Московский государственный технический университет
имени Н.Э. Баумана

В.В. Бондарев

Введение в информационную безопасность автоматизированных систем

Учебное пособие

BAUMANPRESS
Москва
ИЗДАТЕЛЬСТВО
МГТУ им. Н. Э. Баумана
2016

УДК 681.326
ББК 67.408
Б81

Издание доступно в электронном виде на портале *ebooks.bmstu.ru*
по адресу: http://ebooks.bmstu.ru/catalog/117/book1425.html

Факультет «Информатика и системы управления»
Кафедра «Информационная безопасность»

Рекомендовано
Редакционно-издательским советом
МГТУ им. Н.Э. Баумана в качестве учебного пособия

Рецензент
канд. юрид. наук, доцент *Б.Н. Коробец*

Бондарев, В. В.

Б81 Введение в информационную безопасность автоматизированных систем : учебное пособие / В. В. Бондарев. — Москва : Издательство МГТУ им. Н. Э. Баумана, 2016. — 250, [2] с. : ил.

ISBN 978-5-7038-4414-4

Рассмотрена законодательная база информационной безопасности, приведен перечень возможных угроз, отражены основные подходы к созданию систем защиты информации, представлена классификация предупредительных мер, изучены вопросы, связанные с программно-аппаратными механизмами обеспечения информационной безопасности.

Для студентов, обучающихся по направлению подготовки «Информационная безопасность», по специальности «Информационная безопасность автоматизированных систем» и слушателей факультета повышения квалификации. Может быть полезно студентам и аспирантам других специальностей, интересующимся современными средствами и методами обеспечения информационной безопасности.

УДК 681.326
ББК 67.408

ISBN 978-5-7038-4414-4

ПРЕДИСЛОВИЕ

Цель учебного пособия — ознакомление студентов с основами комплексного подхода к обеспечению информационной безопасности (ИБ) автоматизированных систем (АС), проблемами защиты информации и подходами к их решению.

В пособии рассмотрены:

• теоретические и правовые вопросы защиты информации и обеспечения безопасности АС;

• принципы построения комплексных систем защиты АС;

• основные направления деятельности служб технической защиты информации (подразделений обеспечения безопасности АС);

• современная технология обеспечения безопасности АС, предусматривающая рациональное распределение функций и организацию эффективного взаимодействия по вопросам защиты информации сотрудников всех подразделений, которые используют АС в процессе работы и гарантируют ее функционирование;

• вопросы разработки нормативно-методических и организационно-распорядительных документов, необходимых для реализации технологии обеспечения безопасности АС;

• разработка защищенных АС;

• проектирование системы управления информационной безопасностью АС;

• разработка модели угроз и модели нарушителя информационной безопасности АС;

• организация эксплуатации АС с учетом требований информационной безопасности;

• восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций.

Для лучшего усвоения материала студентам необходимо иметь представление о современных информационных технологиях и автоматизированных системах управления, о правовых, организационных и технических аспектах проблемы обеспечения информационной безопасности.

После изучения данного пособия студент должен

➤ *знать:*

• основные угрозы безопасности информации и модели нарушителя в АС;

• АС как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;

• содержание и порядок деятельности персонала по эксплуатации защищенных АС;

• законодательные акты в области защиты информации;

• основные задачи подразделения защиты информации;

• основные меры по защите информации в АС (организационные, правовые, программно-аппаратные, физические, технологические);

• основные защитные механизмы, применяемые в АС;

➤ *уметь:*

• разрабатывать модели угроз и нарушителей в АС;

• анализировать и оценивать риски информационной безопасности;

• разрабатывать структуру системы обеспечения безопасности АС;

• классифицировать уязвимости АС;

• правильно выбирать средства защиты АС;

➤ *иметь навыки:*

• использования основных защитных механизмов подсистем безопасности АС;

• разработки системы организационно-распорядительных и нормативно-методических документов по защите информации;

• определения требований к защите и категорирования ресурсов АС;

• применения штатных и дополнительных средств защиты информации от несанкционированного доступа (НСД);

• построения инфраструктуры управления событиями.

РАЗДЕЛ I

ОСНОВЫ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Глава 1. АКТУАЛЬНОСТЬ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Автоматизированные системы, в состав которых входят информационные технологии (ИТ), основанные на новейших разработках в области средств вычислительной техники (СВТ) и связи, находят все более широкое применение практически во всех сферах жизни и деятельности (в отличие от индустриальных технологий, где основным объектом переработки являются сырье и материалы, информационные технологии «потребляют» и «перерабатывают» информацию). С развитием ИТ объемы обрабатываемой и передаваемой информации, как в абсолютных значениях, так и по отношению к объемам переработки сырья и материалов в индустриальных технологиях, непрерывно возрастают.

1.1. Место и роль автоматизированных систем в управлении бизнес-процессами

Почему же современные компьютеры и средства телекоммуникации так широко востребованы? Что они умеют делать, что становятся необходимыми практически везде? В ответ на эти вопросы, как правило, можно услышать: «Компьютеры позволяют автоматизировать умственный труд». Но разве физический труд они не автоматизируют и как объяснить понятие «умственный труд»?

Ответим на поставленные вопросы. Компьютерные технологии дают возможность автоматизировать процессы управления (умственный труд по управлению — по принятию решений в конкретных ситуациях на основе имеющейся информации). А поскольку управление необходимо везде, всегда и всем, то и средства автоматизации управления применяются повсеместно. Автоматизация на основе современных ИТ позволяет принимать решения более оперативно и

характерные только для них специфические каналы проникновения в систему, что объясняется целым рядом их о с о б е н н о с т е й , среди которых:

• территориальная разнесенность компонентов АС и наличие интенсивного обмена информацией между ними;

• широкий спектр способов представления, хранения и передачи информации;

• интеграция данных, принадлежащих различным субъектам, в рамках единых баз данных и, наоборот, размещение необходимых некоторым субъектам данных в удаленных узлах сети;

• абстрагирование владельцев данных от физических структур и места размещения данных;

• использование режимов распределенной обработки данных;

• участие в процессе автоматизированной обработки информации большого количества пользователей и персонала;

• непосредственный и одновременный доступ к ресурсам (в том числе и информационным) большого числа пользователей;

• разнородность средств вычислительной техники и связи, а также их программного обеспечения;

• отсутствие специальных средств защиты в большинстве типов технических средств, широко используемых в АС.

* * *

Трудности решения практических задач обеспечения безопасности конкретных АС связаны с отсутствием развитой стройной теории и необходимых научно-технических и методических основ обеспечения защиты информации в современных условиях.

Применяемые в настоящее время большинством организаций меры не обеспечивают необходимого уровня безопасности субъектов, участвующих в процессе информационного взаимодействия, и не способны в необходимой степени противостоять разного рода воздействиям в целях доступа к критичной информации и дезорганизации работы автоматизированных систем.

Контрольные вопросы

1. Охарактеризуйте место и роль автоматизированных систем в управлении бизнес-процессами.

2. Какие факторы определяют актуальность проблемы защиты АС в современных условиях?

3. Перечислите особенности современных автоматизированных систем как объектов защиты.

4. Назовите причины обострения проблемы обеспечения информационной безопасности.

