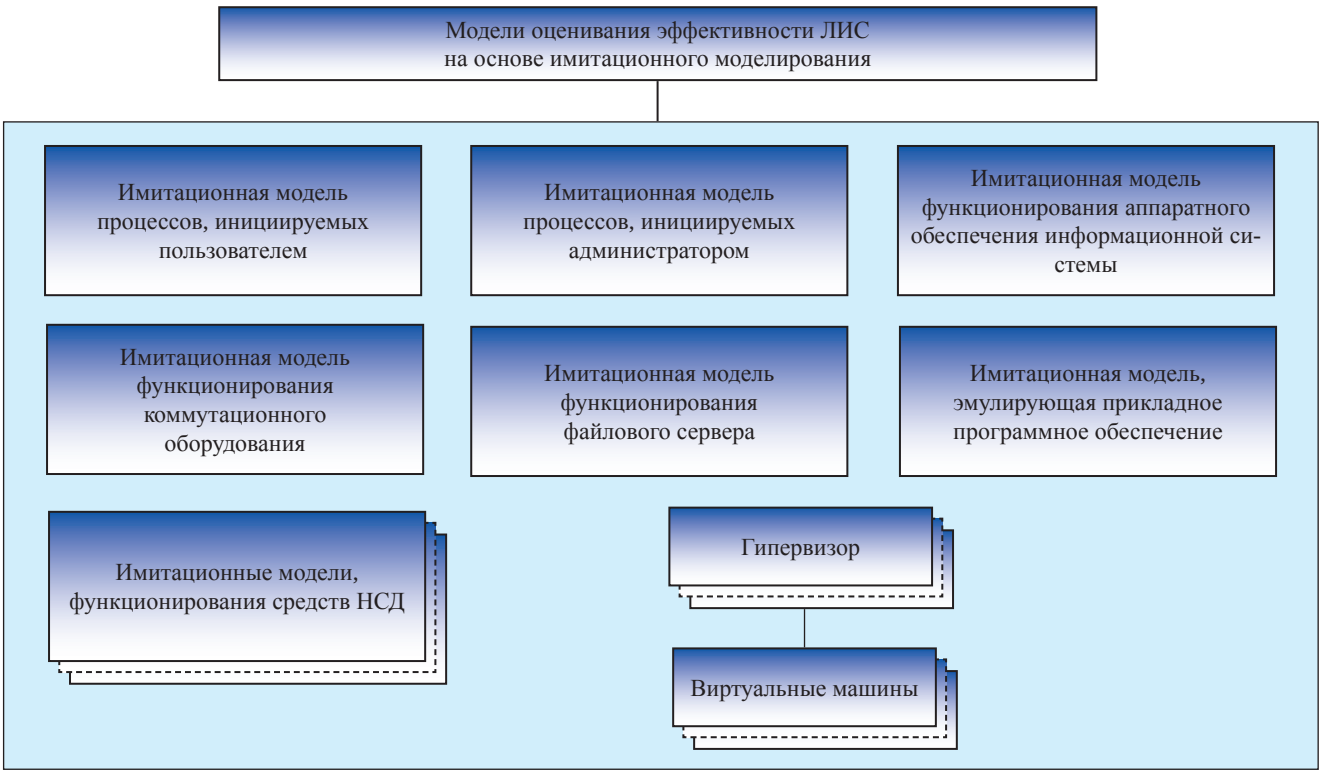


Рис. 5. *– Состав и структура методического обеспечения оценивания эффективности ложных информационных систем*

ходимо разработать в интересах решения задачи оценивания эффективности ЛИС.

Разработанный методический подход к оцениванию эффективности ЛИС направлен на развитие методического обеспечения, которое позволило бы перейти от качественных к количественным процедурам оценивания, что существенно повысит обоснованность характеристик и путей построения ЛИС как перспективных средств защиты информации.

Литература

1. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11.02.2013 № 17 г. Москва.
2. Сердечный, А.Л. Инновационный подход к защите информации в виртуальных вычислительных сетях, основанный на стратегии обмана / А.Л. Сердечный // Информация и безопасность. – 2013. – №3. – 399-403 с.
3. Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных системах – Ростов-на-Дону: СКНЦ ВШ, 2006. – 274 с.
4. Михеев, М.О. Администрирование VMware vSphere 5 // М.:ДМК Пресс, 2012.

References

1. Requirements about protection of the information which are doing not make the state secret, containing in the government information systems. Are confirmed by order FSTEC Russia from 11.02.2013 № 17, Moscow.
2. Serdechnyy A.L., 2013. The innovative approach to information protection in the virtual computer networks, based on deceit strategy // Information and Security 3, 399-403.
3. Yazov Y.K., 2006. Bases methodology of a quantitative estimation effectiveness of information protection in computer systems // Rostov on Don: SKNTS VSH.
4. Miheev, M.O., 2012. VMware vSphere 5 administration // M.:DMK Press.

КИБЕРБЕЗОПАСНОСТЬ И ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ Часть 1

***Карцхия Александр Амиранович**, кандидат юридических наук, профессор*

Цикл статей посвящен современному механизму защиты интеллектуальной собственности в глобальной информационной среде. Поощрение инновационной деятельности и защита правообладателей от киберугроз выходит на первый план в государственных (национальных) стратегиях интеллектуальной собственности. Интеллектуальная собственность как особо ценный нематериальный актив (базы данных, коммерческие секреты и ноу–хау, компьютерных программ и т.д.) является предметом новых угроз в киберпространстве. Кибербезопасность предотвращает нарушение прав интеллектуальной собственности, а также обеспечивает правообладателям конфиденциальность баз данных, коммерческой тайны и ноу–хау. Защита интеллектуальной собственности в киберпространстве (в том числе современные технические средства) создает необходимый уровень конкурентоспособности для правообладателей.

В первой части цикла рассмотрены вопросы влияния глобализации информационной среды, стратегии информационной безопасности и IP в России и за рубежом с точки зрения юриста.

Во второй части будут рассмотрены проблемы интеллектуальной собственность в структуре кибербезопасности, коммерческая тайны и ее защита от киберугроз.

В третьей части предполагаетсяя рассмотреть новые проблемы – защиты доменных имен различного уровня и товарных знаков, юридические проблемы глобализации интернет–торговли и иных услуг в сети Интернет

***Ключевые слова**: интеллектуальная собственность, защита интеллектуальной собственности от киберугроз, права на результаты интеллектуальной деятельности.*

CYBERSECURITY AND INTELLECTUAL PROPERTY Part 1

***Alexsandr Kartskhiya**, Ph.D. (Jur.Sci), Professor*

The series is devoted to modern mechanism of intellectual property protection in a global information environment. Encouraging of innovation activity and the rightholders protection against cyber threats are the forefront of state (national) strategies for intellectual property. Intellectual property as particularly valuable intangible assets (databases, trade secrets and know–how, computer programs, etc.) are the subject of new threats in cyberspace. Cyber security prevents infringement of intellectual property rights, as well as provides the rightholders with confidentiality of databases, trade secrets and know–how. Intellectual property protection in cyberspace (including modern technical means) creates the required level of competitiveness for the rightholders.

***Keywords**: intellectual property, intellectual property protection against cyberthreats, rights to the results of intellectual activity*

Новые цифровые технологии и глобальные информационные сети, совершившие настоящую революцию в сфере накопления и обмена информацией, потребовали изменения установившихся принципов защиты интеллектуальной собственности, которая создавалась в совершенно иной технологической среде. Глобальная интернет-среда и развитие информационно-коммуникационных технологий требуют адекватного регулирования отношений с использованием интеллектуальной собственности.

Новые реалии современных IT-технологий и Интернета, полученные знания в сфере биотехнологий и фармакологии ставят новые задачи, для выполнения которых традиционный механизм прав интеллектуальной собственности не всегда приспособлен.

