Ю. А. Брюхомицкий

Безопасность информационных технологий

учебное пособие

ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
ЮФУ
РОСТОВ-НА-ДОНУ-ТАГАНРОГ

УДК 004.056.5(075.8)
ББК 32.97я73
Б898

Печатается по решению кафедры информационной безопасности Института компьютерных технологий и информационной безопасности Южного федерального университета (протокол № 6 от 6 марта 2020 г.)

Рецензенты:

заведующий кафедрой системного анализа и телекоммуникаций Института компьютерных технологий и информационной безопасности ЮФУ, доктор технических наук, профессор *Ю. И. Рогозов*

директор ООО «Инженерный центр «Интегра», г. Таганрог, кандидат технических наук *А. С. Басан*

Брюхомицкий, Ю. А.

Б898 Безопасность информационных технологий. Часть 1. : учебное пособие : в 2 ч. / Ю. А. Брюхомицкий ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2020.

ISBN 978-5-9275-3526-2

Часть 1. – 171 с.

ISBN 978-5-9275-3571-2 (Ч. 1)

Пособие содержит описание основных понятий информационной безопасности; угроз и уязвимостей информационных систем; стандартов защиты данных; методов и средств аутентификации, контроля доступом; политик и моделей безопасности; технической защиты информации; организационно-правового обеспечения информационной безопасности.

УДК 004.056.5(075.8)
ББК 32.97я73

ISBN 978-5-9275-3571-2 (Ч. 1)
ISBN 978-5-9275-3526-2

1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

Ключевыми терминами в понятии *информационная безопасность* являются *информация* и *безопасность*.

Термин *информация* разные науки определяют различными способами. Так, например, в философии информация рассматривается как свойство материальных объектов и процессов сохранять и порождать определённое состояние, которое в различных вещественно-энергетических формах может быть передано от одного объекта к другому. В кибернетике информацией принято называть меру устранения неопределённости, хаоса. В современных информационных технологиях для обработки информации главным образом используются вычислительные машины. В этом ракурсе под информацией в дальнейшем будем понимать всё то, что может быть представлено в символах конечного (например, бинарного) алфавита.

Основными потребительскими качествами информации являются: репрезентативность, содержательность, достаточность, доступность, актуальность, своевременность, точность, достоверность и устойчивость.

Понятие *безопасность* нашло свое отражение в Федеральном законе «О безопасности» от 28.12.2010 № 390-ФЗ (ред. от 05.10.2015). Безопасность – это состояние защищенности жизненно важных интересов личности, общества, государства от внутренних и внешних угроз [1].

К жизненно важным интересам закон относит совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства. Основные объекты безопасности – личность, ее права и свободы; общество – его материальные и духовные ценности; государство – его конституционный строй, суверенитет и территориальная ценность.

Понятие *информационная безопасность* в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности Российской Федерации (РФ) термин «информационная безопасность» используется в широком смысле как состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства [2].

В свою очередь, под *защищенностью* понимается совокупность правовых, научно-технических, организационных мер, направленных на своевременное выявление, предупреждение и пресечение неправомерного получения и распространения защищаемой информации.

В более узком плане под *информационной безопасностью* следует понимать защиту интересов субъектов информационных отношений.

Субъект – это активный компонент информационной системы (ИС), который обращаясь к пассивному компоненту ИС – объекту (источнику информации), может порождать потоки информации от объекта к субъекту или изменять состояния ИС.

Субъекты информационных отношений заинтересованы в обеспечении [3]:

– своевременного доступа (за приемлемое время) к необходимой информации;

– конфиденциальности (сохранения в тайне) определенной части информации;

– достоверности (полноты, точности, адекватности, целостности) информации;

– защиты от навязывания им ложной (недостоверной, искаженной) информации (дезинформации);

– защиты определенной части информации от ее незаконного тиражирования (защита авторских прав, прав собственника информации);

– разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;

– возможности осуществления непрерывного контроля и управления процессами получения, обработки и передачи информации.

Объект является пассивным компонентом ИС, который принимает, хранит или передает содержащуюся в нем информацию. Доступ субъекта к объекту означает доступ к содержащейся в нем информации [4].

Объектами, подлежащими защите в смысле обеспечения информационной безопасности, являются:

- информация и информационные ресурсы;
- носители информации;
- процессы обработки информации.

Таким образом, с методологической точки зрения обеспечение информационной безопасности сводится к выявлению субъектов информационных отношений и их интересов по использованию информационных ресурсов. Причем для разных категорий субъектов трактовка проблем, связанных с информационной безопасностью, может существенно различаться. Так, в режимных государственных организациях в плане обеспечения информационной безопасности главным является безусловное сохранение секретов, т.е. предотвращение несанкционированного доступа (НСД) к информации. В то же время в различных не режимных организациях, занимающихся обработкой информации не конфиденциального характера, на первом плане стоят целостность (неискаженность) информации, работоспособность и безотказность ИС. То есть субъект информационных отношений может пострадать не только от НСД к закрытой информации, но и от ее искажения и ограниченной доступности.