5. Почему проблема обеспечения безопасности АС относится к числу трудноразрешимых?

6. Что понимается под риском информационной безопасности? Каковы составляющие риска?

7. В чем заключается анализ рисков и управление ими? Перечислите этапы анализа и управления.

8. Каковы требования к методам оценки целесообразности затрат на обеспечение безопасности АС?

9. Назовите категории затрат, связанных с безопасностью АС; кратко охарактеризуйте каждую категорию и перечислите статьи расходов для каждой из них.

ГЛАВА 2. ОСНОВНЫЕ ПОНЯТИЯ В ОБЛАСТИ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Прежде всего, необходимо понять, что же такое безопасность АС и определить *что (кого), от чего (от кого), почему (зачем), как (в какой степени и какими средствами) надо защищать*. Получив четкие ответы на данные вопросы, можно правильно сформулировать общие требования к системе обеспечения безопасности АС и перейти к обсуждению проблем построения соответствующих систем защиты. Основные понятия безопасности и их взаимосвязь приведены в ГОСТ Р ИСО/МЭК15408-1–2012 «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий».

2.1. Определение безопасности автоматизированных систем

Что же такое безопасность вообще и безопасность АС в частности? Нередко можно слышать, что безопасность — это отсутствие опасностей. Данное определение не совсем верно, поскольку полностью устранить все возможные опасности нельзя.

Безопасность — это защищенность от опасностей, более точно, защищенность от возможного ущерба, наносимого при реализации этих опасностей (угроз).

Различают материальный, моральный и физический ущерб. Ущерб может быть причинен как напрямую, так и косвенно. *Субъектами нанесения ущерба, в конечном счете, всегда являются люди*. Даже если пострадают материальные объекты или информационные ресурсы, косвенный ущерб, проблемы возникнут у пользователей, каким-либо образом связанных с этими объектами или заинтересованных в их сохранности и целостности. И чем с бóльшим числом объектов человека что-то связывает, тем в большей опасности для косвенного нанесения ущерба он находится.

Косвенный ущерб интересам пользователя может быть нанесен либо путем сбоя нормального функционирования автоматизированной системы, либо за счет нарушения необходимых свойств отдельных компонентов и ресурсов АС, среди которых не только непосредственно информация, но и ее носители (устройства хранения, обработки, передачи данных), а также процессы обработки и передачи информации.

В этом смысле защита информации от несанкционированного доступа — только часть общей проблемы обеспечения безопасности компьютерных систем и защиты законных интересов субъектов информационных отношений, а сам термин НСД точнее было бы трактовать не как «несанкционированный доступ» (к информации), а шире, — как «несанкционированные (неправомерные) действия», наносящие ущерб субъектам информационных отношений.

* * *

С развитием возможностей новых информационных технологий компьютерным системам поручается решение все более объемных, сложных, важных и ответственных задач, поэтому актуальность проблемы обеспечения безопасности применяемых информационных технологий в дальнейшем будет только возрастать.

Контрольные вопросы

1. Что понимается под безопасностью вообще и безопасностью АС в частности?
2. Дайте определение АС и безопасности АС.
3. Приведите определения информации и информационных ресурсов.
4. Перечислите категории субъектов информационных отношений.
5. Охарактеризуйте три свойства информации — конфиденциальность, целостность и доступность.
6. Сформулируйте цели защиты АС и циркулирующей в ней информации.

Глава 3. УГРОЗЫ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Один из важнейших аспектов проблемы обеспечения безопасности АС — определение, анализ и классификация возможных угроз безопасности АС. Перечень значимых угроз, оценка вероятностей их реализации, а также модель нарушителя служат основой для проведения анализа рисков и формулирования требований к системе защиты АС.

3.1. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем

Автоматизированная система состоит из следующих основных структурно-функциональных э л е м е н т о в :

• *рабочих станций* — отдельных ЭВМ (персональных ЭВМ — ПЭВМ) или терминалов сети, на которых реализуются автоматизированные рабочие места (АРМ) пользователей (абонентов, операторов);

• *серверов* или *host-машин* (служб файлов, печати, баз данных и т. п.) не выделенных (или выделенных, т. е. не совмещенных с рабочими станциями)

из 254 опрошенных по всему миру первых лиц компаний, причем бóльшую часть проблем (83 %) создают сами сотрудники корпораций.

Сотрудники компании являются самой массовой категорией нарушителей в силу их многочисленности, наличия у них санкционированного доступа на территорию, в помещения и к ресурсам системы, разнообразия мотивов совершения разного рода небезопасных действий. Причем подавляющее большинство нарушений со стороны сотрудников неумышленного характера. Однако, ущерб, который они при этом наносят компании, весьма значителен. Именно поэтому борьба с ошибками пользователей и обслуживающего персонала АС — одно из основных направлений работы по обеспечению безопасности.

* * *

Итак, цель защиты ИТ — минимизация рисков для субъектов. Защита (обеспечение безопасности) ИТ — это непрерывный процесс управления рисками, связанный с выявлением информационных активов (ценностей), подлежащих защите, определением стоимости этих активов, размеров ущерба и риска, разработкой плана действий по защите и выбором технологий, реализующих этот план.

На практике это означает сведение всех значимых для субъектов угроз к допустимому (приемлемому) уровню остаточного риска и защиту наиболее важных (критичных) информационных ресурсов, исходя из существующих возможностей и предоставленных финансовых средств.

Уязвимыми являются буквально все основные структурно-функциональные элементы современных АС. Защищать компоненты АС необходимо от всех видов воздействий: стихийных бедствий и аварий, сбоев и отказов технических средств, ошибок персонала и пользователей, ошибок в программах и от преднамеренных действий злоумышленников.

Имеется широчайший спектр вариантов преднамеренного или случайного несанкционированного доступа к данным и вмешательства в процессы обработки и обмена информацией (в том числе, управляющей согласованным функционированием различных компонентов сети).

Правильно построенная модель нарушителя, в которой отражаются его практические и теоретические возможности, время, место действия и другие характеристики — важная составляющая успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты.

Контрольные вопросы

1. Дайте определение понятий «угроза», «уязвимость» и «атака».
2. Какие классификационные схемы угроз ИБ вам известны?
3. Перечислите источники угроз ИБ.
4. Назовите каналы проникновения в автоматизированную систему и утечки информации.
5. Какие факторы лежат в основе формирования модели нарушителя?
6. Каковы цели разработки моделей угроз и нарушителей?
7. В чем разница между нарушителем и злоумышленником?

Глава 4. МЕРЫ И ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

В данной главе рассмотрены меры противодействия угрозам безопасности АС (контрмеры), а также основные принципы построения систем защиты информации. Здесь будет дан ответ на вопрос: «Как защищать ресурсы АС?»

4.1. Виды мер противодействия угрозам безопасности

По способам осуществления меры защиты информации, а также ее носителей и систем обработки подразделяют на следующие виды:

- законодательные;
- морально-этические;
- организационные;
- физические;
- технические (аппаратные и программные).

Законодательные меры включают в себя указы, постановления, законы, руководящие документы и другие нормативно-правовые акты, которые определяют нормы обращения с информацией, права и обязанности участников информационных отношений и устанавливают ответственность за несоблюдение данных норм.

