ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

С. А. Нестеров

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УЧЕБНИК И ПРАКТИКУМ
ДЛЯ АКАДЕМИЧЕСКОГО БАКАЛАВРИАТА

**Книга доступна в электронной библиотечной системе
biblio-online.ru**

Москва ▪ Юрайт ▪ 2016

УДК 004.056(075.8)
ББК 32.81я73
Н56

***Автор*:**

Нестеров Сергей Александрович — кандидат технических наук, доцент кафедры системного анализа и управления Института компьютерных наук и технологий Санкт-Петербургского государственного политехнического университета.

***Рецензенты*:**

Ефремов А. А. — кандидат физико-математических наук, доцент Санкт-Петербургского государственного политехнического университета.

Нестеров, С. А.

Н56 Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2016. — 321 с. — Серия : Университеты России.

ISBN 978-5-9916-7227-6

Серия «Университеты России» позволит высшим учебным заведениям нашей страны использовать в образовательном процессе учебники и учебные пособия по различным дисциплинам, подготовленные преподавателями лучших университетов России и впервые опубликованные в издательствах университетов. Все представленные в этой серии учебники прошли экспертную оценку учебно-методического отдела издательства и публикуются в оригинальной редакции.

В учебнике «Информационная безопасность» автора Нестерова С. А. хорошо представлены защиты информации, основы криптографии, рассмотрены соответствующие описательные примеры, представлены методы расчета и статистические данные.

На данный момент ряд данных (ГОСТы) информационной безопасности, приводимый в учебнике, устарел. Однако это существенно не влияет на процесс обучения анализа и управления рисками в сфере информационной безопасности, и произошедшие изменения при необходимости могут быть учтены преподавателями.

Пособие может использоваться в системах повышения квалификации в рамках образовательной программы дополнительного профессионального образования «Информатика и вычислительная техника». Также может быть полезно широкому кругу специалистов в области информационных технологий.

УДК 004.056(075.8)
ББК 32.81я73

Книга издана в рамках совместного проекта Издательства «Юрайт» и Издательства Санкт-Петербургского политехнического университета Петра Великого.
Оригинал-макет предоставлен Издательством Санкт-Петербургского политехнического университета Петра Великого.

ISBN 978-5-9916-7227-6

ОГЛАВЛЕНИЕ

СПИСОК ПРИНЯТЫХ СОКРАЩЕНИЙ

АС — автоматизированная система (обработки информации);
БД — база данных;
ИБ — информационная безопасность;
ИС — информационная система;
ИТ — информационные технологии;
ЛК — Лаборатория Касперского;
МЭ — межсетевой экран;
НСД — несанкционированный доступ;
ОО — объект оценки;
ОС — операционная система;
ПО — программное обеспечение;
СЗИ — средство защиты информации;
СМИБ — система менеджмента информационной безопасности;
СФБ — стойкость функции безопасности;
ЦС — центр сертификации;
ЭЦП — электронная цифровая подпись;
ACL (Access Control List) — список управления доступом;
AH (Authentication Header) — протокол аутентифицирующего заголовка;
CA (Certification Authority) — центр сертификации или удостоверяющий центр;
CBC (Cipher Block Chaining) — сцепление блоков шифра (режим работы шифра DES);
CFB (Cipher FeedBack) — обратная связь по шифртексту (режим работы шифра DES);
CRL (Certificate Revocation List) — список отозванных сертификатов;
ECB (Electronic Code Book) — электронная кодовая книга (режим работы шифра DES);
ESP (Encapsulating Security Payload) — протокол инкапсулирующей защиты данных;

ICV (Integrity Check Value) — значение контроля целостности;
MAC (Message Authentication Code) — код аутентификации сообщений, имитовставка;
OFB (Output FeedBack) — обратная связь по выходу (режим работы шифра DES);
PKI (Public Key Infrastructure) — инфраструктура открытых ключей;
SA (Security Association) — контекст защиты или ассоциация безопасности;
SPI (Security Parameter Index) — индекс параметров защиты.

