УДК 004.056

А.А. Конев, Е.М. Давыдова

Подход к описанию структуры системы защиты информации

Описывается подход к структуризации системы защиты информации. Данный подход основан на рассмотрении системы защиты информации с позиции эффективности ее работы. Под эффективностью в данном случае понимается наличие комплексных рубежей защиты каждого элемента информационной системы от каждой угрозы.

Ключевые слова: информационная безопасность, система защиты информации, многоуровневая информационная система.

На практике при разработке системы защиты для информационных систем в основном используется типовой набор технических и организационных средств защиты информации. Чаще всего рекомендуется к внедрению какое-либо средство комплексной защиты от НСД, антивирус, межсетевой экран и т.п. Рекомендуемый набор нормативной документации может сильно отличаться у различных организаций, как и конкретные ограничения, указанные в этих документах. Корректность выбора зависит от квалификации эксперта, потому что не существует четкой методики определения необходимого набора механизмов защиты (технических и организационных) в зависимости от структуры информационной системы и существующих в ней угроз. Основная задача – выработка подхода к представлению системы защиты информации, который включал бы однозначную классификацию документопотоков в информационной системе, классификацию угроз в рамках каждого типа документопотоков и классификацию механизмов защиты для каждой типовой угрозы.

Система защиты информации (СЗИ) – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации [1]. Основываясь на этом определении, подходы к структуре системы защиты информации можно рассматривать по двум основным направлениям:

− структура технического (программно-технического) элемента системы защиты, включающего инженерно-технические и программно-аппаратные средства защиты информации;

− структура нормативного элемента системы защиты, регламентирующего работу программно-технического элемента и персонала.

При определении структуры любой сложной системы базовым этапом является формулирование цели и критериев эффективности работы системы. В соответствии с [1] цель защиты информации – заранее намеченный результат защиты информации (результатом защиты информации может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию). Согласно [2], угроза информационной безопасности организации – совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации. При таком подходе основной целью СЗИ является предотвращение ущерба, т.е. предотвращение реализации угроз информационной безопасности.

Эффективность работы можно рассматривать как возможность механизмов защиты информации, реализованных в СЗИ, противостоять угрозам информационной безопасности и адекватно реагировать на них [3]. Угрозы могут быть реализованы в двух случаях:

− отсутствие элемента СЗИ, ответственного за противодействие данной угрозе;

− недостаточный для противодействия данной угрозе уровень защищенности, предоставляемый элементом СЗИ.

На наличие прямой зависимости структуры СЗИ от необходимости нейтрализации угроз информационной безопасности указывается, например, в [4]. Таким образом, структура СЗИ должна зависеть от перечня угроз защищаемой системе. Модель угроз, на основе которой проектируется структура СЗИ, обязательно должна включать следующие разделы:

− перечень угроз информации;

− перечень угроз носителям информации;
− перечень угроз элементам информационной системы;
− перечень угроз элементам системы защиты;
− перечень угроз, касающихся управления системой защиты – невыполнения нормативных документов организации в области информационной безопасности.

Согласно [5], архитектура системы защиты информации должна быть аналогична архитектуре защищаемой системы. Зависимость структуры СЗИ от структуры информационной системы вызвана необходимостью защищать информацию на всех этапах работы с информацией – этапах хранения, обработки, передачи внутри информационной системы; отправки за пределы информационной системы и т.п. Это значит, что построению СЗИ должна предшествовать инвентаризация ресурсов, используемых в информационной системе, включая каналы связи, а также должностных обязанностей сотрудников на наличие прав работы с этими ресурсами и самой информацией.

По сути, защищать (устанавливать рубежи защиты) нужно все возможные потоки информации и места ее обработки в системе. Это позволяет определить количество необходимых экземпляров элементов защиты и их тип. При этом тип зависит от среды распространения информации (акустическая, видовая и т.д.).

Формализованный подход к построению модели информационной системы в целях защиты информации на данный момент отсутствует. Построение структуры чаще всего сводится к построению сетевой конфигурации для конкретной информационной системы и схемы территориального расположения ее элементов. Попытка формализации документопотоков в защищаемой информационной системе рассматривается, например, в [6].