Морально-этические меры предполагают соблюдение норм поведения, которые традиционно сложились в обществе или формируются по мере распространения информационных технологий. Данные нормы не обязательны к применению, как требования нормативных актов, однако, их несоблюдение может нередко привести к снижению престижа компании.

Организационные меры — меры административного характера, которые устанавливают правила функционирования системы обработки данных и деятельности обслуживающего персонала, а также порядок их взаимодействия для снижения вероятности осуществления угроз безопасности или потерь в случае их реализации. К организационным мерам относят надлежащую охрану территории объекта, соблюдение требований разграничения доступа, формирование дисциплины и ответственности сотрудников и др.

Технологические меры предусматривают такие технологические решения и приемы, которые основаны на принципе избыточности (структурной, функциональной, информационной, временно́й и т. п.) и направлены на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках мандатного доступа (например, двойной ввод ответственной информации, инициализация ответственных операций только при наличии разрешений от нескольких должностных лиц, процедура проверки соответствия реквизитов исходящих и входящих сообщений в системах коммутации сообщений, периодическое подведение общего баланса всех банковских счетов и т. п.).

Меры физической защиты на основе механических, электромеханических и электронно-механических устройств позволяют создавать физические препят-

* * *

Таким образом, специалисты по информационной безопасности располагают широким спектром защитных мер: законодательных, морально-этических, административных (организационных), физических и технических. Предпринимаемые меры имеют как достоинства, так и недостатки, которые необходимо знать и правильно учитывать при создании систем защиты.

Все известные каналы проникновения и утечки информации должны быть перекрыты с учетом анализа риска, вероятностей реализации угроз безопасности в конкретной прикладной системе и обоснованного рационального уровня затрат на защиту.

Наилучшие результаты достигаются при системном подходе к вопросам безопасности компьютерных систем и комплексном использовании различных мер защиты на всех этапах жизненного цикла системы, начиная с самых ранних стадий ее проектирования.

Контрольные вопросы

1. Перечислите основные виды мер противодействия угрозам безопасности АС (контрмер).
2. Охарактеризуйте каждую меру противодействия.
3. Какая мера противодействия является, на ваш взгляд, наиболее важной, а какая — второстепенной?
4. Перечислите достоинства и недостатки различных мер защиты.
5. Возможно ли создание идеально надежной системы защиты?
6. Перечислите основные принципы построения систем защиты информации. Какие из них, по вашему мнению, являются важнейшими? Кратко охарактеризуйте каждый принцип.

Глава 5. ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Современный этап развития системы обеспечения информационной безопасности государства и общества характеризуется переходом от тотального сокрытия большого объема сведений к гарантированной защищенности принципиально важных данных, обеспечивающей:

- конституционные права и свободы граждан, предприятий и организаций в сфере информатизации;
- необходимый уровень безопасности информации, подлежащей защите;
- защищенность систем формирования и использования информационных ресурсов (технологий, систем обработки и передачи данных).

В *Стратегии развития информационного общества в Российской Федерации*, утвержденной Указом Президента РФ от 07.02.2008 № 212 одной из основных задач, требующих решения для формирования и развития инфор-

* * *

Развитие информационного общества в Российской Федерации базируется на принципах минимизации рисков и угроз национальной безопасности России, связанных с враждебным и преступным использованием возможностей информационно-коммуникационных технологий, укреплением доверия и безопасности при их использовании.

Правительство Российской Федерации регулирует требования к обеспечению безопасности данных и отдельных граждан (персональных данных) при их обработке, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Контрольные вопросы

1. Приведите классификацию информации по доступности с точки зрения Федерального закона «Об информации, информационных технологиях и о защите информации».
2. Дайте определения обладателя информации и оператора информационной системы.
3. Перечислите права и обязанности обладателя информации.
4. Дайте определение понятия «коммерческая тайна» в соответствии с Федеральным законом «О коммерческой тайне».
5. Какая информация не может быть отнесена к коммерческой тайне?
6. Каким нормативным актом утвержден Перечень сведений конфиденциального характера?
7. В каком кодексе предусмотрена ответственность за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)?
8. В каком кодексе предусмотрена ответственность за «незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»?
9. Какие статьи Уголовного кодекса РФ определяют ответственность за преступления в сфере компьютерной информации?
10. С какого возраста предусмотрена уголовная ответственность за преступления в сфере компьютерной информации?
11. В какой статье Уголовного кодекса РФ определяется ответственность за создание, использование и распространение вредоносных программ для ЭВМ ?
12. Что такое лицензирование?
13. Какие виды лицензирования вам известны?
14. Для кого аттестация АИС по требованиям безопасности информации ФСТЭК России является обязательной?
15. Когда проводится аттестация АИС по требованиям безопасности информации ФСТЭК России?
16. Перечислите классы защищенности СВТ в соответствии с руководящими документами ФСТЭК России.
17. Перечислите классы защищенности АС в соответствии с руководящими документами ФСТЭК России.
18. Какие подсистемы включает в себя комплекс программно-технических средств защиты информации от НСД в АС?

Глава 6. ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Структура государственной системы защиты информации в Российской Федерации, ее задачи и функции, основы организации защиты сведений, отнесенных к государственной или служебной тайне, определены в Положении о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденном *постановлением Совета Министров — Правительства Российской Федерации от 15.09.1993 № 912-51.*

Этот документ обязателен для выполнения при проведении работ по защите информации, содержащей сведения, составляющие государственную или служебную тайну, в органах государственной власти (представительной, исполнительной и судебной властей Российской Федерации, республик в составе Российской Федерации, автономной области, автономных округов, краев, областей, городов Москвы и Санкт-Петербурга) и в органах местного самоуправления, на предприятиях, в учреждениях и организациях независимо от их организационно-правовой формы и формы собственности.

Работы по защите информации в органах государственной власти и на предприятиях проводятся на основе актов законодательства Российской Федерации путем выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий в целях уничтожения или искажения информации в процессе обработки, передачи и хранения, по противодействию иностранным техническим разведкам, а также за счет проведения специальных работ, порядок организации и выполнения которых определяются Правительством Российской Федерации.

6.1. Главные направления работ по защите информации

Мероприятия по защите информации — составная часть управленческой, научной и производственной деятельности — осуществляются во взаимосвязи с другими мерами по обеспечению установленного режима секретности проводимых работ.

Главные направления работ по защите информации:

- обеспечение эффективного управления системой защиты информации;
- определение сведений, охраняемых от технических средств разведки, и демаскирующих признаков, раскрывающих эти сведения;
- анализ и оценка реальной опасности перехвата информации техническими средствами разведки, несанкционированного доступа, разрушения (уничтожения) или искажения путем преднамеренных программно-технических воздействий в процессе ее обработки, передачи и хранения в технических средствах, выявление возможных технических каналов утечки сведений, подлежащих защите;

6.5. Финансирование мероприятий по защите информации

Финансирование мероприятий по защите информации, содержащей сведения, отнесенные к государственной или служебной тайне, а также подразделений по защите информации в органах государственной власти и на бюджетных предприятиях предусматривается в сметах расходов на их содержание.