ВВЕДЕНИЕ

Современный специалист в области информационных технологий должен обладать знаниями и навыками обеспечения информационной безопасности. Связано это с тем, что в информационных системах предприятий и организаций хранится и обрабатывается критически важная информация, нарушение конфиденциальности, целостности или доступности которой может привести к нежелательным последствиям. Поэтому вопросам обеспечения информационной безопасности должно уделяться внимание на всех этапах разработки и эксплуатации информационных систем.

В данном пособии изложен материал учебной дисциплины «Основы информационной безопасности», в ходе изучения которой слушатели получают базовые знания о теории защиты информации, методах и средствах обеспечения информационной безопасности, а также практические навыки организации защиты информационных систем. Пособие включает в себя пять разделов.

В разделе 1 «Теоретические основы защиты информации» вводятся базовые понятия, связанные с обеспечением информационной безопасности, рассматриваются основные угрозы безопасности и меры противодействия им. Также делается обзор формальных моделей безопасности и современных стандартов в этой области.

Раздел 2 «Основы криптографии» включает описание основных понятий криптографии. Также изучаются наиболее распространенные алгоритмы симметричного и асимметричного шифрования, формирования дайджестов сообщений с помощью хэш-функций, процесс создания инфраструктуры открытых ключей (PKI).

В разделе 3 «Защита информации в IP-сетях» рассматриваются протоколы криптографической защиты данных, передаваемых по телекоммуникационным сетям, использующим стек протоколов TCP/IP, использование межсетевых экранов для защиты сетей.

В разделе 4 рассматриваются современные методики анализа и управления рисками, связанными с информационной безопасностью.

В разделе 5 приведены описания лабораторных работ.

Пособие может использоваться в системах повышения квалификации в рамках образовательной программы дополнительного профессионального образования «Информатика и вычислительная техника». Также оно может быть полезно широкому кругу специалистов в области информационных технологий.

1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. БАЗОВЫЕ ПОНЯТИЯ

Начнем изучение дисциплины с определения ряда базовых понятий.

Информация — это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Информация может существовать в различных формах в виде совокупностей некоторых знаков (символов, сигналов и т. д.) на носителях различных типов. Она может представлять ценность для отдельных лиц или организаций.

Защищаемая информация — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственниками информации. Собственниками информации могут быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо [1].

В последнее время все большие объемы информации, в том числе и критически важной для отдельных людей, организаций или государств, хранятся, обрабатываются и передаются с использованием автоматизированных систем (АС) обработки информации. *Система обработки информации* — совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, необходимых для выполнения автоматизированной обработки информации [2]. *Объект информатизации* — совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

В зависимости от конкретных условий может решаться задача обеспечения комплексной безопасности объекта информатизации или защиты отдельных ресурсов — информационных, программных и т. д.

Информационные ресурсы (активы) — отдельные документы и отдельные массивы документов, документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах других видов).

Рассматривая вопросы безопасности АС, можно говорить о наличии некоторых «желательных» состояний системы, через которые и описывается ее «защищенность» или «безопасность». Безопасность является таким же свойством системы, как надежность или производительность, и в последнее время ей уделяется все большее внимание. Чтобы указать на причины выхода системы из безопасного состояния, вводятся понятия «угроза» и «уязвимость».

Угроза (безопасности информации) — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Источник угрозы безопасности информации — субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации. По типу источника угрозы делят на связанные и несвязанные с деятельностью человека. Примерами могут служить, соответственно, удаление пользователем файла с важной информацией и пожар в здании. Угрозы, связанные с деятельностью человека, разделяют на угрозы случайного и преднамеренного характера. В последнем случае источник угрозы называют нарушителем или злоумышленником.

Уязвимость (информационной системы) — свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации. Например, угроза потери информации из-за сбоя в сети электропитания реализуется, ес-

ли в АС не применяются источники бесперебойного питания или средства резервного электроснабжения (это является уязвимостью).