Последние годы произошло усиление коммер-

циализации интеллектуальной собственности, повышение значения коммерческой аспекта использования и инвестиционной привлекательности прав интеллектуальной собственности, применение исключительных прав как инструмента в конкурентной борьбе. В совместном докладе о правах интеллектуальной собственности Европейского патентного ведомства и Комиссии по гармонизации на внутреннем рынке, представленном в октябре 2013 года отмечалось, что отрасли европейской экономики, которые непосредственно связаны с интенсивным использованием прав интеллектуальной собственности, составляют 39% общего объема промышленной деятельности (ежегодно около € 4700 млрд.), обеспечивая 26% всех рабочих мест (т.е. 56 млн. рабочих мест). В этих отраслях средняя заработная плата выше на 40%, чем в других отраслях промышленности. К аналогичным результатам в отношении экономики США пришли в проведенном в 2012 году исследовании Ведомства США по патентам и товарным знакам совместно с Агентством экономики и статистики администрации США [1].

Глобализация информационной среды

Современная эпоха, эпоха «интеллектуального капитализма» [2], основана на базовых институтах капитализма (право частной собственности, частный интерес в извлечении прибыли, конкурентные рынки и свободное предпринимательство), где производственные активы и процессы, также как коммерческие сделки и товары, связаны преимущественно с рыночным оборотом нематериальных (интеллектуальных) ценностей, в отличие от товарных рынков материальных активов и продукции. Права интеллектуальной собственности обеспечивают инвесторам своеобразные гарантии инвестиционных рисков и уже рассматриваются как товарная продукция, или даже как своеобразная «валюта».

Вместе с тем, созданная для ускорения инновационного развития посредством защиты интересов правообладателей и стимулирования процесса инноваций система защиты прав интеллектуальной собственности имеет оборотную сторону: стабильное экономическое и технологическое развитие сопровождается снижением конкуренции, высокими затратами по доступу к современным товарным продуктам и технологиям, более высокими ценами на них. Кроме того, оказавшись в центре международного внимания в последние два десятилетия, сфера отношений интеллектуальной собственности породила острые дискуссии и не менее острые вопросы: что такое «интеллектуальная собственность», является ли она финансовым активом или средством национальной и международной конкуренции, либо «моральной» (нематериальной) субстанцией, или же представляет собой средство быстрого разрешения сложных технологических проблем[3] .

Новый облик глобальных экономических отношений, обозначенный как «турбоакпитализм»[4], связан с серьезными рисками «практически непредсказуемого возникновения и разрастания кризисных процессов в любых национальных или отраслевых сегментах глобальной экономики», рисками, непосредственно влияющими на осуществление права собственности и социальных прав огромными массами людей. Эти риски находятся вне сферы полноценного правового регулирования и приводят к эрозии национальных систем правовой регуляции экономических отношений. В итоге глобальные процессы «либерализации» экономического законодательства и его трансформации в направлении «свободы рынка», неуклонно сужавшие права государства по контролю за деятельностью бизнес-структур, привели к целой серии корпоративных крахов в период мирового экономического кризиса [5].

Основная проблема современного экономического развития, по мнению В.Д.Зорькина, «заключается в усилении дисбаланса между ценностями экономической свободы и социальной справедливости в условиях экспансии финансового турбокапитализма и необузданной игры суперкорпораций на глобальных рынках, не может быть решена на уровне национального правового регулирования. Решение этой проблемы требует введения активизма крупнейших транснациональных игроков глобального рынка в рамки глобального правопорядка» [6]. В качестве примера правовых деформаций приводятся факты несоблюдения норм Всемирной торговой организации национальными юрисдикциями за счет искусственного выстраивания разного рода протекционистских барьеров (лицензирование импорта, антидемпинговые расследования и др.).

По оценкам экспертов, транснациональные корпорации отвели существенное место интеллектуальной собственности в стратегиях усиления своих позиций на мировых рынках в целях получения конкурентных преимуществ и монополизации отраслевых товарных рынков и услуг. Применение высокоэффективных стратегий ведения «патентных воин», связанных с переходом от защиты отдельных изделий к агрессивным формам защиты перспективных секторов рынка наукоемкой продукции и формированием мощного портфеля патентов для блокировки научно-техни-

ческих разработок и производства конкурирующих компаний, изменил условия реализации прав интеллектуальной собственности [7].

Стремительное увеличение оборота разнообразной информации (включая коммерческую информацию, информацию о новых технологиях, информацию в составе баз данных), глобализация доступа к ней и появление новых средств ее формирования, распространения и использования актуализировали вопросы сохранности и легального использования массивов информации. Информационная безопасность выходит за рамки потребностей отдельных обладателей и выступает уже в качестве одного из направлений национальных стратегий развития.

Во многих странах в настоящее время уже имеется действующее законодательство, связанное с обеспечением информационной безопасности в информационно-коммуникационных сетях, применяются собственные стратегии информационной безопасности. Однако геополитический скандал с незаконным получением информации Агентством национальной безопасности США вновь привлек внимание государственных структур и общественное мнение к проблемам информационной безопасности и защиты частной жизни, в том числе защиты от кибератак и сохранности персональных данных в сети Интернет.

Достаточно показателен в этом отношении тот факт, что Европейский Союз инициировал пересмотр заключенного с Министерством торговли США соглашения Safe Harbor, предусматривающего возможность передачи персональных данных за пределы ЕС американскими компаниями, ведущими деятельность в Евросоюзе. Это происходит на волне публичного скандала с программой сбора данных PRISM Агентства национальной безопасности США. Европейцы утверждают, что Safe Harbor не соответствует Директиве ЕС о защите данных (EU Data Protection Directive) и может входить в конфликт с новым законодательством ЕС о защите персональных данных.

Последствия киберугроз и незаконных действий в информационно-коммуникационной среде приводят не только к имущественным, но и репутационным потерям для обладателей информации. К примеру, в начале сентября 2013, оператор мобильной связи Vodafone (Германия) обнародовал данные о краже данных более чем у двух миллионов из 36 миллионов своих немецких пользователей, включая имена, адреса, банковские коды и номера счетов. Хотя эти данные не давали прямого доступа к личным банковским счетам, а риск реального ущерба был сведен к минимуму, благодаря оперативному установлению и привлечению к ответственности источника инсайдерской информации, эта ситуация наглядно демонстрирует реальность угроз кибербезопасности [8].

По недавним оценкам органов государственного контроля Великобритании затраты на борьбу с киберпреступностью обходятся стране ежегодно в сумме от 18 до 27 млрд. фунтов стерлингов. Такая ситуация в информационно-коммуникационной среде вынуждает правительства многих стран принимать активные контрмеры по защите государственных и частных интересов в киберпространстве, включая разработку нового законодательства в этой сфере.

Стратегии информационной безопасности и IP в России и за рубежом

Обеспечение информационной безопасности как принципиальный момент соблюдении национальных интересов Российской Федерации, как отмечается в Доктрине информационной безопасности Российской Федерации, подразумевает, в том числе, укрепление механизмов правового регулирования отношений в области охраны интеллектуальной собственности и создание условий для соблюдения установленных федеральным законодательством на доступ к конфиденциальной информации, а также противодействие угрозам информационной безопасности. Важная роль в обеспечении информационной безопасности России отводится определению приоритетных направлений и механизмов реализации государственной политики Российской Федерации в области международной информационной безопасности в целях противодействия основным угроз в этой области. Представляется исключительно актуальным и важным инициатива по разработке концепции стратегии кибербезопасности Российской Федерации, проект которой в настоящее время предложен к обсуждению в Совете Федерации Федерального Собрания РФ.