Обеспечение техническими средствами защиты информации, не требующее капитальных вложений, осуществляется в пределах средств, выделяемых заказчиком на научно-исследовательские и опытно-конструкторские работы, связанные с разработкой продукции. Расходы по разработке технических средств защиты включаются в стоимость разработки образца продукции.

Создание технических средств защиты информации, требующее капитальных вложений, осуществляется в пределах средств, выделяемых заказчиком на строительство (реконструкцию) сооружений или объектов.

* * *

Ключевым моментом политики государства в области обеспечения АС является осознание необходимости защиты любых информационных ресурсов и информационных технологий, неправомерное обращение с которыми может нанести ущерб их обладателю (собственнику, владельцу, пользователю) или иному лицу.

Соответствие технического средства и его программного обеспечения требованиям защищенности подтверждается сертификатом, выдаваемым предприятием, имеющим лицензию на этот вид деятельности.

Информация, содержащая сведения, отнесенные к государственной или служебной тайне, должна обрабатываться с использованием либо защищенных систем и средств информатизации и связи, либо технических и программных средств защиты, сертифицированных в установленном порядке.

Контрольные вопросы

1. Назовите главные направления работ по защите информации.
2. Перечислите основные организационно-технические мероприятия в области защиты информации.
3. В чем заключаются основные задачи государственной системы защиты информации?
4. Какова структура государственной системы защиты информации?
5. Каковы цели защиты информации?
6. В чем заключается контроль состояния защиты информации?
7. Каковы источники финансирования мероприятий по защите информации?

РАЗДЕЛ II

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Глава 7. ОРГАНИЗАЦИОННАЯ СТРУКТУРА СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Проблемы безопасности АС каждой конкретной организации «не уникальны», поэтому приведенная далее технология управления безопасностью информации и ресурсов в автоматизированной системе носит универсальный характер, поскольку в ней обобщен опыт специалистов многих организаций и стран.

Целью создания системы обеспечения безопасности информационных технологий является достижение заданного уровня информационной безопасности организации (предприятия), чтобы предотвратить или минимизировать ущерб, наносимый субъектам информационных отношений посредством нежелательного воздействия на информацию, ее носители и процессы обработки.

Основная задача системы защиты — обеспечение необходимого уровня доступности, целостности и конфиденциальности компонентов АС соответствующими методами и средствами.

7.1. Технология управления безопасностью информации и ресурсов в автоматизированной системе

Как уже отмечалось, обеспечение безопасности АС есть процесс управления рисками, следовательно, система защиты — это система управления, реализующая технологию обеспечения безопасности (управления безопасностью). Любая технология предусматривает определенный набор операций и процессов взаимодействия их исполнителей, направленный на достижение конечного результата (цели).

закрепляющие требования по обеспечению информационной безопасности при работе в АС и ответственность сотрудников за реализацию мер по обеспечению установленного режима защиты информации.

* * *

Задачи организации и функции по обеспечению безопасности ИТ, ее подразделений и сотрудников должны формулироваться в документах с учетом положений действующего в России законодательства по информатизации и защите информации (федеральных законов, указов Президента Российской Федерации, постановлений Правительства Российской Федерации и других руководящих и нормативно-методических документов).

Организационные (административные) меры регламентируют процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности.

Четкое знание и строгое соблюдение всеми сотрудниками, использующими и обслуживающими аппаратные и программные средства АС, требований организационно-распорядительных документов по вопросам обеспечения безопасности информации, а также персональная ответственность за свои действия дают возможность поддерживать безопасность АС на необходимом уровне.

Контрольные вопросы

1. Что понимается под технологией обеспечения безопасности информации и ресурсов в АС?
2. Каковы условия для реализации технологий обеспечения безопасности информации и ресурсов в АС?
3. Какова цель создания системы обеспечения безопасности АС?
4. Охарактеризуйте влияние на состояние безопасности АС различных категорий сотрудников.
5. Перечислите основные организационные и организационно-технические мероприятия по созданию и обеспечению функционирования комплексной системы защиты.
6. В чем заключается политика безопасности организации?

Глава 8. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ И ОТВЕТСТВЕННЫХ ЗА ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПОДРАЗДЕЛЕНИЯХ

Пользователь автоматизированной системы является важнейшим информационным ресурсом АС, который реализует критичные функции, настраивает ПО, хранит пароли, управляет безопасностью ИТ. Система безопасности ИТ должна обеспечить защиту АС от нарушений со стороны конечных поль-

В случае перевода сотрудника на другую работу, увольнения и иных обстоятельствах он обязан сдать (сразу по окончании последнего сеанса работы) персональный ключевой носитель ответственному за обеспечение безопасности подразделения под роспись в журнале учета ключевых носителей, который информирует об этом уполномоченного сотрудника ЦУКС для принятия действий по блокированию использования ЭП увольняемого сотрудника.

Уничтожение ключей осуществляют двумя способами: 1) физическим уничтожением ключевого носителя, на котором он расположен; 2) стиранием (разрушением) ключей без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

Ключевые носители уничтожаются либо исполнителями (только принадлежащие им ключи), либо ответственными за обеспечение безопасности ИТ под роспись в соответствующих журналах. Централизованное уничтожение ключей по акту производит комиссия, состоящая из сотрудников ЦУКС и ответственного за обеспечение безопасности ИТ.

* * *

Сотрудники — пользователи АС должны знать и строго выполнять правила работы со средствами защиты информации, установленными на его рабочей станции, надежно хранить и никому не передавать свои пароли, личные печати и ЭП; немедленно информировать ответственного за обеспечение безопасности ИТ подразделения о некорректном функционировании технических средств защиты.

Контрольные вопросы

1. Каковы общие правила обеспечения безопасности информационных технологий при работе сотрудников с ресурсами АС?
2. Перечислите права и обязанности ответственного за обеспечение безопасности ИТ в подразделении.
3. Что такое явная и неявная компрометация ключей шифрования?
4. Какие действия должен предпринять сотрудник при компрометации ключей?
5. Каков порядок уничтожения ключей шифрования?

ГЛАВА 9. РЕГЛАМЕНТАЦИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Допуск сотрудников подразделений к работе с автоматизированной системой и доступ к ее ресурсам должен быть строго регламентирован. Аппаратно-программная конфигурация автоматизированных рабочих мест, на которых обрабатывается защищаемая информация и с которых возможен доступ к защищаемым ресурсам, должна соответствовать кругу возложенных на сотрудников (пользователей данного АРМ) функциональных обязанностей.

разделения-заказчика участвуют в разработке специальных требований по обеспечению безопасности ИТ в должностных инструкциях пользователей АС.

Взаимодействия подразделений в процессе эксплуатации (сопровождения). Изменения настроек средств защиты в соответствии с утвержденными заявками на изменение полномочий пользователей осуществляют специалисты, системные администраторы и администраторы безопасности, отвечающие за эксплуатацию соответствующих подсистем (комплексов задач).

Изменения в конфигурацию аппаратно-программных средств подсистемы (в том числе при снятии задач с эксплуатации и передаче аппаратных средств в ремонт) вносят специалисты подразделений эксплуатации и технического сопровождения на основании утвержденных и согласованных с подразделением обеспечения безопасности ИТ заявок (заданий) от руководителей операционных подразделений в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы организации».