Если говорить об информационных ресурсах, то реализация угрозы может привести к таким последствиям, как получение информации людьми, которым она не предназначена, уничтожение или изменение информации, недоступность ресурсов для пользователей. Таким образом, мы подошли к определению трех основных угроз безопасности.

Угроза конфиденциальности (угроза раскрытия) — это угроза, в результате реализации которой конфиденциальная или секретная информация становится доступной лицу, группе лиц или какой-либо организации, которой она не предназначалась. Здесь надо пояснить разницу между секретной и конфиденциальной информацией. В отечественной литературе «секретной» обычно называют информацию, относящуюся к разряду государственной тайны, а «конфиденциальной» — персональные данные, коммерческую тайну и т. п.

Угроза целостности — угроза, в результате реализации которой информация становится измененной или уничтоженной. Необходимо отметить, что и в нормальном режиме работы АС данные могут изменяться и удаляться. Являются ли эти действия легальными или нет, должно определяться политикой безопасности. *Политика безопасности* — совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Угроза отказа в обслуживании (угроза доступности) — угроза, реализация которой приведет к отказу в обслуживании клиентов АС, несанкционированному использованию ресурсов злоумышленниками по своему усмотрению.

Ряд авторов [3] дополняют приведенную классификацию, вводя *угрозу раскрытия параметров* АС, включающей в себя подсистему защиты. Угроза считается реализованной, если злоумышленником в

ходе нелегального исследования системы определены все ее уязвимости. Данную угрозу относят к разряду опосредованных: последствия ее реализации не причиняют какой-либо ущерб обрабатываемой информации, но дают возможность для реализации первичных (непосредственных) угроз.

Таким образом, *безопасность информации* — это состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность. *Защита информации* может быть определена как деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Выделяются следующие направления защиты информации:

- *правовая защита информации* — защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением;

- *техническая защита информации* — защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;

- *криптографическая защита информации* — защита информации с помощью ее криптографического преобразования[1];

- *физическая защита информации* — защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Защита информации осуществляется с использованием способов и средств защиты. *Способ защиты информации* — порядок и правила

[1] Вопросы, связанные с криптографической защитой информации, будут более подробно рассмотрены в разделе 2.

применения определенных принципов и средств защиты информации. *Средство защиты информации* — техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации. Отдельно выделяют:

- средства контроля эффективности защиты информации;
- средства физической защиты информации;
- криптографические средства защиты информации.

1.2. ОБЩАЯ СХЕМА ПРОЦЕССА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Рассмотрим теперь взаимосвязь основных субъектов и объектов обеспечения безопасности, как это предлагается в международном стандарте ISO/IEC-15408 (в России он принят как ГОСТ Р ИСО/МЭК 15408-2002 [4]).

Безопасность связана с защитой активов от угроз. Разработчики стандарта отмечают, что следует рассматривать все разновидности угроз, но в сфере безопасности наибольшее внимание уделяется тем из них, которые связаны с действиями человека. Рис. 1.1 иллюстрирует взаимосвязь между высокоуровневыми понятиями безопасности.

За сохранность активов отвечают их владельцы, для которых они имеют ценность. Существующие или предполагаемые нарушители также могут придавать значение этим активам и стремиться использовать их вопреки интересам их владельца. Действия нарушителей приводят к появлению угроз. Как уже отмечалось выше, угрозы реализуются через имеющиеся в системе уязвимости.

Владельцы активов анализируют возможные угрозы, чтобы определить, какие из них могут быть реализованы в отношении рассматриваемой системы. В результате анализа определяются риски (т. е. события или ситуации, которые предполагают возможность ущерба) и проводится их анализ.

