Приманка KFSensor работает на прикладном уровне, поэтому она не может имитировать набор протоколов IP и, в частности, не позволяет имитировать маршруты прохождения трафика, но для большинства атак этот сервис избыточен.

В том случае, если сетевой трафик велик и программные анализаторы пакетов не справляются с потоком, рекомендуется использовать в качестве средств анализа пакетов и обнаружения атак аппаратные средства – либо специализированные аппаратные IDS, либо функции анализа трафика, встроенные в коммутационное оборудование.

ЛИТЕРАТУРА

1. Узнай своего врага: Honeynets. Проект Honeynet / перевод В.В. Мяснянкина // Bugtraq.ru Информационная безопасность [Электронный ресурс]. — Режим доступа: http://bugtraq.ru/library/security/honeynet.html?k=9.
2. Первое описание концепции honeypot // Security Lab by Positive Technologies [Электронный ресурс]. — Режим доступа: http://www.securitylab.ru/informer/240663.php.
3. *Спитцнер, Л.* Honeynet Project: ловушка для хакеров. // CIT Forum [Электронный ресурс]. — Режим доступа: http://citforum.edunet.kz/security/internet/honeynet/.
4. *Мяснянкин, В.* Все любят мед //Bugtraq.ru Информационная безопасность [Электронный ресурс]. — Режим доступа: http://www.bugtraq.ru/library/security/honey.html.
5. *Глушко, С.* Ловушка для хищника // Xaker.Ru [Электронный ресурс]. — Режим доступа: http://www.xakep.ru/magazine/xa/106/066/1.asp.
6. Построение виртуальных ловушек // Security Lab by Positive Technologies [Электронный ресурс]. — Режим доступа: http://www.securitylab.ru/analytics/216223.php.
7. Система обнаружения вторжений на базе IDS Snort (snort ids). // The OpenNET Project [Электронный ресурс]. — Режим доступа: http://www.opennet.ru/base/sec/snort_ids.txt.html.
8. *Граймз, Р.* Использование приманок на базе Windows // Windows IT Pro. 2004. №4. (электронная версия: [Электронный ресурс]. — Режим доступа: http://www.osp.ru/win2000/2004/04/176949/).

ОРГАНИЗАЦИОННО-ПРАВОВАЯ СПЕЦИФИКА РАЗВИТИЯ СОСТАВЛЯЮЩИХ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

И.В. Поночевная

Санкт-Петербургский государственный инженерно-экономический университет
Санкт-Петербург

В настоящее время во всем мире резко повысилось внимание к проблеме системе информационной безопасности (СИБ). Это обусловлено процессами стремительного расширения потоков развития информационных ресурсов в глобальной компьютерной сети Internet , пронизывающих все сферы жизни общества и государства. К значительной части информационных ресурсов глобальной компьютерной сети Internet предъявляются требования по обеспечению определенной степени конфиденциальности.

Отличительной особенностью информационных объектов является комплексное использование на них информационных и телекоммуникационных систем, то есть инфокоммуникационных систем, что вызывает необходимость применения более широкого спектра составляющих для защиты информационного ресурса в информационном пространстве.

Рассматриваемые в работе декомпозиции составляющих СИБ могут оказаться совершенно бесполезными, если не будет соблюден надлежащий действующий пакет политик.

Действующий пакет политик включает в себя концепцию пакета политик безопасности (КППБ) и является в совокупности с составляющими СИБ основным документом, определяющим защищенность информационного пространства от внутренних, внешних и комбинированных «субъектов угроз» (Рис.2).

Полезные рекомендации на этот счет содержаться в международных стандартах, в частности в международном стандарте безопасности информационных систем ISO 17799-2005 (стандарт построения эффективной системы безопасности разработан в 2000 году Международной организацией по стандартизации и является официальным документом, описывающим комплексный подход к вопросам безопасности и рассматривающим в качестве элементов управления как технические, так и организационно-административные меры, обеспечивающие конфиденциальность, целостность, доступность и достоверность информации).

Решение данной задачи предполагает, что защищенность может быть обеспечена только соблюдением концепции пакета политик безопасности, на основе комплексного подхода, реализация которого начинается с организационно-правовых, инженерно-технических и технологических составляющих на единой концептуальной основе.

Инженерно-техническое направление защиты формируется программно-аппаратными средствами защиты. Это направление формирует единую инженерно-техническую политику безопасности в части выбора средств защиты и текущее состояние системы безопасности.

Под программным средством защиты следует понимать совокупность специальных программ, реализующих функции безопасности и режима функционирования системы.

К аппаратным средствам защиты относятся механические, оптические, лазерные, радиотехнические, биометрические и другие средства.

Технологическое направление защиты. Система безопасности должна быть эффективной, устойчивой к воздействиям, обеспечивать прозрачность, то есть соответствовать требованиям международных и отечественных стандартов.

Организационно-правовое направление защиты основано на нормативно-правовой основе, предполагающей, что разглашение, утечка ценной информации и несанкционированный доступ или взлом или подбор пароля в систему будет невозможным или существенно затруднен за счет проведения организационных мероприятий.

Одним из основных компонентов организационного направления является служба информационной безопасности. Основная цель функционирования службы информационной безопасности, использующей комплекс средств защиты, избежать или свести до минимума возможность нарушения, или вовремя заметить и устранить последствия дестабилизирующих факторов по отношению к системе.