Российское законодательство устанавливает, что информация, являясь объектом публичных, гражданских или иных правовых отношений, может свободно использоваться и передаваться любым лицом, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения. Закрепив право на доступ к информации и определив общие требования о защите информации и ответственности за правонарушения в сфере информации, информационных технологий и защиты информации, Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите инфор-

мации» определил правила ограничения доступа к информации в сети Интернет, включая распространение информации с нарушением исключительных прав на фильмы, в том числе кинофильмы, телефильмы. Законом также предусмотрен порядок ограничения доступа в информационно-коммуникационных сетях (включая Интернет) к информации, распространяемой с нарушением закона, в которой содержаться призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях.

Проблемы информационной безопасности выходят на первый план и в национальных стратегиях других стран. В частности, в феврале 2013 года Еврокомиссия утвердила Стратегию кибербезопасности в Европе (EU Cyber Security Strategy). Стратегия устанавливает общие минимальные требования к сетевой и информационной безопасности между государствами-членами; определяет согласованную линию на профилактику, обнаружение и смягчения последствий и механизмов киберугроз, а также предусматривает повышение уровня готовности и участия в общей стратегии частного бизнеса. Стратегия направлена на стимулирование спроса на высоко безопасные продукты информационно-коммуникационных технологий и их сертификацию путем создания платформы для выявления и разработки стандартов кибербезопасности, включая сферу «облачных» вычислений. Стратегия опирается на ранее принятые акты в области защиты от киберинцедентов, в частности: Директиву об охране частной жизни в цифровом пространстве (E-Privacy Directive (2002/58/EC), требующей в целях управления рисками в киберсети от поставщиков электронных коммуникаций сообщать о значительных нарушениях безопасности или целостности сети; Директива о критической инфраструктуре (European Critical Infrastructures Directive (2008/114/EC), в целях безопасности обязывающая операторов сетевой инфраструктуры разрабатывать планы обеспечения безопасности, включая анализ рисков и противодействия для прерывания обслуживания или уничтожения сетевой инфраструктуры; Директива о защите данных (Data Protection Directive (95/46/EC), обязывающая обладателей соответствующих баз данных реализовывать соответствующие технические и организационные меры для защиты персональных данных.

Защите данных информационных систем посвящена специальная Директива Европарламента и Еврокомиссии от 12 августа 2013г. (Directive 2013/40/EU on attacks against information systems). В настоящее время новый проект правил о защите персональных данных (General Data Protection Regulation) обсуждается в Европейском парламенте. Она включает в себя новые обязательства, такие как обязательства назначить представителя данных в ЕС и уведомлять об утечке персональных данных. Одновременно со Стратегией предложен проект Директивы о кибербезопасности, на основе которой каждое государство-член Евросоюза должно принять свою собственную стратегию сетевой и информационной безопасности («NIS»).

В 2011 году Федеральным министерством внутренних дел Германии принята общенациональная Стратегия кибербезопасности, направленная на применение эффективных мер и выработке взаимодействия государственных органов, частных предприятий и общественности в сфере кибербезопасности. В стране также обсуждается проект Закона ФРГ об IT безопасности.

С учетом разработанной Национальной стратегии кибербезопасности в Великобритании в настоящее время тестируется новая форма взаимодействия государства и частного бизнеса в сфере информационной безопасности - Партнерство по обмену информационной безопасности (Cybersecurity Information Sharing Partnership («CISP»). CISP призвана установить новую «защищенную среду» обмена и получения информации между государственными органами и частным бизнесом. Современное законодательство Великобритании уже обязывает всех операторов данных применять соответствующие технические и организационные меры против незаконной обработки данных, а в случаях серьезного нарушения информационной безопасности могут налагаться денежные штрафы в размере до £500 000. Кроме того, финансовые компании обязаны исполнять дополнительные нормативные требования, включая организацию систем и средств контроля соблюдения правил финансовых операций.

Особое значение придается кибербезопасности в США. Наряду с уже действующим законодательством указом (executive order) Президента США в феврале 2013 года определена государственная политика по повышению кибербезопасности критической инфраструктуры США. Жизненно важные для США системы и активы (физические или виртуальные), недееспособность или уничтожение которых будет иметь пагубные последствия для национальной и экономической безопасности страны или здоровья и безопасности ее граждан (критическая инфраструктура) и ее защита от киберугроз отнесены эти документом к сфере исключительных национальных интересов США. Национальная политика кибербезопасности США должна обеспечить повышение безопасно-

сти и устойчивости важнейших объектов инфраструктуры нации, поддержание киберусловий, способствующих эффективности, инновациям и экономическому процветанию, обеспечивать конфиденциальность в бизнесе и неприкосновенность частной жизни и гражданских свобод. Поставленные задачи планируется достичь в рамках партнерства с владельцами и операторами критической инфраструктуры, мерами улучшения обмена информацией по кибербезопасности и разработкой и внедрением стандартов о рисках.

Выработка многими странами стратегий информационной безопасности тесно связана с национальными стратегиями развития интеллектуальной собственности. Так, в США в 2013 году принят очередной стратегический план стимулирования и защиты интеллектуальной собственности в 21 веке, который определяет ориентиры в борьбе правительства с контрафактной продукцией и интеллектуальным пиратством, пресечением нарушений прав IP в интернете; предусматривает повышение открытости правоприменительной политики и международных переговоров, а также улучшение взаимодействия государственных органов и всех заинтересованных сторон в области интеллектуальной собственности; акцентирует внимание авторов на применение доктрины добросовестного использования (fair use); предусматривает повышении эффективности взаимодействия федеральных, органов штатов и местных правоохранительных органов (включая выявление новых технологий защиты IP при пограничном и иных формах контроля); усиление защиты от угроз нарушения IP на иностранных интернет-сайтах и защиты доменов первого уровня в сочетании с поддержкой национальных предприятий на внешних рынках; предусматривает систематизацию действующего законодательства по IP.

В материалах к стратегическому плану отмечается, что информационная безопасность является необходимым условием инноваций. Инновационный процесс, посредством которого новые идеи генерируются и успешно внедряются на рынке, как предусматривает национальная стратегия, служит основной движущей силой экономического роста и национальной конкурентоспособности США. Подобно тому, как использование торговых марок американскими компаниями позволяет отличить их товары и услуги от конкурентов, предоставление дополнительной поддержки инновациям позволяет национальным компаниям захватить долю рынка, что способствует росту американской экономики. Поощрение и защита прав интеллектуальной собственности является жизненно важным для продвижения инноваций и составляет важный элемент свободного предпринимательства и рыночной системы. Патенты, товарные знаки и авторские права являются основным средством используется для установления прав собственности на изобретения и творческие идеи в их различных формах, обеспечивающих правовую основу для создания ощутимых выгод от инноваций для компаний, работников и потребителей. Без этих правовых рамок создатели интеллектуальной собственности, как правило, не могут воспользоваться экономическими плодами своей собственной работы, тем самым подрывая стимулы к осуществлению необходимых инвестиций в развитие IP. Более того, без защиты IP, новатор (изобретатель), вложивший время и деньги в разработку нового продукта или услуги (невозвратные издержки) всегда будет в невыгодном положении по сравнению с компанией, просто копирующей инновационный продукт и выводящей его на рынок, без необходимости окупить такие невозвратные издержки или выплачивать более высокую заработную плату разработчикам, обладающим творческими талантами и навыками. В результате преимущества от американских инноваций будут иметь тенденцию утекать за пределы США [9].