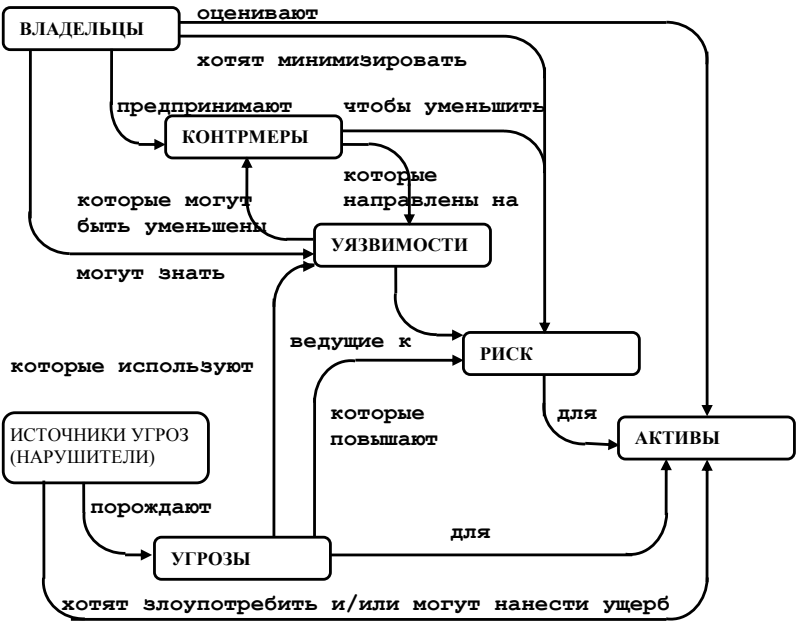

Рис. 1.1. Понятия безопасности и их взаимосвязь

Владельцы актива предпринимают контрмеры для уменьшения уязвимостей и выполнения политики безопасности. Но и после введения этих контрмер могут сохраняться остаточные уязвимости и соответственно — остаточный риск.

1.3. ИДЕНТИФИКАЦИЯ, АУТЕНТИФИКАЦИЯ, УПРАВЛЕНИЕ ДОСТУПОМ. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

В этом разделе будут рассмотрены вопросы, связанные с защитой информации от несанкционированного доступа (НСД).

Защита информации от несанкционированного доступа — защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами)

или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Для защиты от НСД, как правило, используется идентификация, аутентификация и управление доступом. В дополнение к перечисленным, могут применяться и другие методы.

Идентификация — присвоение пользователям идентификаторов (уникальных имен или меток) под которыми система «знает» пользователя. Кроме идентификации пользователей, может проводиться идентификация групп пользователей, ресурсов АС и т. д. Идентификация нужна и для других системных задач, например, для ведения журналов событий. В большинстве случаев идентификация сопровождается аутентификацией. *Аутентификация* — установление подлинности — проверка принадлежности пользователю предъявленного им идентификатора. Например, в начале сеанса работы в АС пользователь вводит имя и пароль. На основании этих данных система проводит идентификацию (по имени пользователя) и аутентификацию (сопоставляя имя пользователя и введенный пароль).

Управление доступом — метод защиты информации путем регулирования использования всех ресурсов системы.

Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от НСД любой информационной системы. Обычно выделяют 3 группы методов аутентификации.

1. Аутентификация по наличию у пользователя уникального объекта заданного типа. Иногда этот класс методов аутентификации называют по-английски “I have” («у меня есть»). В качестве примера можно привести аутентификацию с помощью смарт-карт или электронных USB-ключей.

2. Аутентификация, основанная на том, что пользователю известна некоторая конфиденциальная информация — “I know” («я знаю»). Например, аутентификация по паролю. Более подробно парольные системы рассматриваются далее в этом разделе.

3. Аутентификация пользователя по его собственным уникальным характеристикам — “I am” («я есть»). Эти методы также называются биометрическими. Биометрические методы аутентификации делят на статические и динамические.

Примеры аутентификации по статическим признакам — это проверка отпечатка пальца, рисунка радужной оболочки глаз, геометрии кисти руки, сравнение с фотографией и т. д. Достоинством этих методов является достаточно высокая точность. Но надо отметить, что подобные методы, как правило, требуют наличия специализированного оборудования (например, специальных сканеров) и имеют ограниченную область применения (например, при аутентификации по отпечатку пальца из-за грязи на руке человек может не пройти аутентификацию, т. е. подобные методы неприменимы на стройках и на многих производствах).