Одной из основных проблем при построении структуры информационной системы является необходимость учета ее многоуровневости. В СТО БР ИББС-1.0-2010 [7] используется многоуровневое представление информационной инфраструктуры. Иерархия основных уровней:

− физический (линии связи, аппаратные средства и пр.);
− сетевого оборудования (маршрутизаторы, коммутаторы, концентраторы и пр.) [13];
− сетевых приложений и сервисов;
− операционных систем (ОС);
− систем управления базами данных (СУБД);
− банковских технологических процессов и приложений;
− бизнес-процессов организации.

Существует подход и к многоуровневому описанию инженерно-технической структуры информационной системы [8], включающий следующие зоны:

− территория, занимаемая организацией;
− здание на территории;
− коридор или его часть;
− помещение (служебное, кабинет, комната, зал, техническое помещение, склад и др.);
− шкаф, сейф, хранилище.

На каждом из уровней информационной системы могут быть установлены средства защиты информации, что приводит к появлению рубежей защиты – элемента системы защиты, включающего само программное (программно-аппаратное) или техническое средство и нормативное обеспечение его работы. Еще одним следствием учета многоуровневой структуры информационной системы и многоуровневой структуры СЗИ является необходимость составления перечня угроз для каждого уровня системы и для каждого рубежа защиты.

Дополнительно должно рассматриваться обеспечение контроля корректности работы информационной системы и рубежей защиты. Контроль может осуществляться в ручном или автоматизированном режиме. Так, в [9] предлагается реализовать:

1) восстановление системы защиты информации и защищаемой информации после воздействия угроз;
2) обеспечение контроля функционирования средств и системы защиты информации и немедленное реагирование на их выход из строя;
3) обеспечение оперативного контроля работы подсистемы защиты информации и мониторинга действий пользователей.

В [10] приводится классификация объектов угроз, позволяющая определить ресурсы, подлежащие защите. Кроме информации, в перечень объектов включены:

− элементы информационной системы (программные и аппаратные) и их настройки;

− элементы системы защиты (программные и аппаратные) и их настройки.

Подход к построению СЗИ на основе защиты от угроз позволяет рассматривать структуру СЗИ на уровне «Тип угрозы – Тип рубежа защиты». Тогда классификация методов и средств защиты сводится к следующим типам (рис. 1):

1) рубежи защиты информации и ее носителей от угроз конфиденциальности, целостности и доступности;

2) рубежи защиты элементов информационной системы (баз данных, операционных систем, сетевых сервисов и т.п.), включая программно-технические средства защиты информации, и их настроек от угроз конфиденциальности и целостности;

3) рубежи защиты, отвечающие за контроль выполнения правил работы с защищаемой информацией и программно-техническими средствами СЗИ.