В стратегиях развития IP активизируется и Китай. Национальная стратегия интеллектуальной собственности, принятая в КНР в 2013 году на пятилетний период, определила несколько главных целей: (1) поощрение создания интеллектуальной собственности, т.е. повышение качества прав интеллектуальной собственности и инновационной эффективности, улучшение оценки патентов, товарных знаков, авторских прав, новых сортов растений и др., совершенствование системы оценки эффективности IP, поощрение создателей IP и переход от количества к качеству и значению IP для модернизации; (2) усиление влияния IP в ключевых отраслях экономики через государственное планирование использования ИС в стратегических новых отраслях промышленности с применением преференциальной экспертизы патентных заявок на изобретения в этих отраслях и новейших технологиях (в т.ч. энергосбережение и охрана окружающей среды, информационных технологий нового поколения, биологии, производства высококачественное оборудование, новой энергии, новых материалов, а также технологии, поддерживающие зеленый развития, такие как низкоуглеродистых технологий и ресурсосберегающих технологий); (3) содействие внедрению IP посредством укрепления ключевой роли в использовании IP предприятиями и улучшение коммерциализации нового поколения прав ИС в коммуникационных

технологиях, трансфера прав на технологии военного и гражданского назначения, улучшения менеджмента ИС, применения финансовых инструментов использования ИС (залог и кредит прав ИС), прав на лицензии, прав в уставных капиталах и других активов; (4) усиление защиты IP путем совершенствования законодательства и оценки эффективности защиты ИС, повышение эффективности судебной защиты прав интеллектуальной собственности и потенциала административного правоприменения, включая международные споры; (5) повышение эффективности управления ИС, включая информационные, сервисные и юридические и патентные услуги по продвижению патентов, товарных знаков, авторских прав, правовой оценке ИС; (6) развитие культуры обращения ИС.

Литература:

1. Intellectual Property Rights intensive industries: contribution to economic performance and employment in Europe. Report of the European Patent Office and the Office for Harmonization in the Internal Market, September, 30th, 2013. http://europa.eu/rapid/press-release_IP-13-889_en.htm?locale=en.
2. Подробнее см.: Ove Granstrand. The Economics and Management of Intellectual Property: Towards Intellectual Capitalism. Edward Elgar, Cheltenham, UK, Northhampton, MA, USA, 2000. C.3-4 и др. ; Economics, Law and Intellectual Property (edited by Ove Granstrand). Kluwer Academic Publishers Boston. 2003.
3. Matthew Littleton. The TRIPS Agreement and Transfer of Climate-Change-Related Technologies to Developing Countries. United Nations Department of Economic and Social Affairs. Working Paper No. 71. ST/ESA/2008/DWP/71. C.1-2
4. Edward Luttwak. Turbocapitalism: Winners and Losers in the Global Economy. New York, 1999.
5. В.Зорькин. Трансформация отношений собственности: глобальные тенденции и российский опыт. Российская газета, 31.05.2012. www.rg.ru.
6. В.Зорькин., там же.
7. Мухопад В.И. Коммерциализация интеллектуальной собственности. Москва. Магистр. Инфра-М . 2010. с. 218-219.
8. Friedrich Geiger and Archibald Preuschat. Hacker Hits Vodafone in Germany. Wall Street Journal (Sept. 12, 2013). Источник: http://online.wsj.com/.
9. Joint Strategic Plan on Intellectual Property Enforcement 2013. www.uspto.gov/web/offices/com/strat21/index.htm.
10. Dawn A.Rudenko. Trade secrets in the United States. Intellectual Asset Management July/August 2010. www.iam-magazine.com
11. Подробнее см.: Карцхия А.А. Права промышленной собственности в российском праве: навстречу вызовам современности. Lambert Academic Publishing. Germany, 2013.

References:

1. Intellectual Property Rights intensive industries: contribution to economic performance and employment in Europe. Report of the European Patent Office and the Office for Harmonization in the Internal Market, September, 30th, 2013. http://europa.eu/rapid/press-release_IP-13-889_en.htm?locale=en.
2. Ove Granstrand. The Economics and Management of Intellectual Property: Towards Intellectual Capitalism. Edward Elgar, Cheltenham, UK, Northhampton, MA, USA, 2000. C.3-4 и др. ; Economics, Law and Intellectual Property (edited by Ove Granstrand). Kluwer Academic Publishers Boston. 2003.
3. Matthew Littleton. The TRIPS Agreement and Transfer of Climate-Change-Related Technologies to Developing Countries. United Nations Department of Economic and Social Affairs. Working Paper No.71. ST/ESA/2008/DWP/71.p.1-2
4. Edward Luttwak. Turbocapitalism: Winners and Losers in the Global Economy. New York, 1999.
5. V.Zorkin. Transformation of property relations: Global Trends and Russian experience. Rossiyskaya Gazeta, 31.05.2012. www.rg.ru.
6. V.Zorkin. Transformation of property relations: Global Trends and Russian experience. Rossiyskaya Gazeta, 31.05.2012. (www.rg.ru).
7. Muhopad V.I. Commercialization of intellectual property. Moscow. Master. Infra-M. 2010. p.218-219.
8. Friedrich Geiger and Archibald Preuschat. Hacker Hits Vodafone in Germany. Wall Street Journal (Sept. 12, 2013). Источник: http://online.wsj.com/.
9. Joint Strategic Plan on Intellectual Property Enforcement 2013. www.uspto.gov/web/offices/com/strat21/index.htm.
10. Dawn A.Rudenko. Trade secrets in the United States. Intellectual Asset Management July/August 2010. www.iam-magazine.com
11. Kartskhiya A.A. Industrial property rights in the Russian law: towards challenges. Lambert Academic Publishing. Germany, 2013.

МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ОСНОВНЫЕ КОНЦЕПЦИИ

***Дорофеев Александр Владимирович**, CISSP, CISA*
***Марков Алексей Сергеевич**, кандидат технических наук, старший научный сотрудник, CISSP*

Публикация открывает серию статей, посвященных подготовке к сертификации специалистов по информационной безопасности. Рассмотрены основные понятия информационной безопасности: свойства, угрозы, уязвимости, риски, меры безопасности. Приведены классификация и примеры угроз информационной безопасности. Дано описание системы менеджмента информационной безопасности. Рассмотрены меры безопасности в контексте ISO 27001. Представлен порядок использования политик, стандартов, руководств.

***Ключевые слова**: сертификация специалистов, информационная безопасность, CISSP, менеджмент информационной безопасности, СМИБ.*

INFORMATION SECURITY MANAGEMENT: BASIC CONCEPTS

***Alexander Dorofeev**, CISSP*
***Alexey Markov**, Ph.D., Associate Professor, CISSP*

Publication opens a series of articles devoted to preparation for certification for information system security professionals. The basic concepts of information security such as properties, threats, vulnerabilities, risks, controls are reviewed. The classification and examples of information security threats are given. The information security management system is described. The measures of security in the context of ISO 27001 are discussed. The order of using of policies, standards and guidelines is shown.

***Keywords**: experts certification, information security, security controls, CISSP, information security management, ISMS, PDCA–model.*

Основные понятия информационной безопасности

Залогом успешной сдачи экзамена CISSP является хорошее понимание концепции управления информационной безопасностью в организации [1].

Прежде всего, следует разобраться, что стоит за такими понятиями как информационная безопасность, актив, угроза, уязвимость, контроль и риск.

Под *информационной безопасностью* (ИБ) обычно понимают состояние (свойство) защищенности ресурсов информационной системы в условиях наличия угроз в информационной сфере. Защита информации - это процесс, направленный на обеспечение информационной безопасности.

Определяющими факторами информационной безопасности являются угроза (threat) и риск (risk). *Угрозой* называют потенциальную причину (событие, нарушение, инцидент), снижающую уровень информационной безопасности системы, т.е. потенциально способную привести к негативным последствиям (impact) и ущербу (loss) системы или организации.

Риск представляет собой возможный ущерб, т.е. комбинацию (как правило, произведение) вероятности реализации угрозы и ущерба от нее.