Примеры динамической аутентификации — аутентификация по голосу (при произнесении заранее определенной фразы или произвольного текста), аутентификация по «клавиатурному почерку» (проверяются особенности работы пользователя на клавиатуре, такие как время задержки при нажатии клавиш в различных сочетаниях) и т. д.

Нередко используются комбинированные схемы аутентификации, объединяющие методы разных классов. Например, двухфакторная аутентификация — пользователь предъявляет системе смарт-карту и вводит пин-код для ее активации.

Аутентификация может быть *односторонней*, когда одна сторона аутентифицирует другую (например, сервер проверяет подлинность клиентов), и *двусторонней*, когда стороны проводят взаимную проверку подлинности.

Также аутентификация может быть *непосредственной*, когда в процедуре аутентификации участвуют только две стороны, или *с участием доверенной стороны*. В последнем случае в процессе аутентификации участвуют не только стороны, проверяющие подлинность друг друга, но и другая или другие, вспомогательные. Эту третью

сторону иногда называют сервером аутентификации (англ. «authentication server») или арбитром (англ. «arbitrator»).

Парольные системы аутентификации

Наиболее распространенными на данный момент являются парольные системы аутентификации. Определим ряд понятий, использующихся при описании подобных систем.

Идентификатор пользователя — уникальная информация, позволяющая различить отдельных пользователей парольной системы (провести идентификацию). Это может быть имя учетной записи пользователя в системе или специально генерируемые уникальные числовые идентификаторы.

Пароль пользователя — секретная информация, известная только пользователю (и возможно — системе), которая используется для прохождения аутентификации. В зависимости от реализации системы, пароль может быть одноразовым или многоразовым. При прочих равных условиях системы с одноразовыми паролями являются более надежными. В них исключаются некоторые риски, связанные с перехватом паролей — пароль действителен только на одну сессию и, если легальный пользователь его уже задействовал, нарушитель не сможет такой пароль повторно использовать. Но системы с многоразовыми паролями (в них пароль может быть использован многократно) проще реализовать и дешевле поддерживать, поэтому они более распространены.

Учетная запись пользователя — совокупность идентификатора, пароля и, возможно, дополнительной информации, служащей для описания пользователя. Учетные записи хранятся в базе данных парольной системы.

Парольная система — это программный или программно-аппаратный комплекс, реализующий функции идентификации и аутентификации пользователей компьютерной системы путем проверки паролей. В отдельных случаях подобная система может выполнять дополнительные функции, такие как генерация и распределение

криптографических ключей и т. д. Как правило, парольная система включает в себя интерфейс пользователя, интерфейс администратора, базу учетных записей, модули сопряжения с другими компонентами подсистемы безопасности (подсистемой разграничения доступа, регистрации событий и т. д.).

Рассмотрим некоторые рекомендации по администрированию парольной системы, использующей многоразовые пароли.

1. Задание минимальной длины используемых в системе паролей. Это усложняет атаку путем подбора паролей. Как правило, рекомендуют устанавливать минимальную длину в 6–8 символов.

2. Установка требования использовать в пароле разные группы символов — большие и маленькие буквы, цифры, специальные символы. Это также усложняет подбор.

3. Периодическая проверка администраторами безопасности качества используемых паролей путем имитации атак[1], таких как подбор паролей «по словарю» (т. е. проверка на использование в качестве пароля слов естественного языка и простых комбинаций символов, таких как «1234»).

4. Установление максимального и минимального сроков жизни пароля, использование механизма принудительной смены старых паролей. При внедрении данной меры надо учитывать, что при невысокой квалификации пользователей от администратора потребуются дополнительные усилия по разъяснению пользователям того, что «от них требует система».

5. Ограничение числа неудачных попыток ввода пароля (блокирование учетной записи после заданного числа неудачных попыток войти в систему). Данная мера позволяет защититься от атак путем подбора паролей. Но при необдуманном внедрении также может привести к дополнительным проблемам — легальные пользователи из-за

[1] *Компьютерная атака* — целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.