В экстренных случаях (в кризисных ситуациях) основанием для принятия решений специалистами подразделений эксплуатации и технического сопровождения является План обеспечения непрерывной работы и восстановления (ПОНРВ).

* * *

Конечные пользователи (специалисты операционных подразделений) при работе с АС руководствуются должностными инструкциями и инструкцией пользователя по вопросам обеспечения безопасности ИТ и должны соблюдать правила парольной и антивирусной защиты.

Правильность функционирования и настройки системы защиты периодически контролируется специалистами подразделений эксплуатации (системными администраторами), а также специалистами подразделения обеспечения безопасности ИТ (администраторами информационной безопасности).

Физическая охрана объектов информации предусматривает организацию и обеспечение визуального и технического контроля за контролируемой территорией объекта защиты, установку механических, кодовых и электронных замков и др.

Контрольные вопросы

1. Каковы требования к пользовательским паролям?
2. Перечислите недостатки парольной аутентификации.
3. Какова периодичность плановой смены пароля?
4. В каких случаях проводится неплановая смена пароля?
5. Охарактеризуйте в общих чертах требования к технологии антивирусной защиты.
6. Опишите алгоритм действий при обнаружении вирусов.
7. Дайте определение авторизации.
8. Что устанавливается в рамках разрешительной системы (системы авторизации)?

9. Опишите алгоритм авторизации пользователя.

10. Какие сотрудники участвуют в процессе авторизации пользователя?

11. Какова процедура авторизации?

12. Каковы цели изготовления копий заявки об авторизации?

13. Что включает в себя физическая охрана объектов информатизации?

14. Опишите процедуру внесения изменений в конфигурацию аппаратных и программных средств защищенных серверов и рабочих станций системы.

15. Какие категории сотрудников имеют право внесения изменений в системное и прикладное ПО?

16. Кто имеет право вносить изменения в конфигурацию аппаратно-программных средств защиты?

17. Каков порядок экстренной модификации технических средств?

18. Кто определяет требования к характеристикам средств защиты в разрабатываемых подсистемах?

19. Что такое фонд алгоритмов и программ?

20. Опишите порядок взаимодействия подразделений на этапах проектирования, разработки, испытания и внедрения новых автоматизированных подсистем.

Глава 10. КАТЕГОРИРОВАНИЕ И ДОКУМЕНТИРОВАНИЕ ЗАЩИЩАЕМЫХ РЕСУРСОВ

Наибольшую сложность при решении вопросов обеспечения безопасности информационных технологий представляет задача определения требований к защите конкретной информации, ее носителей и процессов обработки. Ключом к решению данной задачи для общего случая служит учет интересов всех затрагиваемых технологией субъектов информационных отношений.

10.1. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов

Сложившийся подход к классификации государственной информации (данных) по уровням требований к ее защищенности основан на рассмотрении и обеспечении только одного свойства информации — ее конфиденциальности (грифа секретности). Требования по обеспечению целостности и доступности информации, как правило, лишь косвенно фигурируют среди общих требований к системам обработки этих данных. Считается, что поскольку к информации имеет доступ узкий круг доверенных лиц, вероятность ее искажения (несанкционированного уничтожения) незначительна.

Если такой подход в некоторой степени оправдан в силу существующей приоритетности свойств безопасности важной государственной информации, то это вовсе не означает, что его механический перенос в другую предметную область (с другими субъектами и их интересами) будет иметь успех.

защиты (полномочия доступа групп пользователей к перечисленным ресурсам задачи). Эти сведения будут использованы в качестве эталона настроек средств защиты соответствующих компьютеров, на которых будет решаться данная задача, и для контроля правильности их установки;

3. Категорирование компьютеров. Категория компьютера устанавливается исходя из максимальной категории специальных задач, решаемых на нем, и максимальных категорий конфиденциальности и целостности информации, используемой при решении данных задач. Информацию о категории компьютера (триаду) заносят в его формуляр.

* * *

В ходе обследования конкретных подразделений организации и автоматизированных подсистем выявляются и анализируются все функциональные задачи, решаемые с использованием АС, а также все виды информации (сведений), применяемые при решении этих задач в подразделениях. Одновременно с этим ведется учет программных средств (общих, специальных), с помощью которых решают функциональные задачи подразделения.

При составлении перечня и формуляров функциональных задач, решаемых в организации, необходимо выяснять периодичность их решения, максимально допустимое время задержки получения результатов решения задач и степень серьезности последствий, к которым могут привести нарушения их доступности (блокирование возможности решения задач). В случае невозможности количественной оценки вероятного ущерба проводится качественная оценка.

Контрольные вопросы

1. Каков примерный порядок определения требований к защищенности циркулирующей в системе информации?
2. Что необходимо учитывать при определении уровня возможного ущерба?
3. Перечислите цели категорирования ресурсов.
4. Приведите примеры категорий защищаемой информации и функциональных задач.
5. Опишите порядок проведения информационного обследования и документирования защищаемых ресурсов.

Глава 11. КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ПЛАНЫ ЗАЩИТЫ И ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОЙ РАБОТЫ И ВОССТАНОВЛЕНИЯ ПОДСИСТЕМ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

Концепция информационной безопасности организации (далее – Концепция) определяет порядок обеспечения безопасности информации в орга-

Для *полного восстановления подсистемы* следует:

• восстановить работоспособность всех поврежденных аппаратных средств, при необходимости произвести замену отказавших узлов и блоков резервными;

• восстановить и настроить все поврежденные программы, используя эталонные (страховые) копии;

• восстановить все поврежденные данные, используя страховые копии и журналы транзакций;

• настроить средства защиты подсистемы в соответствии с планом защиты информации;

• уведомить администратора системы (базы данных) о результатах восстановления.

Далее необходимо провести расследование причин возникновения кризисной ситуации и ответить на вопросы:

• случайная или преднамеренная кризисная ситуация;

• учитывалась ли возможность возникновения кризисной ситуации в плане защиты информации и плане обеспечения непрерывной работы и восстановления подсистем АС;

• можно ли было ее предусмотреть;

• вызвана ли она слабостью средств защиты и регистрации;

• превысил ли ущерб от нее установленный уровень;

• есть ли невосполнимый ущерб и велик ли он;

• это первая кризисная ситуация такого рода;

• есть ли возможность точно определить круг подозреваемых лиц;

• есть ли возможность точно установить виновника;

• какова причина возникновения кризисной ситуации и др.

Ответственным за расследование является администратор безопасности подсистемы. Отчет о результатах расследования и предложениях по совершенствованию системы направляют администратору системы (базы данных) и руководству организации.

* * *

Концепция информационной безопасности организации разрабатывается на основе нормативно-правовой базы, регламентирующей вопросы защиты информации в АС и служит руководящим документом при формировании политики безопасности в организации. Планы защиты информации и обеспечения непрерывной работы и восстановления подсистем АС составляют для конкретизации положений Концепции информационной безопасности.

Контрольные вопросы

1. Каково назначение Концепции информационной безопасности?
2. Какие факторы учитываются при разработке Концепции?
3. Что служит правовой основой для разработки Концепции?
4. Какие вопросы отражены в Концепции?

