УДК 002.6

НЕКОТОРЫЕ АСПЕКТЫ ЗАЩИТЫ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

***Н.Р. Шевко**, старший преподаватель кафедры экономической теории, правовой статистики, математики и информатики Казанского юридического института МВД России, кандидат экономических наук*

В современной постиндустриальной эпохе информация становится наиболее важным ресурсом. При этом возрастает роль информационных технологий, которые являются значимым фактором. Независимо от сферы деятельности одним из самых важных ресурсов становятся информационные. Все большую ценность в современных условиях приобретают оперативность их получения и обработки, а также надежность защиты. Но информация – специфическая субстанция. Ее невозможно хранить в сейфе. Ценность она приобретает лишь при ежедневном использовании. Вся информация хранится, обрабатывается и передается с помощью компьютеров или сетей. При этом главный принцип большинства компьютерных технологий – открытость и доступность. Возникает вопрос, как совместить открытость с необходимостью надежной защиты информации, предотвращением воздействия информационных угроз.

Под информационной безопасностью (ИБ) понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности. Угроза – это потенциальная возможность определенным образом нарушить информационную безопасность. По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды[1]:

угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

угрозы информационному обеспечению государственной политики Российской Федерации;

угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

угрозы безопасности информационных и телекоммуникационных средств и систем как уже развернутых, так и создаваемых на территории России.

Угрозами безопасности информационных систем (ИС) могут также являться:

противоправные сбор и использование информации;

нарушения технологии обработки информации;

внедрение в аппаратные и программные изделия компонентов, реализу-

ющих функции, не предусмотренные документацией на эти изделия;

разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;

компрометация ключей и средств криптографической защиты информации;

утечка информации по техническим каналам;

внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;

уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;

использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;

несанкционированный доступ к информации, находящейся в банках и базах данных;

нарушение законных ограничений на распространение информации.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем. Например, возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении.

Подчеркну, что само понятие «угроза» в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнуто открытой организации угроз конфиденциальности может просто не существовать – вся информация считается общедоступной; однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в ИБ, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется окном опасности, ассоциированным с данным уязвимым местом. Пока существует окно опасности, возможны успешные атаки на ИС.

Если речь идет об ошибках в программном обеспечении, то окно опасности «открывается» с появлением средств использования ошибки и ликвидируется при наложении заплат, ее исправляющих.

Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда – недель).

Новые уязвимые места и средства их использования появляются постоянно; это значит, во-первых, что почти всегда существуют окна опасности и, во-вторых, что отслеживание таких окон должно производиться постоянно, а выпуск и наложение заплат – как можно более оперативно.

Отмечу, что некоторые угрозы нельзя считать следствием каких-то ошибок или просчетов; они существуют в силу самой природы современных ИС. Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания.

Рассмотрим наиболее распространенные угрозы, которым подвержены современные информационные системы.

Угрозы ИБ можно классифицировать по нескольким критериям:

– по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;

– по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);

– по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);

– по расположению источника угроз (внутри/вне рассматриваемой ИС).

Классифицировать угрозы можно по возможности нанесения ущерба субъекту отношений при нарушении целей безопасности. Ущерб может быть причинен каким-либо субъектом (преступление, вина или небрежность), а также стать следствием, независящим от субъекта проявлений. Угрозы могут быть:

1. При обеспечении конфиденциальности информации:

– хищение (копирование) информации и средств ее обработки;

– утрата (неумышленная потеря, утечка) информации.

2. При обеспечении целостности информации:

– модификация (искажение) информации, отрицание подлинности информации, навязывание ложной информации.

3. При обеспечении доступности информации:

– блокирование информации;

– уничтожение информации и средств ее обработки.

Еще угрозы бывают:

1. Угроза нарушения конфиденциальности заключается в том, что информация становится известна тому, кто не располагает полномочиями доступа к ней, правами доступа.

2. Угроза целостности включает в себя любое умышленное изменение информации, хранящейся в вычислительной системе или при передаче информации из одной системы в другую.

3. Угроза отказа служб (угроза блокирования доступа) возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых злоумышленником или другим пользователем, блокируется доступ к некоему ресурсу вычислительной системы.

4. Раскрытие параметров системы. Защита системы считается преодоленной, если в ходе тестирования системы были выявлены все уязвимости системы.

Основные методы реализации угроз:

– непосредственное обращение к объектам доступа; создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;

– модификация средств защиты, позволяющая реализовать угрозы информационной безопасности.