В контексте информационных отношений под информационной безопасностью 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 [5].

Деятельность, направленную на обеспечение информационной безопасности, принято называть защитой информации.

Следует обратить внимание, что в определении информационной безопасности фигурирует понятие «неприемлемый ущерб». Это означает, что застраховаться от всех видов ущерба невозможно, и тем более невозможно сделать это экономически целесообразным способом, при котором стоимость защитных средств будет меньше размера возможного ущерба. Из этого вытекает важный вывод: защитные меры следует применять только от тех возможных угроз, реализация которых приведет к недопустимому ущербу (нанесение вреда жизни и здоровью людей, состоянию окружающей среды, финансовому состоянию предприятия, стабильности его функционирования). Следовательно, правилом создания информационной защиты является уменьшение размеров ущерба до приемлемого уровня.

Информационные ресурсы определяются как отдельные документы и массивы документов, представленные самостоятельно или в различных информационных системах (библиотеках, архивах, фондах, базах данных и др.).

Информационные ресурсы можно классифицировать:

- *по виду информации* – правовые, научно-технические, политические, финансово-экономические, статистические, метрологические, социальные, персональные, медицинские, о чрезвычайных ситуациях и т.п.;
- *режиму доступа* – открытые, ограниченного доступа, государственная тайна, конфиденциальная информация, коммерческая тайна, профессиональная тайна, служебная тайна, персональная тайна и др.;
- *форме собственности* – государственные, федеральные, муниципальные, коллективные, частные;
- *виду носителя* – на бумаге (документы, письма, медицинские карты, телефонные справочники организаций, черновики и распечатки); – на экране, в памяти ИС, в канале связи, на гибких и жестких магнитных дисках и на других носителях.

Носителями информации могут также являться отдельные знающие люди, которые бесспорно владеют важной информацией (эксперты), а также специально завербованные, внедренные или даже случайные информаторы – осведомители.

Важнейшим в сфере информационной безопасности является понятие угрозы. В глобальном смысле *угрозы безопасности* – это совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

В сфере информационной безопасности угрозы – это потенциальные или реально существующие возможности негативного влияния на процесс использования информационных технологий. (Угрозы информационной безопасности более подробно будут рассмотрены в следующем разделе данного учебного пособия).

В контексте угроз информационной безопасности под «информационной безопасностью» понимается состояние защищенности всей информационной сферы (предприятия, организации, общества, государства) от внутренних и внешних угроз.

В современных условиях информация преимущественно принимается, обрабатывается, хранится и передается с использованием информационно-вычислительных систем – компьютеров. Компьютеры, оснащенные специализированными аппаратными и программными средствами, являются лишь составной частью, технической базой, инструментом ИС, обслуживаемой персоналом и связанной с обширной поддерживающей инфраструктурой. В этой связи следует различать понятия «компьютерная безопасность» и «информационная безопасность». Понятие «компьютерная безопасность» обозначает состояние безопасности самих компьютеров, т.е. технической базы, предназначенной для приема, обработки, хранения и передачи информации. В то же время, согласно определению информационной безопасности, она зависит не только от компьютеров, но и от *поддерживающей инфраструктуры*, к которой можно отнести средства коммуникации, системы электро-, водо- и теплоснабжения, вентиляции, кондиционирования, охранной и пожарной сигнализации, радиофикации и др. и, что очень важно, обслуживающий персонал. Эта обширная инфраструктура имеет самостоятельную ценность и значимость, но в рамках данного пособия она будет учитываться только в ракурсе того, как она влияет на выполнение ИС предписанных им функций.

При использовании информационных ресурсов возникают три аспекта, по которым следует рассматривать защиту информации:

- обеспечение конфиденциальности информации;
- обеспечение целостности информации;
- обеспечение доступности информационных ресурсов и поддерживающей инфраструктуры.

Конфиденциальность (от лат. confidentia, от англ. confidence – доверие) – это необходимость предотвращения разглашения, утечки какой-либо информации, т.е. защита от НСД к информации.

К конфиденциальной информации относится та информация, доступ к которой ограничен федеральными законами. Цели у ограничений разные. Например, защита основ конституционного строя, нравственности, здоровья, прав и законных интересов некоторых лиц, обеспечение обороны страны и безопасности государства. В РФ конфиденциальность определяется как обязательное для выполнения лицом, получившим доступ к опре-

деленным сведениям, требование не передавать их третьим лицам, без согласия лица, создавшего информацию, либо получившего на законном основании право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Целостность – это актуальность и непротиворечивость информации, ее защищенность от несанкционированного изменения и разрушения.