5. Охарактеризуйте статус Концепции.

6. Охарактеризуйте цель разработки и содержание плана защиты информации.

7. Охарактеризуйте цель разработки и содержание плана обеспечения непрерывной работы и восстановления.

8. Что такое кризисная ситуация?

9. Назовите категории кризисных ситуаций.

10. Перечислите меры обеспечения непрерывной работы и восстановления работоспособности подсистем АС.

11. Приведите перечень обязанностей и действий персонала по обеспечению непрерывной работы и восстановлению работоспособности подсистем АС.

РАЗДЕЛ III

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Глава 12. НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

В зависимости от вида мер противодействия угрозе безопасности АС (правовые, морально-этические, организационные и др., см. гл. 4) применяют различные защитные механизмы.

12.1. Основные механизмы защиты автоматизированных систем

Для защиты АС от НСД к информации используются следующие механизмы:

- идентификация (именование и распознавание) и аутентификация (подтверждение подлинности) пользователей системы;
- разграничение доступа пользователей к ресурсам системы и авторизация (присвоение полномочий) пользователей;
- регистрация и оперативное оповещение о событиях, происходящих в системе;
- криптографическое шифрование хранимых и передаваемых по каналам связи данных;
- контроль целостности и аутентичности (подлинности и авторства) данных;
- резервирование и резервное копирование;
- фильтрация трафика и трансляция адресов;
- обнаружение вторжений (атак);
- выявление и нейтрализация компьютерных вирусов;
- затирание остаточной информации на носителях;
- выявление уязвимостей «слабых мест» системы;

К параметрам, влияющим на ставку страхования, относят:

• стоимость застрахованных ресурсов;

• используемые средства защиты —чем известнее система защиты, тем ниже ставка страхования;

• статистика атак для аналогичных организаций отрасли.

* * *

Таким образом, универсальные механизмы защиты, которыми располагают специалисты по безопасности, обладают как достоинствами, так и недостатками, и могут применяться в различных вариациях и совокупностях в конкретных методах и средствах защиты. Повышать уровень стойкости системы защиты за счет применения более совершенных физических и технических средств можно только до уровня стойкости персонала из ядра безопасности системы. Успех или неудача масштабного применения систем защиты информации зависит от наличия в них развитых средств управления режимами работы защитными механизмами и реализации функций, позволяющих существенно упрощать процессы установки, настройки и эксплуатации средств защиты.

Контрольные вопросы

1. Назовите этапы идентификации и аутентификации. В чем их различие и как они связаны между собой?

2. Приведите примеры различных идентификаторов и аутентификаторов пользователя.

3. Что понимают под авторизацией пользователя?

4. Перечислите недостатки парольных подсистем идентификации и аутентификации.

5. Перечислите основные виды угроз парольных подсистем идентификации и аутентификации.

6. Приведите примеры технических устройств, с помощью которых может решаться задача идентификации пользователя.

7. Приведите примеры технических устройств, с помощью которых может решаться задача идентификации и аутентификации пользователя.

8. Перечислите основные задачи, решаемые криптографией.

9. Опишите традиционные симметричные криптосистемы и укажите их недостатки.

10. Сколько секретных ключей используется при взаимном обмене зашифрованными (симметричным алгоритмом) сообщениями двух сторон?

11. Что понимают под ЭП?

12. Какой ключ используется для формирования ЭП почтового сообщения?

13. Что понимают под инфраструктурой открытых ключей?

14. Как осуществляется защита периметра компьютерных сетей и каковы основные средства защиты?

15. Какие события относят к страховым случаям?

Глава 13. АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

С момента создания и начала функционирования системы сертификации средств защиты информации по требованиям безопасности информации ФСТЭК России было сертифицировано несколько десятков СЗИ НСД. Далее будут приведены рекомендации по выбору СЗИ НСД, рассмотрены некоторые из существующих на рынке СЗИ НСД (полный перечень сертифицированных средств защиты информации опубликован на сайте ФСТЭК России).

13.1. Рекомендации по выбору средств защиты информации от несанкционированного доступа

Выбор средств защиты информации зависит от потребности организации в определенном уровне защищенности автоматизированной системы, количества компьютеров, их технических характеристик, применяемых операционных систем и других факторов.

При выборе соответствующих уровню защищенности АС конкретных средств защиты необходимо пользоваться руководящими документами ФСТЭК России: 1) Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации; 2) Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.

Защищенность СВТ определяется их способностью предотвращать или существенно затруднять НСД к информации при использовании СВТ в составе АС.

Защита АС и СВТ обеспечивается комплексом программно-технических средств (КСЗ) и соответствующих организационных мер.

Требования ФСТЭК России к защищенности АС приведены в табл. 13.1, СВТ — в табл. 13.2.

Таблица 13.1

Распределение показателей защищенности по классам для автоматизированных систем

Подсистемы и требования	Класс защищенности								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1. Подсистема управления доступом									
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:									
в систему	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	-	-	+	-	+	+	+	+
к программам	-	-	-	+	-	+	+	+	+
1.2. Управление потоками информации	-	-	-	+	-	-	+	+	+

Эффективное использование данного инструмента возможно в том случае, если соблюдаются еще, по крайней мере, два условия, требующие организационных мер. Для пользователей внутренними нормативными документами организации установлен запрет на передачу своих реквизитов входа другому лицу либо их запись в доступном для других лиц месте (классический пример — стикер с паролем, наклеенный на монитор). Другой возможный вариант — разработка некоторой бюрократической процедуры передачи реквизитов входа, с тем чтобы по соответствующим данным бумажного учета можно было однозначно установить, какой сотрудник воспользовался указанной учетной записью в данный момент.

Контрольные вопросы

1. Какие факторы влияют на выбор конкретных средств защиты информации?
2. Что определяет класс защищенности АС или СВТ?
3. Сколько и какие подсистемы образуют систему защищенности АС?
4. Охарактеризуйте классы защищенности СВТ.
5. Каковы критерии выбора СЗИ от НСД?
6. Какие СЗИ от НСД вам известны?
7. Перечислите задачи, решаемые средствами аппаратной поддержки систем защиты информации от НСД.
8. Охарактеризуйте существующие средства аппаратной поддержки.
9. Какие устройства аутентификации на базе смарт-карт и/или USB-токенов вам известны?
10. Каков алгоритм аутентификации пользователя с использованием OTP-токена?
11. Что понимается под биометрической аутентификацией пользователя? Приведите примеры биометрических характеристик.
12. Назовите основные отличия методов биометрической аутентификации пользователя от других (например, парольных).

Глава 14. ПРИМЕНЕНИЕ ШТАТНЫХ И ДОПОЛНИТЕЛЬНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Рассмотренные в гл. 13 средства идентификации и аутентификации позволяют решить только одну из задач, возлагаемых на СЗИ НСД, — задачу защиты от вмешательства посторонних лиц в процессы нормального функционирования АС. После того, как сеанс работы пользователя начат либо разблокирован, вступают в действие другие защитные механизмы, реализованные в составе штатных средств ОС и дополнительных средствах защиты от НСД, позволяющие, при соблюдении определенных условий (при внедрении необходимых организационных мер), решить остальные задачи по защите АС.