Успех в области информационной безопасности может принести только комплексный подход, сочетающий меры четырех уровней: законодательного; административного; процедурного и программно-технического.

Проблема информационной безопасности – не только (и не столько) техническая. Без законодательной базы, без постоянного внимания руководства организации и выделения необходимых ресурсов, без мер управления персоналом и физической защиты решить ее невозможно. Комплексность также усложняет проблематику информационной безопасности; требуется взаимодействие специалистов из разных областей.

Российские правовые акты в большинстве своем имеют ограничительную направленность. Но то, что для Уголовного или Гражданского кодекса естественно, по отношению к ФЗ «Об информации, информационных технологиях и о защите информации»[2] является принципиальным недостатком. Сами по себе лицензирование и сертификация не обеспечивают безопаснос-

ти. К тому же в законах не предусмотрена ответственность государственных органов за нарушения ИБ.

Одним из методов защиты информации является криптографический. Все, что связано с криптографией, сложно не столько с технической, сколько с юридической точки зрения; для шифрования это верно вдвойне. Данный сервис является инфраструктурным, его реализации должны присутствовать на всех аппаратно-программных платформах и удовлетворять жестким требованиям не только к безопасности, но и к производительности. Пока же единственным доступным выходом является применение свободно распространяемого программного обеспечения.

Надежный контроль целостности также базируется на криптографических методах с аналогичными проблемами и методами их решения. К счастью, к статической целостности есть и некриптографические подходы, основанные на использовании запоминающих устройств, данные на которых доступны только для чтения. Если в системе разделить статическую и динамическую составляющие и поместить первую в ПЗУ или на компакт-диск, можно в корне пресечь угрозы целостности. Разумно, например, записывать регистрационную информацию на устройства с однократной записью; тогда злоумышленник не сможет «замести следы».

Обеспечение отказоустойчивости и безопасного восстановления – аспекты высокой доступности. При их реализации на первый план выходят архитектурные вопросы, в первую очередь – внесение в конфигурацию (как аппаратную, так и программную) определенной избыточности, с учетом возможных угроз и соответствующих зон поражения. Безопасное восстановление – действительно последний рубеж, требующий особого внимания, тщательности при проектировании, реализации и сопровождении. Управление – это инфраструктурный сервис. Безопасная система должна быть управляемой. Всегда должна быть возможность узнать, что на самом деле происходит в ИС (а в идеале – и получить прогноз развития ситуации). Возможно, наиболее практичным решением для большинства организаций является использование какого-либо свободно распространяемого каркаса с постепенным добавлением к нему собственных функций.

Принцип работы систем защиты информации в большинстве случаев один и тот же. Вы указываете программе, какая информация, по-вашему, является конфиденциальной. Это могут быть отдельный документ, папка документов, целая база данных, письма и записные книжки или вообще бухгалтерская программа со всеми своими приложениями. Все, что вы указали, надежно шифруется и становится недоступным до тех пор, пока не будет введен пароль и не вставлены ключ или смарт-карта. Даже если кто-то узнал пароль и украл компьютер, все равно он не сможет прочесть информацию, не имея физического ключа. В зависимости от вашего предпочтения таковыми могут быть электронный брелок, смарт-карта, PCMCIA-карта или обычный электронный ключ, вставляемый в разъем компьютера.

Чтобы надежные системы защиты легко вошли в массовый обиход, необходим ряд условий: простота в установке и эксплуатации; приемлемая цена; наличие в широкой сети магазинов и сервисных фирм и др.

ПРИМЕЧАНИЯ

[1] Доктрина информационной безопасности РФ (утв. Президентом РФ 09.09.2000 № Пр-1895) // СПС КонсультантПлюс.

[2] Об информации, информационных технологиях и о защите информации. Федеральный Закон от 27 июля 2006 г. № 149-ФЗ // СПС КонсультантПлюс.

Аннотация

В статье рассматриваются вопросы защиты информационных ресурсов современного общества, а также информационных систем. Раскрыто понятие информационной безопасности, защиты информации, а также виды и методы реализации угроз информационной безопасности, некоторые способы защиты информационных ресурсов.

Ключевые слова: информация, защита информационных ресурсов, постиндустриальная эпоха, информационная безопасность, способы защиты информационных систем.

Summary

The article considers the questions of the defence of information resources of modern society and information systems, reveals the notion of information security, the defence of information, types and methods of realization of threats of information security, some ways of the defence of information resources.