В работе предполагается, что организационно-правовая составляющая пакета политик играет первостепенную роль, так как эффективность самых дорогостоящих и сложных средств защиты сводятся к нулю, если пользователи системы будут игнорировать элементарные правила работы.

Таким образом, если система будет соответствовать стандартам, то она будет прозрачна для взаимодействия с любой другой системой, которая соответствует также стандартам. Это относится к средствам криптографической защиты, к средствам защиты от несанкционированного воздействия, к средствам антивирусной защиты и т.д. Обобщающий мировой опыт международных стандартов в этой области, является результатом развития национальных стандартов.

Особенно актуальны эти требования для инфокоммуникационных систем специального назначения, поскольку они предназначены, как правило, для передачи информационного ресурса, составляющей государственную тайну.

Вместе с развитием способов и методов передачи и преобразования информационного ресурса постоянно развиваются и методы обеспечения ее безопасности. Современный этап развития этой проблемы характеризуется переходом от традиционного ее представления как проблемы защиты информации к более широкому пониманию – проблеме информационной безопасности (инфобезопасности), заключающийся в комплексном ее решении по двум основным составляющим.

К первой составляющей можно отнести защиту государственной тайны и конфиденциальных сведений, обеспечивающую главным образом невозможность несанкционированного доступа к ним. При этом под конфиденциальными сведениями понимаются сведения ограниченного доступа общественного характера (коммерческая тайна, и т.д.), а также личная конфиденциальная информация (интеллектуальная собственность, персональные данные и т.д.).

Ко второй составляющей относится защита от информационного воздействия на человека, общество и государства, которая в последнее время приобретает международный масштаб и стратегический характер.

Исходя из вышесказанного, в последнее время проблема защиты информации рассматривается как проблема системы информационной безопасности как неотъемлемой составной части национальной безопасности Российской Федерации. Это ясно определяется концепцией национальной безопасности Российской Федерации и Доктриной информационной безопасности Российской Федерации, так как система национальных интересов России определяется совокупностью основных интересов личности, общества и государства.

Информационная безопасность Российской Федерации определяется в Доктрине как состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационном пространстве заключается в реализации конституционных прав человека и гражданина на доступ к информации, использовании ее в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационном пространстве заключается в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия.

Интересы государства заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод граждан в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности; защиты информационных ресурсов государства от несанкционированного доступа; обеспечение безопасности информационных и телекоммуникационных систем России.

Из вышесказанного среди всей совокупности средств и методов обеспечения информационной безопасности организационно-правовая специфика стоит на особом месте, так как играет одну из наиболее важных ролей в создании и функционировании прочной системы защиты информации в информационном пространстве.

Это направление обуславливается тем, что возможности несанкционированного использования конфиденциальной информации в значительной мере зависят не от технических аспектов защиты, а от злоумышленных, небрежных и халатных действий пользователей системы и персонала объекта обработки информационного ресурса. Влияние этих аспектов практически невозможно избежать с помощью технических и программных средств защиты. Для этого необходимо организационное обеспечение системы информационной безопасности (инфобезопасности) – регламентация деятельности по обработке и защите конфиденциального информационного ресурса и взаимоотношений обслуживающего персонала на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к информационному ресурсу становится невозможным или существенно затрудняются за счет проведения организационных мероприятий.

Вышеизложенное говорит о том, что работоспособность системы информационной безопасности, должны базироваться на концепции пакета политик, так как важность этой проблемы подчеркивает такой факт, как создание по инициативе Президента Российской Федерации «Доктрины информационной безопасности», и выделены общие методы обеспечения информационной безопасности: организационно-правовые, технические и экономические. Доктрина информационной безопасности Российской Федерации», является основой для формирования государственной политики в области обеспечения информационной безопасности России [1].

ЛИТЕРАТУРА

1. Доктрина информационной безопасности РФ от 9 сентября 2000г. № Пр-1895.

ВОЗМОЖНОСТИ ЭЛЕКТРОННОЙ БИБЛИОТЕКИ РЕСПУБЛИКИ КАРЕЛИЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ УЧЕБНОЙ И НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ

Н.С. Рузанова, А.Г. Марахтанов
Петрозаводский государственный университет
Петрозаводск

Электронная библиотека Республики Карелия (ЭБ РК) разработана Региональным Центром Новых Информационных Технологий (РЦ НИТ) Петрозаводского государственного университета (ПетрГУ) в 2004 году и с тех пор предоставляет бесплатный доступ к значительному числу полнотекстовых изданий. Любой пользователь сети Интернет может обратиться к ресурсам библиотеки, по адресу http://elibrary.karelia.ru.

ПетрГУ является многопрофильным вузом, в состав которого входят 17 факультетов и 85 кафедр, что требует формирования фондов библиотеки из изданий различных тематик и предметных областей. В ЭБ РК доступны издания по истории, филологии, медицине, математике, физике и др. Помимо Научной библиотеки и издательства ПетрГУ, в наполнении электронной библиотеки принимают участие Национальная библиотека Республики Карелия, библиотеки Карельской государственной педагогической академии (КГПА) и Карельского научного центра Российской академии наук. РЦ НИТ ПетрГУ осуществляет техническое сопровождение, а также разработку и внедрение новых сервисов.

Значительную часть коллекции составляют цифровые копии старинных редких книг, изданных в XVII – XIX веках. Среди них – «EPISTOLARVM AD FAMILIARES LIB. XVI» Цицерона, изданная в 1610