Отметим, что угроза и риск определяются не вообще, а относительно конкретного защищаемого ресурса. В терминологии менеджмента бизнес-процессов вместо ресурса используется синонимическое понятие - *актив* (asset), под определение которого подпадает все, что имеет ценность для организации. В информационной сфере примерами активов являются: информация, программное обеспечение, аппаратное обеспечение, информационная система (сложный актив, включающий предыдущие), человек, имидж организации. В итоге, активами представляются все те объекты, которые подлежат защите путем выстраивания процессов информационной безопасности.

Таблица 1.

Примеры угроз информационной безопасности

Направления обеспечения безопасности	Техногенные		Природные
	Преднамеренные	Случайные	
Контроль физического доступа	Бомбардировка	Сон вахтерши	Торнадо
Сохранность оборудования	Вандализм	Запыление	Шаровые молнии
Управление коммуникациями	Прослушивание сети	Флуктуации в сети	Магнитные бури
Защита информационных хранилищ	Взлом парольной системы	Сбой криптосредств	Грибки
Управление непрерывностью деятельности	Последствие DOS-атаки	Последствия тестов на проникновения	Карстовые процессы
Соответствие законодательству	Компьютерное пиратство	Тиражирование персональных данных	Природные пожары

Угрозы классифицируют по ряду критериев:

- по причине возникновения (природные или техногенные, в том числе преднамеренные или случайные);
- по расположению источника (внешние или внутренние);
- по компрометируемой подсистеме или сегменту (сетевые, криптографические и др.);
- по этапу формирования в жизненном цикле системы (реализационные и эксплуатационные);
- по результирующему действию (нарушают целостность, конфиденциальность, доступность).

Примеры угроз представлены в табл.1.

Довольно подробные каталоги угроз подготовлены немецким федеральным агентством по информационной безопасности (BSI) [2].

Одной из основных угроз ИБ компьютерных систем является возможность реализации уязвимости (vulnerability) в ресурсах системы. Под *уязвимостью* понимают реализационный дефект («слабость»), снижающий уровень защищенности ресурсов от тех или иных угроз. Отметим, наличие уязвимости становится угрозой, если ее можно реализовать так, что это приведет к недопустимому ущербу организации. Например, наличие сетевых уязвимостей в программном обеспечении изолированного компьютера не является угрозой.

Умышленная реализация уязвимостей в компьютерных системах, приводящая к ущербу организации, называется *атакой* на ресурсы.

Защищенность системы достигается обеспечением совокупности свойств ИБ ресурсов и инфраструктуры, основными из которых являются:

- конфиденциальность (confidentiality),
- целостность (integrity),
- доступность (availability).

В зарубежных учебниках свойства конфиденциальности, целостности, доступности часто графически представляются в виде ссылки на треугольник CIA.

Конфиденциальность - свойство системы, определяющее ее защищенность от несанкционированного раскрытия информации.

Целостность - свойство, определяющее защищенность от несанкционированного изменения. Разделяют логическую и физическую целостность. Физическая целостность подразумевает неизменность физического состояния данных на машинном носителе. Логическая целостность отражает корректность выполнения процессов (транзакций), полноту и непротиворечивость информации, например, в СУБД, файловых системах, электронных архивах, хранилищах данных, системах управления документооборотом и т.д.

Доступность - характеристика, определяющая возможность за приемлемое время получить требуемую информационную услугу авторизованному пользователю. С доступностью часто связывают такую характеристику системы как готовность - способность к выполнению заявленных функций в установленных технических условиях. Атаки, имеющие целью нарушить степень доступности получили название атак на отказ в обслуживании (DOS-атаки).

Кроме названных, часто в качестве наиболее важных свойств ИБ системы, для выражения значимости, упоминают аутентичность, подотчетность, неотказуемость, надежность и др.

Повышение и обеспечение заданных уровней конфиденциальности, целостности и доступности ресурсов осуществляется путем применения мер (механизмов) безопасности, которые на профессиональном жаргоне часто называются контролями (от. англ. слова controls - инструменты/средства управления). Очень важно не путать этот жаргонизм с привычным словом «контроль», имеющим другое значение: наблюдение за поведением управляемой системы с целью обеспечения ее оптимального функционирования.

Контроли могут иметь технический (technical), организационный (administrative) и физический (physical) характер. Под понятие «технические контроли» подпадают программные и программно-аппаратные средства защиты, такие как антивирусы, межсетевые экраны, системы обнаружения вторжений, средства шифрования данных и т. п. В качестве организационных контролей выступают правила, обязательные для исполнения сотрудниками. Например, наличие согласования заявки на предоставление доступа к системе у ее владельца (как правило, руководителя бизнес-подразделения, отвечающего за процессы, которые поддерживаются данной системой). Хорошими примерами физических контролей являются двери, решетки, заборы, ограничивающие физический доступ к нашим активам.

Контроли могут придерживаться различных целей, например, быть превентивными (preventive), детективными (detective), корректирующими (corrective), восстанавливающими (recovery) и другими. Более подробно контроли мы рассмотрим в следующей публикации, касающейся вопросов обеспечения безопасного доступа.

Применение различных видов и типов контролей тесно связано с концепцией эшелонированной обороны (defense in depth, multilevel security), представляющей идеологию проектирования систем защиты с несколькими уровнями мер (механизмов) безопасности, позволяющими обеспечить эффективную защиту даже в случае «пробивания» обороны на одном уровне.

Управление информационной безопасностью

Скоординированные действия, выполняемые с целью повышения и поддержания на требуемом уровне ИБ организации, называются управлением (менеджментом[1]) информационной безопасностью.

Система менеджмента информационной безопасности (СМИБ, ISMS) организации основывается на подходе бизнес-риска и предназначена для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения ИБ. В рамках СМИБ рассматривают структуру системы, политики, действия по планированию, обязанности, практики, процедуры, процессы и ресурсы организации.

Концепция СМИБ определяется в международном стандарте ISO/IEC 27001. В предыдущих редакциях стандарта требования к СМИБ были довольно явно сопоставлены с элементами модели Шухарта-Деминга «Планирование (Plan) - Реализация (Do) - Проверка (Check) – Совершенствование (Act)» (PDCA)[2]. По сути, цикл PDCA отражает руководство здравым смыслом при внедрении какого-либо процесса: прежде чем что-нибудь сделать мы планируем, затем это выполняем, после чего контролируем, что то, что сделали, соответствует тому, что хотели, а выявленные недостатки и отклонения устраняем. Из новой версии стандарта, вышедшей в 2013-м году, данная модель изъята, чтобы не ограничивать организации в выборе концепций управления процессами.

Рассмотрим, что требует от нас стандарт ISO 27001:2013 для построения системы управления информационной безопасностью[3].

В первую очередь необходимо определить контекст, в котором работает организация и четко понимать потребности и ожидания всех сторон, заинтересованных в функционирующей системе управления информационной безопасностью. К заинтересованным сторонам можно отнести владельцев бизнеса, клиентов, партнеров, регулирующие органы, сотрудников и др.

Важно, что стандарт позволяет задать границы системы управления информационной безопасностью, то есть дает возможность внедрить СМИБ «вокруг» определенных критичных бизнес-процессов, а затем уже при необходимости расширять область действия СМИБ на другие процессы.

Внедрение СМИБ невозможно без реальной поддержки со стороны топ-менеджмента организации, определяющего четкую политику информационной безопасности, включающую цели и обязательства выполнять все применимые требования (законодательства, партнеров, клиентов

1 Термин управление в данном разделе тождественен понятию менеджмента, используемому в системах качества по ISO 9000.

2 ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems – Requirements

3 ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements

и т.п.). Руководство компании должно определить роли и обязанности в области ИБ и дать соответствующие полномочия сотрудникам, занимающимся внедрением СМИБ.