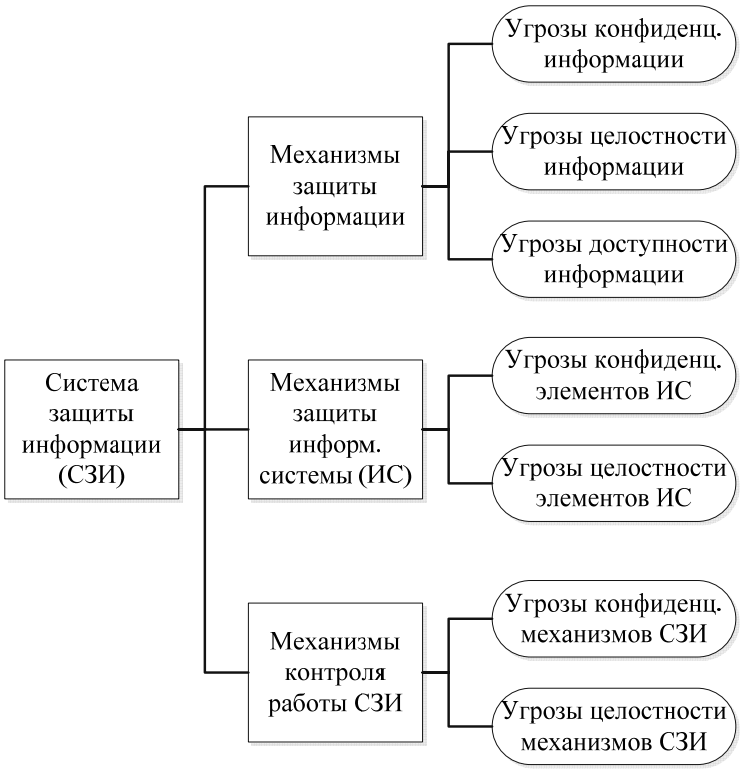

Рис. 1. Подход к структуризации системы защиты информации

При структуризации СЗИ можно рассматривать следующие группы механизмов защиты:

− механизмы защиты информации, ее носителей и элементов информационной системы от угроз конфиденциальности;

− механизмы защиты информации, ее носителей и элементов информационной системы от угроз целостности.

Угрозы доступности могут быть реализованы после нарушения целостности элементов информационной системы или после перегрузки каналов связи. Соответственно, механизмами защиты от угроз доступности информации будет являться обеспечение целостности элементов информационной системы (например, сетевых сервисов) и проектирование каналов связи, выдерживающих пиковые нагрузки.

Механизмы защиты от угроз конфиденциальности можно разделить на следующие типы:

− механизмы, препятствующие доступу несанкционированных лиц к защищаемой информации или к элементам информационной системы;

− механизмы, препятствующие неконтролируемому выходу информации за пределы санкционированного объекта;

− механизмы, контролирующие потоки защищаемой информации.

Механизмы защиты от несанкционированного доступа включают: разграничение доступа, аутентификацию и шифрование. Шифрование используется для ограничения доступа к самой информации, а управление доступом может использоваться на всех уровнях информационной системы для защиты носителей информации.

Под механизмами, препятствующими выходу информации за пределы контролируемой зоны, подразумеваются средства, противодействующие пассивному наблюдению злоумышленника [11]. Для бумажных документов – это гарантированное уничтожение всех черновиков и других выделенных к уничтожению документов с защищаемой информацией. Основные методы и средства для защиты визуальной информации – политика «чистого стола»; положение монитора, препятствующее несанкционированному съему с него информации; жалюзи и т.п. При работе с файловой системой такие же угрозы возникают, например, при удалении драйвером защищаемого файла. Механизм защиты – многократная перезапись освобождаемой области памяти на жестком диске.

Наиболее распространенный механизм контроля потоков защищаемой информации – аудит действий пользователя в операционной системе, его обращения к файлам, запуск программ и т.п.

Механизмы защиты от угроз нарушения целостности состоят из двух частей – механизмы контроля целостности и механизмы восстановления. Угрозы нарушения целостности существуют на всех уровнях информационной системы:

− угрозы целостности (достоверности) информации;

− угрозы целостности носителя информации (уничтожение носителя и хранящейся на нем информации);

− угрозы целостности исполняемых файлов;

− угрозы целостности программной среды (запуск несанкционированных приложений) [12];

− угрозы целостности аппаратной конфигурации информационной системы;

− угрозы целостности защищаемого помещения, здания, прилегающей территории (проникновение нарушителя);

− угрозы отключения средств защиты;

− угрозы изменения настроек средств защиты и т.д.

Таким образом, в работе приведены основные требования к описанию структуры системы защиты информации. Структура СЗИ должна быть формализована таким образом, чтобы была возможность оценки достаточности комплекса средств защиты и нормативных документов, используемых в ней.

Формальное описание структуры СЗИ должно опираться на несколько моделей:

− модель системы документооборота;

− модель информационной системы;

− модель угроз информации и информационной системе;

− модель угроз средствам защиты информации.

Модель системы документооборота позволит определить, в рамках каких сред циркулирует информация в информационной системе, а также объекты и субъектов, которым разрешено хранение, обработка и передача информации.

Модель информационной системы позволит учесть типы каналов передачи информации и многоуровневость зон работы с информацией, определив необходимое количество рубежей защиты.

Модель угроз информации должна включать весь возможный перечень угроз, для каждой из которых будут определены методы и средства защиты в рамках каждой среды.