• подключения удаленных пользователей или малых офисов;

• передачи конфиденциальной информации в ЛВС от нарушителей, не являющихся пользователями автоматизированных систем, но имеющих доступ к ЛВС и/или нарушителей-пользователей, не имеющих необходимых полномочий.

* * *

Сервер безопасности, кроме работы с клиентами (агентами), должен обеспечивать взаимодействие со средствами централизованного управления и оперативного контроля, размещаемыми на компьютерах администраторов безопасности.

Изменение различных составляющих управляющей информации производится по-разному: одна часть информации корректируется централизованно (в групповых политиках) с рабочего места администратора, другая — децентрализованно (в локальной политике безопасности) с соответствующих рабочих станций. В локальной политике безопасности для корректировки доступны только те параметры, которые не заданы через групповые политики. Для параметров СЗИ действуют те же правила наследования, что и для стандартных настроек, назначаемых через групповые политики.

Контрольные вопросы

1. Охарактеризуйте стратегию безопасности Microsoft.
2. Какие сертифицированные ФСТЭК России решения Microsoft в области безопасности вам известны? Охарактеризуйте их.
3. Каковы направления работы компании Microsoft в области биометрии?
4. Какие подходы к разграничению доступа пользователей вам известны? Кратко опишите их.
5. Опишите алгоритм работы AD RMS.
6. Какова схема работы ACS?
7. Какие средства шифрования позволяют обеспечить защиту данных от копирования и перехвата?

РАЗДЕЛ IV

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

Глава 15. ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ

В настоящее время корпоративные компьютерные сети играют важную роль в деятельности большинства организаций. Многие из них подключены к глобальной сети — Интернет. Если раньше сеть Интернет объединяла небольшое число людей, доверявших друг другу, то в настоящее время количество ее пользователей составляет уже сотни миллионов. В связи с этим все серьезнее становится угроза внешнего вмешательства в процессы нормального функционирования корпоративных сетей и несанкционированного доступа к их ресурсам со стороны злоумышленников — так называемых хакеров.

15.1. Типовая корпоративная сеть

Сеть организации может быть как изолированной от внешнего мира (что весьма условно), так и иметь соединение с другими сетями, например с Интернетом.

Подключение к сетям общего пользования осуществляется организациями для решения следующих задач:

- обеспечить внутренним пользователям доступ к внешним ресурсам www-ресурсам, FTP-архивам и т. п.;
- предоставить доступ пользователям из внешней сети к некоторым внутренним ресурсам (корпоративному веб-серверу, FTP-серверу и т. д.);
- обеспечить взаимодействие с удаленными филиалами и отделениями;
- организовать доступ к ресурсам внутренней сети мобильных пользователей.

При решении перечисленных задач у руководства организации возникают проблемы, связанные с безопасностью (например, проблема разграничения доступа пользователей к ресурсам). Предоставление всеобщего доступа

код, например обеспечивающий удаленное управление узлом (так называемый reverse shell);

3) нарушитель незаметно для пользователя выполняет подключение к своему узлу, возможно происходит загрузка дополнительных модулей вредоносного программного обеспечения, и получает контроль над объектом атаки.

15.5. Средства защиты сетей

Для защиты корпоративной сети обычно используется комплекс средств безопасности, реализующий основные защитные механизмы и состоящий из нескольких подсистем:

- защиты рабочих станций и серверов от НСД;
- межсетевого экранирования при необходимости с выделением отдельной подсистемы защищенного доступа к ресурсам сети Интернет;
- криптографической защиты сетевого трафика;
- антивирусной защиты;
- анализа защищенности;
- обнаружения атак.

* * *

В основе функционирования всемирной сети Интернет лежат стандарты IP-сетей. Огромный потенциал IP- и интернет-технологий только начинает использоваться. Все бóльшую популярность приобретает технология передачи голоса поверх IP (Voice over IP, VoIP), для связи между офисами все шире применяются виртуальные частные сети. Электронная коммерция из абстрактного понятия все более превращается в реальность.

Контрольные вопросы

1. Охарактеризуйте уровни информационной инфраструктуры корпоративной сети.
2. Дайте определения угрозы, уязвимости и атаки. Охарактеризуйте на примерах взаимосвязь между этими понятиями.
3. Приведите классификационные схемы уязвимостей и атак.
4. Какой из механизмов реализации сетевых атак наиболее сложен с точки зрения обнаружения?
5. Какой из механизмов реализации сетевых атак не подразумевает использования какой-либо уязвимости?
6. Какие средства защиты сетей вам известны?

Глава 16. ЗАЩИТА ПЕРИМЕТРА КОРПОРАТИВНОЙ СЕТИ

Периметр корпоративной сети должен быть защищен и в то же время иметь взаимодействие с окружающим миром.

Возможными точками взаимодействия с окружающим миром могут быть:

• точка подключения к сети Интернет;

• выделенные каналы, соединяющие филиалы друг с другом или обеспечивающие взаимодействие с сетями партнеров;

• клиентские приложения, нередко имеющие постоянное соединение с ресурсами, расположенными в недоверенных сетях;

• сегменты, обеспечивающие удаленный доступ к сети, включая доступ посредством виртуальных частных сетей (Virtual Private Network, VPN);

• беспроводные сегменты, позволяющие нарушать границы сети на физическом и канальном уровнях.

Виртуальные частные сети позволяют предоставить удаленным мобильным пользователям, где бы они ни находились, безопасный доступ к корпоративным ЛВС, а партнерам и клиентам — безопасный доступ к определенным внутренним информационным ресурсам организации за счет создания криптографически защищенных туннелей для пересылки данных из одной конечной точки в другую.

В современных условиях границы сетей становятся все более «размытыми». Иногда говорят, что точка периметра находится на границе между двумя сетями с разными политиками безопасности. Возможные названия этих областей приведены на рис. 16.1.

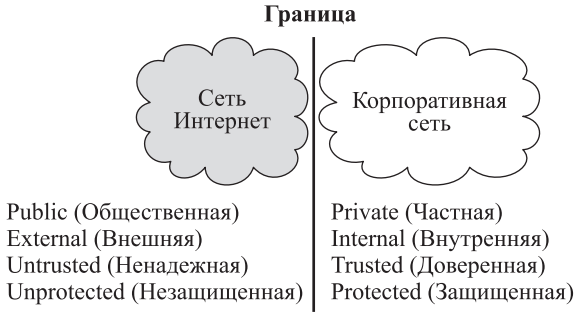

Рис. 16.1. Граница между двумя сетями с разными политиками безопасности

На рис. 16.2 перечислены каналы, через которые в корпоративную сеть может попасть какая-либо информация или, наоборот, уйти из нее.

Разумеется, информация может попасть в сеть (или «уйти» из нее) и через различные портативные устройства (флэш-карты, диски и т. п.), однако эти вопросы касаются физической безопасности и в рамках данного курса не рассматриваются.

МЭ с технологией «stateful inspection»), которые должны быть сертифицированы в соответствии с требованиями ФСТЭК России или ФСБ России.

Дополнительный контроль циркулирующей в системе информации необходим для почтового и веб-трафика.