Целостность информации можно рассматривать как статическую в смысле ее неизменности как информационного объекта и динамическую, означаемую корректное ее изменение как информационного объекта (транзакции) [6].

Доступность – это возможность за приемлемое время получить требуемую информационную услугу.

Если по каким-то причинам ИС не в состоянии предоставить пользователям законные услуги, то это наносит ущерб соответствующим субъектам информационных отношений [6].

Степень важности каждой из трех составляющих информационной безопасности в итоге определяется характером и видом деятельности организаций в сфере информационных отношений.

С правовой точки зрения при обеспечении информационной безопасности можно выделить три основных принципа.

Принцип обоснованности заключается в установлении необходимости ограничения доступа к какой-либо информации с учетом вероятных последствий такого ограничения, исходя из баланса жизненно важных интересов личности, общества и государства.

Принцип своевременности защиты информации заключается в правильной временной раскладке процедур ограничения доступа к защищаемой информации с момента ее разработки, получения или заблаговременно.

Принцип прогноза информационной безопасности заключается в анализе угроз охраняемой информации, объективной оценке степени ее необходимой защиты, оценке всей инфраструктуры, участвующей в обработке охраняемой информации, моделировании возможной противоправной деятельности по отношению к охраняемой информации.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных:

– на соблюдение конфиденциальности информации ограниченного доступа;

– обеспечение защиты информации от НСД, ее уничтожения, модифицирования, блокирования, несанкционированного копирования, предоставления и распространения и прочих неправомерных действий в отношении защищаемой информации;

– реализацию права на правомерный доступ к информации [7].

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований по защите информации и ответственности за нарушение этих требований.

Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

Правонарушения в сфере информационных технологий и защиты информации влекут за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ.

Обеспечение безопасности приема, обработки, хранения и передачи информации в ИС достигается проведением определенной политики информационной безопасности.

Под *политикой информационной безопасности* понимают совокупность требований, норм, правил, рекомендаций, регламентирующих работу средств защиты ИС от заданного множества угроз безопасности.

Система защиты информации – совокупность применяемых требований, норм, мер, мероприятий, обеспечивающих реальную защищенность информации в ИС согласно с принятой политикой безопасности [8].

Другими словами, политика информационной безопасности – это то, что требуется для обеспечения ИС, а система защиты информации – это то, что реализовано в соответствии принятой политикой безопасности.

Информационная безопасность – важнейшая составляющая интегральной безопасности на всех уровнях – национальном, отраслевом, корпоративном или персональном. В Доктрине информационной безопасности РФ обеспечение безопасности информационных и телекоммуникационных систем выделено в качестве важной составляющей национальных интересов РФ в информационной сфере [8].

2. УГРОЗЫ И УЯЗВИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Обеспечение информационной безопасности конкретной ИС строится, как правило, на этапе, предшествующем вводу ее в эксплуатацию. Методология обеспечения информационной безопасности ИС представляет собой комплексный анализ, включающий пять взаимосвязанных этапов:

1. Анализ и идентификация возможных источников угроз в конкретных условиях эксплуатации данной ИС.
2. Анализ уязвимостей ИС, которые могут способствовать реализации угроз, выявленных на этапе 1.
3. Анализ возможных последствий реализации угроз, выявленных на этапе 1.
4. Выделение актуального перечня угроз, реализация которых может принести неприемлемый ущерб для владельца ИС (физическое или юридическое лицо).
5. Формулирование политики безопасности ИС.

На рис. 2.1 показана логическая цепочка обеспечения безопасности ИС.

Рис. 2.1. Логическая цепочка обеспечения безопасности ИС

Основными понятиями, фигурирующими в процессе обеспечения безопасности ИС, являются: угрозы, уязвимости, последствия и политика безопасности.

Под *угрозой* понимают потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию или другие компоненты ИС может прямо или косвенно привести к нанесению ущерба интересам владельца ИС.

Уязвимость – это наличие в ИС потенциально возможных способов нарушения безопасности информации, обусловленные недостатками архитектуры, программного обеспечения, аппаратных средств, интерфейса, протоколов обмена, условий эксплуатации, ошибками обслуживающего персонала.

Последствия – это возможный негативный результат реализации угроз через имеющиеся в ИС уязвимости, приводящий к нарушению информационной безопасности.

Источники угроз – это потенциальные объективные явления или действия субъектов-злоумышленников, приводящие к нарушению информационной безопасности.

2.1. Классификация источников угроз информационной безопасности

Источники угроз информационной безопасности по происхождению делятся на три основные группы: антропогенные, техногенные и стихийные [8].

Антропогенные источники обусловлены человеческим фактором. Это действия субъектов, которые могут привести к нарушению информационной безопасности. Эти действия могут быть как умышленными, так и случайными, могут исходить как извне (из сетевой среды), так и из внутренней среды организации, от людей, имеющих прямое или косвенное отношение к обработке информации. Действия этой категории источников поддаются прогнозированию, что позволяет в большинстве случаев своевременно принять адекватные меры защиты. Группа антропогенных источников показана на рис. 2.2.