Модель угроз средствам защиты позволит учитывать в структуре системы защиты мероприятия, необходимые для обеспечения непрерывной работы СЗИ.

При этом структура СЗИ должна быть основана на едином описании программно-технического и нормативного элемента системы защиты, позволяя комплексно оценить качество защиты от каждой угрозы.

Работа выполнена в рамках проекта 7.701.2011 (проект 1/12) при поддержке Министерства образования и науки Российской Федерации.

Литература

1. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. – Введ. 2008-02-01. – М.: Стандартинформ, 2008. – 12 с.

2. ГОСТ Р 53114–2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – Введ. 2009-09-30. – М.: Стандартинформ, 2009. – 20 с.

3. Джоган В.А. Особенности синтеза системы показателей эффективности защиты информации в компьютерных системах / В.А. Джоган, А.П. Курило, Н.С. Шимон // Безопасность информационных технологий. – 2011. – №4. – С. 170–175.

4. Отавин А.Д. Интеграционный подход к построению защищенных распределенных вычислительных систем: автореф. дис. ... канд. техн. наук. – СПб., 2001. – 18 с.

5. Основы информационной безопасности: учеб. пособие для вузов / Р.В. Мещеряков, А.А. Шелупанов, Е.Б. Белов, В.П. Лось. М.: Горячая линия-Телеком, 2006. – 389 с.

6. Конев А.А. Подход к построению модели угроз защищаемой информации // Доклады ТУСУРа. – 2012. – №1 (25), ч. 2. – С. 34–39.

7. СТО БР ИББС-1.0-2010. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. – Банк России. – Введ. 2010-06-21 [Электронный ресурс] – Режим доступа: http://cbr.ru/credit/Gubzi_docs/st-10-10.pdf, свободный (дата обращения: 25.05.2013).

8. Зайцев А.П. Технические средства и методы защиты информации: учебник для вузов / А.П. Зайцев, А.А. Шелупанов. – 7-е изд. испр. – М.: Горячая линия-Телеком, 2012. – 442 с.

9. Встраивание криптографических функций в систему связи с ограниченными ресурсами / С.К. Росошек, Р.В. Мещеряков, А.А. Шелупанов, С.С. Бондарчук // Вопросы защиты информации. – 2004. – № 2. – С. 22–25.

10. Филькин К.Н. Информационно-управляющая система поддержки принятия решений при управлении информационной безопасностью территориально распределенной организацией / К.Н. Филькин, С.Н. Филькин, А.А. Шелупанов // Безопасность информационных технологий. – 2007. – № 4. – С. 83–86.

11. Зыков Д.Д. Проблема информационной безопасности производства наноэлектроники / Д.Д. Зыков, Р.В. Мещеряков, С.С. Бондарчук // Доклады ТУСУРа. – 2010. – № 1 (21), ч. 1. – С. 93–94.

12. Принципы моделирования механизмов воздействия вредоносных программ на защищенные информационные системы в интересах оценки угроз их безопасности / О.С. Авсентьев, В.В. Александров, Г.И. Рябинин и др. // Доклады ТУСУРа. – 2008. – № 2 (18), ч. 1. – С. 135–136.

13. Исхаков С.Ю. Разработка методического и программного обеспечения для мониторинга работы локальных сетей / С.Ю. Исхаков, А.А. Шелупанов // Телекоммуникации. – 2013. – № 6. – С. 16–20.

Конев Антон Александрович
Канд. техн. наук, доцент каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Тел.: 8 (382-2) 41-34-26
Эл. почта: kaa1@kibevs.tusur.ru

Давыдова Елена Михайловна
Канд. техн. наук, доцент каф. КИБЭВС
Тел.: 8 (382-2) 41-34-26
Эл. почта: dem@kibevs.tusur.ru

Konev A.A., Davydova E.M.
Approach to structuring information security systems

This paper describes an approach to structuring information security systems. This approach is based on the analysis of information security from the perspective of its effectiveness. Effectiveness in this case refers to the presence of complex defense line from each threat for every element of the information system.
Keywords: information security, security system, multi-level information system.