Введение в оценку рисков

На этапе планирования внедрения СМИБ в первую очередь формализуется процесс оценки рисков (risk assessment) информационной безопасности.

Методология оценки рисков в первую очередь должна определять критерии оценки и условия принятия рисков (рис. 1).

Методология должна быть разработана таким образом, чтобы его можно было повторить и получить сравнимые результаты.

В соответствии с ISO 27001:2013 в ходе процесса анализа рисков необходимо в первую очередь идентифицировать риски ИБ (risk identification) и определить владельцев рисков. Затем провести анализ рисков (risk analysis), в ходе которого определить вероятность риска, размер ущерба и соответственно определить уровень рисков. После чего провести оценивание риска (risk evaluation) относительно установленных критериев принятия рисков и задать приоритеты для обработки рисков (risk treatment).

Необходимо отметить, что отсутствует общепризнанное разделение процессов идентификации, анализа и оценивания рисков, поэтому в ходе экзамена кандидату необходимо в первую очередь обращать внимание на контекст, в котором используется тот или иной термин.

Очень важно понимать, что подходы к оценке рисков предусматривают также оценку уязвимостей (vulnerability assessment) и существующих контролей (control evaluation) для минимизации угроз.

Конкретные подходы к проведению оценки рисков информационной безопасности более подробно мы рассмотрим в следующем номере журнала.

В отношении рисков, значения которых не соответствуют критериям принятия, важно определиться с решением относительно их обработки. Приступая к выбору варианта «реагирования» на риск менеджмент компании, как правило, рассматривают различные аспекты, среди которых: соотношение стоимости затрат на внедрение предлагаемого контроля к возможному ущербу от реализации угрозы, соответствие контрмеры культуре компании, законодательству и т.п.

Помимо уже упомянутого принятия риска (risk accepting), заключающегося в том, что организация соглашается с возможной реализацией угрозы и принимает последствия, вариантами обработки рисков являются:

- *минимизация риска* (risk mitigation, reducing risk) посредством внедрения контролей;

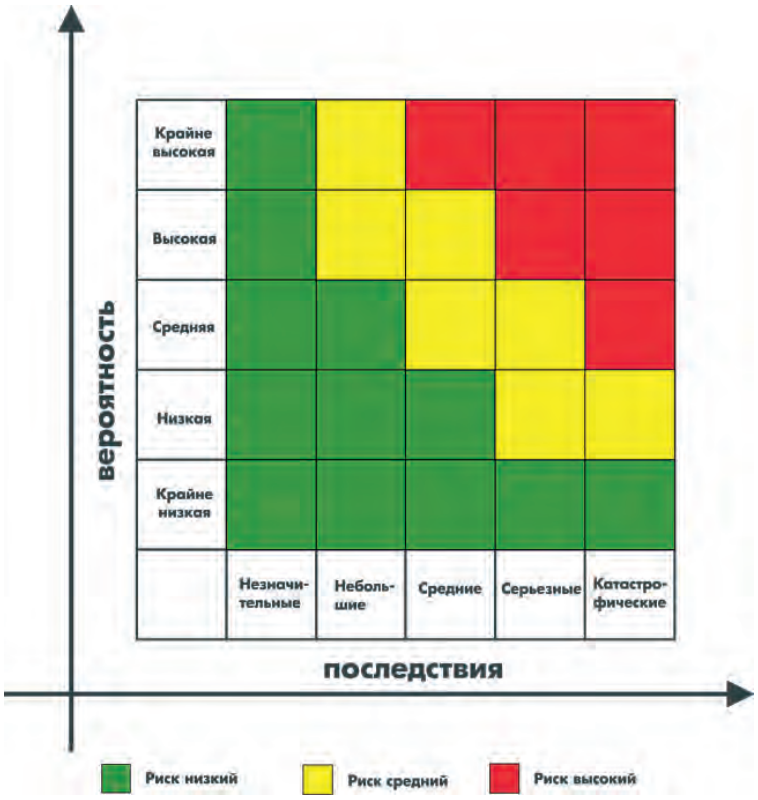


Рис. 1. *Матрица оценки рисков*

- *передача риска* (assigning risk, transferring risk), которая может заключаться как в его страховании, так и передаче подрядчику (в совокупности с процессами, передающимися на аутсорсинг),

- *избежание риска* (rejecting risk, avoiding risk), которое может заключаться в изменении процесса таким образом, что риск становится неактуальным.

Необходимо отметить, что в результате обработки риска остается так называемый *остаточный риск* (residual risk), который принимается менеджментом компании (владельцами рисков).

Внедрение контролей безопасности

На практике для большинства выявленных рисков принимается решение об их минимизации путем внедрения контролей. Стандарт ISO 27001:2013 содержит Приложение А, в котором приведены 114 контролей, распределенных по следующим 14-ти доменам:

A.5: Политики информационной безопасности
A.6: Организационные аспекты информационной безопасности
A.7: Вопросы безопасности, связанные с персоналом
A.8: Управление активами
A.9: Управление доступом
A.10: Криптография
A.11: Физическая безопасность и защита от угроз окружающей среды
A.12: Безопасность операций
A.13: Безопасность коммуникаций
A.14: Приемка, разработка и поддержка систем
A.15: Отношения с поставщиками услуг
A.16: Управление инцидентами информационной безопасности
A.17: Аспекты информационной безопасности в обеспечении непрерывности бизнеса
A.18: Соответствие требованиям

В случае внедрения СМИБ в соответствии с ISO 27001:2013 компания руководствуется Приложением А для выбора контролей, при этом, исключение контроля должно быть обоснованным, как и включение контроля, отсутствующего в стандарте.

Интересно, что контроли неравноценны. В целом контроли из Приложения А относятся к организационным мерам, например, встречаются контроли «Политика контроля доступа» (A.9.1.1), «Правила использования активов» (A.8.1.3), предусматривающие определение правил информационной безопасности в форме политик. Что же касается технически мер, то они формулируются исключительно общими словами, например, «Безопасность сетевых сервисов» (A.13.1.2).

После решения задачи выбора контролей, которые должны быть внедрены, чтобы снизить риски до приемлемого уровня, определяется: что конкретно должно быть сделано, какие ресурсы для этого необходимо задействовать, кто будет ответственным, и как будет проводиться оценка выполнения.

На данном этапе разрабатываются политики, процедуры, инструкции (подробнее о них ниже), внедряются технические средства защиты информации, проводится обучение специалистов, задействованных в процессах обеспечения ИБ, внедряется программа повышения осведомленности сотрудников компании в вопросах безопасности (security awareness program).

Контроль процессов

В результате внедрения контролей должны быть получены работающие процессы СМИБ, которые выполняются, измеряются и контролируются. Необходимо отметить следующие три важных составляющих контроля работы СМИБ:

- операционный контроль;
- внутренний аудит;
- анализ со стороны руководства.

Операционный контроль подразумевает собой текущий контроль со стороны непосредственных руководителей. Например, принятая процедура предусматривает выполнение периодического сканирования на наличие уязвимостей сетевых сервисов, и отвечает за эту функцию конкретный специалист отдела ИБ. Соответственно руководитель отдела следит за тем, чтобы задача выполнялась подчиненным, и он вовремя получал отчет с результатами сканирования.

Внутренний аудит заключается в периодической проверке эффективности контролей. Например, аудитор просит системного администратора предоставить перечень учетных записей, созданных в течение прошлого года, выбирает несколько и просит показать заявки, по которым он может убедиться, что доступ был согласован руководителями сотрудников и владельцами системы.

Анализ со стороны руководства подразумевает, что менеджмент интересуется тем, как работает СМИБ и, в частности, анализирует результаты проведенных аудитов (как внутренних, так и внешних), информацию о количестве произошедших инцидентов ИБ, в каком объеме требуются ресурсы для работы системы и т.п.