Техногенные источники. Они обусловлены некачественным функционированием основных технических средств, имеющих непосредственное отношение к обработке информации, а также различных вспомогательных технических средств, обеспечивающих необходимые условия для нормального функционирования основных средств, персонала и пользователей. Эти источники угроз лишь частично прогнозируемы в рамках сертификации основных и вспомогательных средств и уровня квалификации основного и вспомогательного персонала. Техногенные источники угроз информационной безопасности могут быть как внутренними, так и внешними. Группа техногенных источников показана на рис. 2.3.

Рис. 2.2. Группа антропогенных источников

Рис. 2.3. Группа техногенных источников

Стихийные источники. Данную группу обычно составляют различные природные катаклизмы и форс-мажорные обстоятельства. Эти источники носят объективный и абсолютный характер, составляющий непреодолимую силу. Стихийные источники невозможно предусмотреть и предотвратить или возможно предусмотреть, но невозможно предотвратить. В большинстве случаев такие источники угроз не поддаются прогнозированию. Это приводит к тому, что меры против их возможного проявления должны предусматриваться всегда. Стихийные источники, как правило, являются внешними по отношению к защищаемому объекту.

Группа стихийных источников показана на рис. 2.4.

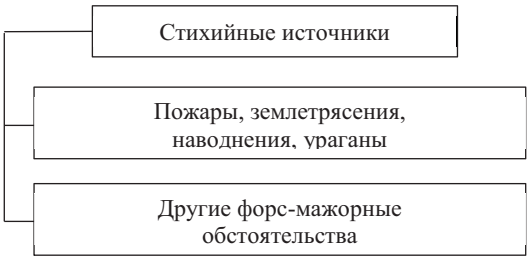

Рис. 2.4. Группа стихийных источников

В информационной безопасности утвердилось следующее определение угроз безопасности информации.

Под угрозами безопасности информации понимаются потенциальные или реально возможные действия по отношению к информационной сфере, приводящие к несанкционированным нарушениям основных свойств информации – конфиденциальности, целостности и доступности.

По механизму реализации и конечному проявлению можно выделить следующие угрозы безопасности информации:

- ознакомление;
- модификация;
- уничтожение;
- блокирование.

Конкретные реализации угроз безопасности информации называют *сценариями угроз информации*.

Соответствие свойств информации и угроз ее безопасности показано рис. 2.5.

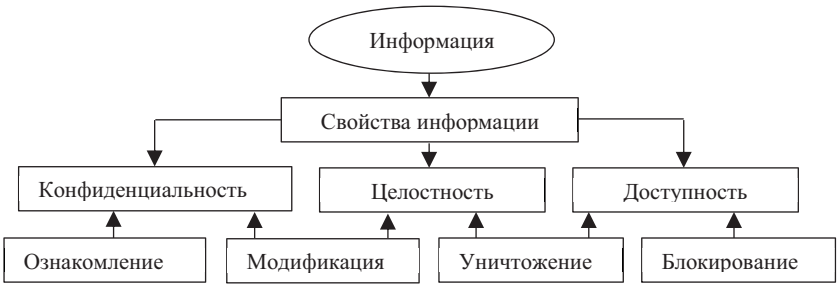

Рис. 2.5. Соответствие свойств информации и угроз ее безопасности

Ознакомление с конфиденциальной информацией может проходить различными путями и способами, при этом существенным является отсутствие изменений самой информации.

Если ознакомление с конфиденциальной информацией произошло лицами, для которых она не предназначалась, то это расценивается как нарушение свойства конфиденциальности информации. При этом степень конфиденциальности информации и круг лиц, имеющих доступ к ней, определяет владелец этой информации. Нарушение конфиденциальности информации происходит также при несанкционированном изменении грифа конфиденциальности (секретности).

Модификация информации означает изменение ее состава и содержания и, возможно, степени ее конфиденциальности (секретности) вследствие подмены сведений. При этом происходит нарушение свойств целостности и конфиденциальности информации. Модификация информации не приводит к ее полному уничтожению.

Уничтожение информации приводит к ее полному разрушению и утрате без возможности восстановления. При этом происходит нарушение свойств целостности и доступности информации.

Блокирование информации приводит к ее недоступности для субъектов, имеющих право доступа к этой информации. При этом происходит нарушение свойства доступности информации.

Перечисленные угрозы могут осуществляться в любые моменты и в любом сочетании с нарушением свойств конфиденциальности, целостности и доступности информации, что приводит к нарушению установленного режима доступа к данным и в итоге – к моральным и (или) материальным потерям.

СОДЕРЖАНИЕ