Результатом подобных контрольных мероприятий будет информация о недостатках и необходимых улучшениях системы. Концепция постоянного улучшения (continual improvement) СМИБ является одним из основных принципов стандарта.

Политики, процедуры, стандарты

Очевидно, что «спонтанно бессознательная» организация управления неприменима для сложных систем, поэтому СМИБ основывается на наборе внутренних нормативных документов: политиках, процедурах, корпоративных стандартах, руководствах и инструкциях.

Политика (policy) представляет собой документ, в котором определяются цели, задачи и пути их достижения, принципы.

Следует помнить, что часто под политикой информационной безопасности (information security policy) понимается высокоуровневый документ, предназначенный для обеспечения управления ИБ в соответствии с требованиями бизнеса, партнеров, клиентов, законодательной базы.

Высокоуровневая политика безопасности, как правило, представляет собой достаточно статичный документ. Такой документ обычно содержит:

- общую информацию об обеспечении ИБ в организации (в которой мотивировано определена необходимость обеспечения и поддержки режима безопасности);
- заявление о поддержке (commitment) мероприятий по обеспечению ИБ на всех управленческих уровнях;
- основные положения по определению целей ИБ;
- распределение ролей и определение общей ответственности за реализацию мероприятий по обеспечению ИБ (в том числе по разработке и корректировке политик);
- ссылки на низкоуровневые документы, конкретно определяющие порядок реализации тех или иных аспектов, связанных с обеспечением ИБ.

Документированная политика ИБ должна быть утверждена руководством и доведена до сведения всех сотрудников организации и внешних сторон, к которым она относится.

Кроме высокоуровневой политики выделяют низкоуровневые политики (частные политики, подполитики), как правило, отражающие требования в определенной области (домене). В качестве примеров политик низкого уровня можно привести политику управления доступом, политику управления паролями, политику резервного копирования и т.п.

Точный состав частных политик зависит от особенностей организации: ее размера, структуры, корпоративной культуры и т.п.

Стандарт (standard) определяет обязательное требование, практику применения какого-либо решения. Примером корпоративного стандарта является, например, стандарт на конфигурацию серверов под управлением Linux. Такие стандарты можно разрабатывать на основе чеклистов, доступных на сайте Center of Internet Security [3].

Руководства (guidelines) отличаются от стандартов в первую очередь тем, что носят рекомендательный характер. Руководства, в частности, могут определять, как именно следует реализовывать то или иное требование на практике с учётом локальной специфики. Так, например, специалист по информационной безопасности может разработать руководство, описывающее различные алгоритмы генерации надежных паролей, чтобы облегчить задачу выбора пароля пользователю.

Процедура (procedure) представляют собой документ, определяющий последовательность действий по выполнению какой-либо задачи в соответствии с требованиями политик и стандартов. Из процедуры должно быть ясно, кто, что и когда делает. Хорошим примером процедуры является процедура регистрации пользователей в системе, описывающая этапы согласования заявки на доступ.

Необходимо отметить, что, в основном, упомянутые документы ориентированы на специалистов отделов ИТ/ИБ, руководителей подразделений. Для неподготовленных сотрудников содержание данных документов может быть непонятным. В таких случаях разрабатывается документ «Свод правил для сотрудников», в котором доступным языком без использования технических терминов формулируются требования, которые должны выполнять сотрудники. Также функционал по обеспечению ИБ должен быть закреплен в положениях об отделах и должностных инструкциях.

К отдельным видам документов стоит отнести так называемые записи (records). Записи представляют собой те документы, которые создаются при выполнения процедуры, например, заявка на предоставление доступа к системе, журнал системы контроля доступа с информацией о том, кто входил в серверное помещение и т.п.

При внедрении СМИБ названия документов и их состав определяют, исходя из устоявшейся практики в компании. Политика может называться положением, процесс - порядком и т.п.

На рисунке 2 представлен возможный вариант структуры документации СМИБ.

Заключение

В настоящей статье мы рассмотрели ключевые понятия менеджмента информационной безопас-

Рис. 2. *Возможная структура документации СМИБ*

ности, разобравшись в которых можно серьезно повысить свои шансы на успешную сдачу экзамена CISSP [4-7].

Приоритетность изучения данной учебной информации обусловлена тем, что в пройденном разделе представлены основные понятия информационной безопасности, на которые мы будем ссылаться при публикации очередного учебного материала.

В следующем номере мы детально рассмотрим подходы к оценке рисков информационной безопасности.

Литература

1. Дорофеев А.В. Статус CISSP: как получить и не потерять? // Вопросы кибербезопасности. 2013. № 1(1). С.65-68
2. IT-Grundschutz Catalogues. Bundesamt für Sicherheit in der Informationstechnik, 2005. URL: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html (Дата обращения: 1.03.2014).
3. CIS Security Benchmarks. Center for Internet Security, 2014. URL: https://benchmarks.cisecurity.org/downloads/ (Дата обращения: 1.03.2014).
4. Steven Hernandez. Official (ISC)2 Guide to the CISSP CBK, Third Edition. - ISC2 Press, 2012. 968 p.
5. James M. Stewart, Mike Chapple, Darril Gibson. CISSP: Certified Information Systems Security Professional Study Guide, 6th Edition. - Sybex, 2012. 936 p.
6. Shon Harris, CISSP All-in-One Exam Guide, 6th Edition - McGrawHill, 2012. 1216 p.
7. Eric Conrad, Seth Misenar, Joshua Feldman. CISSP Study Guide, Second Edition - Syngress, 2012. 600 p.

References

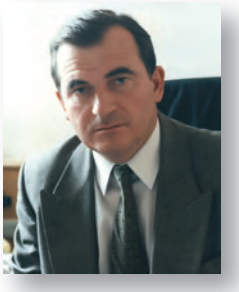
1. Dorofeyev A.V. Status CISSP: kak poluchit i ne poteryat? Voprosy kiberbezopasnosti, 2013, No 1(1), pp. 65-68
2. IT-Grundschutz Catalogues, Bundesamt für Sicherheit in der Informationstechnik, 2005, URL: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html
3. CIS Security Benchmarks, Center for Internet Security, 2014, URL: https://benchmarks.cisecurity.org/downloads/
4. Steven Hernandez. Official (ISC)2 Guide to the CISSP CBK, Third Edition. - ISC2 Press, 2012, 968 p.
5. James M. Stewart, Mike Chapple, Darril Gibson. CISSP: Certified Information Systems Security Professional Study Guide, 6th Edition. - Sybex, 2012, 936 p.
6. Shon Harris, CISSP All-in-One Exam Guide, 6th Edition - McGrawHill, 2012, 1216 p.
7. Eric Conrad, Seth Misenar, Joshua Feldman. CISSP Study Guide, Second Edition - Syngress, 2012, 600 p.

Сведения об авторах Information about the authors

Безкоровайный Михаил Михайлович, кандидат технических наук, доцент, начальник управления Международного центра по информатике и электронике (ИнтерЭВМ), г. Москва

Mikhail Bezkorovainy, Ph.D., Associate Professor, Head of Department of International Center for Informatics and Electronics, Moscow

E-mail: mbezkor@inevm.ru



Бородакий Юрий Владимирович, академик РАН, Заслуженный деятель науки Российской Федерации, доктор технических наук,профессор, Генеральный директор ОАО «Концерн «Системпром», г. Москва

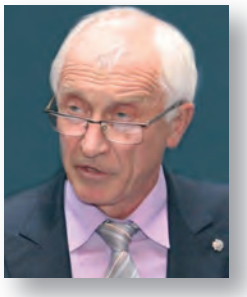
Yuri Borodakiy, Member of the RAS, Honored Scientist of the Russian Federation, Doctor of Technical Sciences, Professor, CEO of Concern Systemprom

E-mail: info@systemprom.ru

Бутусов Игорь Викторович, начальник отдела ОАО «Концерн «Системпром», г. Москва

Igor Butusov., Head of Department of the Concern Systemprom, Moscow

E-mail: skm@vivos.ru



Добродеев Александр Юрьевич, кандидат технических наук, старший научный сотрудник, заместитель генерального директора по информационной безопасности ОАО «Концерн «Системпром», г. Москва

Alexander Dobrodeyev, Ph.D., Associate Professor, Deputy Director General for Information Security of Concern Systemprom

E-mail: skm@vivos.ru

Дорофеев Александр Владимирович, CISSP, CISM, CISA, директор Учебного центра «Эшелон», г. Москва

Alexander Dorofeev, CISSP, CISM, CISA, CEO of the EC Echelon

E-mail: mail@uc-echelon.ru

Жидков Игорь Васильевич, кандидат технических наук, доцент, заместитель начальника управления 3 ЦНИИ Министерства обороны Российской Федерации, г. Москва

Igor Zhidkov, Ph.D., Associate Professor, Deputy Head of Department of the 3 CRI of Russian Ministry of Defense, Moscow

Кадушкин Иван Викторович, начальник отдела 3 ЦНИИ Министерства обороны Российской Федерации, г. Москва

Ivan Kadushkin, Head of Department of 3 CRI of Russian Ministry of Defense, Moscow

E-mail: ivanvk79@mail.ru

Калашников Андрей Олегович, доктор технических наук
ведущий научный сотрудник Института проблем управления
им. В.А. Трапезникова РАН, г. Москва

Andrey KALASHNIKOV, Sc. Dr., Leading Scientist of the Institute of Control Sciences of the RAS named after V. A. Trapeznikov, Moscow
E-mail: tigrilla1962@mail.ru

Карцхия Александр Амиранович, кандидат юридических наук, профессор Российского государственного университета нефти и газа им. И.М.Губкина, г. Москва

Alexandr A.Kartskhia, Ph.D in Law, Professor of the Russian State University of Oil and Gas named after I.M.Gubkin, Moscow

Макаренко Сергей Иванович, кандидат технических наук, доцент кафедры Военно-космической академии имени А.Ф.Можайского, г. Санкт-Петербург

Sergey Makarenko, Ph.D., Associate Professor of the Mozhaisky Military Space Academy, Saint Petersburg
E-mail: mak-serg@yandex.ru

Малмквист Кен, главный консультант по безопасности программных систем компании AsTech Consulting, член Открытого Проекта по Безопасности Веб-приложений (OWASP), г. Сан-Франциско, США

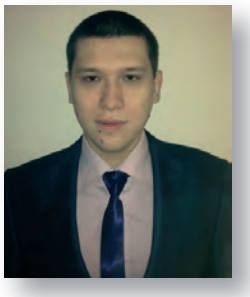
Kenneth Malmquist, Senior Application Security Consultant at AsTech Consulting, Member of the Open Web Application Security Project (OWASP), San Francisco, USA
E-mail: ken.malmquist@astechconsulting.com

Марков Алексей Сергеевич, кандидат технических наук, старший научный сотрудник, CISSP, SBCI, генеральный директор ЗАО «НПО «Эшелон», г. Москва

Alexey Markov, Ph.D., Associate Professor, CISSP, SBCI, CEO of the NPO Echelon, Moscow
E-mail: am@npo-echelon.com

Рибер, Грегори основатель и генеральный директор компании AsTech Consulting, член Института Компьютерной Безопасности (CSI), Ассоциации по Аудиту и Контролю Информационных Систем (ISACA), Открытого Проекта по Безопасности Веб-приложений (OWASP), г. Сан-Франциско, США

Reber, Gregory , Founder and CEO of AsTech Consulting, Member of Computer Security Institute (CSI), Information Systems Audit and Control Association (ISACA), the Open Web Application Security Project (OWASP), San Francisco, USA
E-mail: greg.reber@astechconsulting.com



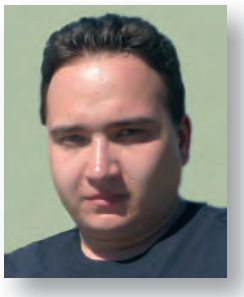
Сердечный Алексей Леонидович, старший научный сотрудник Государственного научно-исследовательского испытательного института проблем технической защиты информации Федеральной службы по техническому и экспортному контролю, г. Воронеж

Alexey Serdechnyy, Senior Scientist of the National Scientific and Research Institute of Problems in Technical Information Defense of the Federal Service for Technical and Export Control, Voronezh
E-mail: alex-voronezh@mail.ru

Сведения об авторах

Татузов Александр Леонидович, доктор технических наук, доцент, ведущий научный сотрудник Международного центра по информатике и электронике (ИнтерЭВМ), г. Москва

Alexander L. Tatuzov, Sc. Dr., Associate Professor, Leading Scientist of the International Center for Informatics and Electronics, Moscow
E-mail: tatuzov@yandex.ru

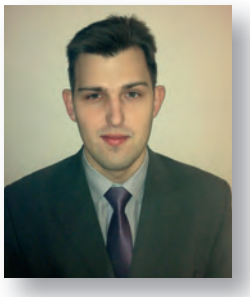


Цирлов Валентин Леонидович, кандидат технических наук, CISSP, CISM, AMBCI, исполнительный директор ЗАО «НПО «Эшелон» , г. Москва

Valentin Tsirlov, Ph.D., CISSP, CISM, AMBCI, Executive Director of NPO Echelon, Moscow
E-mail: vz@npo-echelon.com

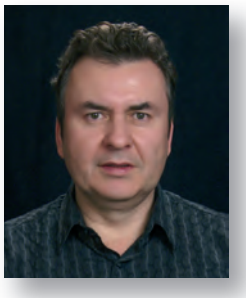
Чукляев Илья Игоревич. кандидат технических наук, доцент, Докторант Военной академии войсковой противовоздушной обороны Вооруженных Сил Российской Федерации имени Маршала Советского Союза А.М. Василевского, г. Смоленск

Ilya Chucklyaev, Ph.D., Associate Professor, Doctoral Student of the Army Air Defense Military Academy named after Marshal of the Soviet Union A.M.Vasilevsky, Smolensk
E-mail: Chucklyaev@yandex.ru



Шаров Иван Александрович, научный сотрудник Государственного научно-исследовательского испытательного института проблем технической защиты информации Федеральной службы по техническому и экспортному контролю, г. Воронеж

Ivan Sharov, Research Associate of the National Scientific and Research Institute of Problems in Technical Information Defense of the Federal Service for Technical and Export Control, Voronezh
E-mail: Sharov.Ivan@mail.ru



Щербаков, Алексей, GSSP, SCEA, SCJP, главный консультант по безопасности программных систем компании AsTech Consulting, член Открытого Проекта по Безопасности Веб-приложений (OWASP), Консорциума по Безопасности Веб-приложений (WASC), г. Сан-Франциско, США

Alexey Shcherbakov, GSSP, SCEA, SCJP, Senior Application Security Consultant at AsTech Consulting, Member of the Open Web Application Security Project (OWASP), Web Application Security Consortium (WASC), San Francisco, USA
E-mail: alec.shcherbakov@astechconsulting.com

Язов Юрий Константинович, доктор технических наук, профессор, главный научный сотрудник Государственного научно-исследовательского испытательного института проблем технической защиты информации Федеральной службы по техническому и экспортному контролю, г. Воронеж

Yury Yazov, Sc. Dr., Professor, Chief Researcher of the National Scientific and Research Institute of Problems in Technical Information Defense of the Federal Service for Technical and Export Control, Voronezh
E-mail: Yazoff_1946@mail.ru