При выборе средств для построения VPN прежде всего необходимо обращать внимание на следующие вопросы: какой протокол туннелирования поддерживает криптографический модуль (межсетевой экран, криптошлюз и т. п.), какие криптографические алгоритмы используются для шифрования, какие механизмы сжатия туннелируемых данных применяются, какова способность системы работать с отдельным удаленным пользователем.

Контрольные вопросы

1. Почему необходимо защищать периметр корпоративной сети?
2. Перечислите составляющие механизма защиты периметра сети.
3. Что такое демилитаризованная зона в применении к компьютерным сетям?
4. Дайте определение понятия межсетевого экрана. В чем заключается его функция?
5. Перечислите основные типы межсетевых экранов. Охарактеризуйте функции МЭ каждого типа, их достоинства и недостатки.
6. В чем состоит главный недостаток пакетных фильтров — разновидности межсетевых экранов?
7. В чем разница между обычным пакетным фильтром и пакетным фильтром с контролем состояния «stateful»?
8. В чем разница между пакетным фильтром с контролем состояния «stateful» и классическим посредником сеансового уровня?
9. Каковы особенности анализа содержимого электронной почты?
10. Перечислите критерии фильтрации содержимого электронной почты.
11. Каковы особенности анализа содержимого HTTP-трафика?

ГЛАВА 17. ОБНАРУЖЕНИЕ И УСТРАНЕНИЕ УЯЗВИМОСТЕЙ. ВОЗМОЖНОСТИ СКАНЕРОВ БЕЗОПАСНОСТИ

Подсистема управления уязвимостями представляет собой комплекс организационно-технических мероприятий, направленных на предотвращение использования известных уязвимостей, потенциально существующих в защищаемой системе или сети. В частности, в рамках управления уязвимостями проводятся такие мероприятия, как периодический мониторинг защищенности информационных систем и устранение обнаруженных уязвимостей.

17.1. Управление уязвимостями

Контроль состояния защищенности относится к категории так называемых превентивных защитных механизмов, главное назначение которых —

• поиском файлов или ключей реестра, свидетельствующих о наличии в узле того или иного приложения (вируса и т. п.);

• сравнением текущих значений параметров конфигурации с требуемыми значениями (в этом случае пользователь должен задать эти значения, которые обычно являются частью политики безопасности).

* * *

Для обнаружения и устранения уязвимостей применяют сканеры безопасности сетевого и системного уровня, грань между которыми весьма тонка (многие проверки, выполняемые сетевыми сканерами, доступны системным сканерам).

Сканеры уровня узла используют только пассивные методы идентификации уязвимостей, поскольку их, как правило, устанавливают на важном сервере и они должны оказывать на него минимальное влияние.

Контрольные вопросы

1. В чем особенности распределенной архитектуры систем управления уязвимостями?
2. Какие задачи могут быть решены сетевым сканером безопасности?
3. Перечислите типы проверок, используемых в сетевых сканерах безопасности
4. Какую дополнительную критичную информацию может получить злоумышленник в результате сканирования портов?
5. Какая причина затрудняет использование в организациях сетевых сканеров безопасности?

Глава 18. МОНИТОРИНГ СОБЫТИЙ БЕЗОПАСНОСТИ

Среди многочисленных перечисленных ранее механизмов защиты имеются два, которые направлены на выявление случаев удачных и неудачных попыток нарушений безопасности, т. е. относящихся к категории «детективных» (позволяющих как можно более оперативно зафиксировать факт атаки):

• регистрация и оперативное оповещение о событиях безопасности;

• обнаружение атак.

И в том, и другом случае накапливается информация о событиях безопасности, анализ которой позволяет выявить факты совершения нарушений, характер воздействий на систему, определить степень нарушения, метод расследования, способы поиска нарушителя и исправления ситуации.

18.1. Введение в управление журналами событий

Регистрация событий безопасности обычно предполагает их размещение в каком-либо журнале.

признаков атак. К данному виду относится бóльшая часть систем обнаружения атак;

• на базе узла (host-based) — системы, ориентированной на защиту отдельного узла (в некоторых случаях удобнее поместить систему обнаружения атак непосредственно на защищаемом узле). Входными данными для таких систем являются журналы регистрации и действий пользователей защищаемого узла.

Классификация по технологии обнаружения показывает, произошла атака или нет:

• обнаружение злоупотреблений (Misuse Detection) — известен перечень атак;

• обнаружение аномалий (Anomaly Detection) — известно поведение контролируемого объекта и любое отклонение считается атакой.

Данными для построения *профиля поведения* могут служить:

• объемы трафика;

• отношения между узлами и группами узлов;

• архив потоков данных.

* * *

В журналах фиксируются события, которые происходят на уровне операционной системы или отдельного приложения с различными сетевыми устройствами. Многообразие журналов требует управления ими. Инфраструктура управления журналами реализует дополнительные функции, связанные с обнаружением атак на систему по различным признакам. Методы анализа информации об атаках позволяют использовать разнообразные механизмы реагирования, такие как оповещение, блокировка и др.

Контрольные вопросы

1. Дайте определение инфраструктуры управления журналами событий.
2. Перечислите категории журналов событий.
3. Дайте характеристику протоколов syslog и SEM.
4. Опишите классификационные схемы систем обнаружения атак.
5. Какие механизмы реагирования на атаки вам известны?

ГЛОССАРИЙ

Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники.

Авторизация – предоставление аутентифицированному субъекту соответствующих (предписанных установленным порядком) прав на доступ к объектам системы: какие данные и как он может использовать (какие операции с ними осуществлять), какие программы может выполнять, когда, как долго и с каких терминалов может работать, какие ресурсы системы может использовать и т. п.

Авторизованный субъект доступа – субъект, которому предоставлены соответствующие права доступа к объектам системы (полномочия).

Аппаратные шифровальные (криптографические) средства — устройства и их компоненты, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации без использования программ для электронных вычислительных машин.

Аттестация объектов информатизации — комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных уполномоченными федеральными органами исполнительной власти.

Аутентификация — проверка (подтверждение) подлинности идентификации субъекта или объекта системы.

Блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Владелец сертификата ключа проверки электронной подписи — лицо, которому в установленном законом порядке выдан сертификат ключа проверки электронной подписи.

Доступ к информации — ознакомление с информацией (чтение, копирование, модификация (корректировка), уничтожение (удаление) и т. п.).

ЛИТЕРАТУРА

Бабаш А.В., Баранова Е.К., Мельников Ю.Н. Информационная безопасность. Лабораторный практикум. М.: КноРус, 2013. 136 с.

Будаковский Д.С. Способы совершения преступлений в сфере компьютерной информации // Российский следователь. 2011. № 4.

Волков П.П. Экспертный анализ методов защиты информации от утечки по техническим каналам // Эксперт-криминалист. 2009. № 4.

Воронцова С.В. Киберпреступность: проблемы квалификации преступных деяний. Российская юстиция. 2011. № 2.

Воротников В.Л. О правовой защите компьютерной информации // Администратор суда. 2009. № 2.

Гафнер В.В. Информационная безопасность. Ростов н/Д: Феникс, 2012. 324 с.

Громов Ю.Ю., Драчев В.О., Иванова О.Г. Информационная безопасность и защита информации. Ст. Оскол: ТНТ, 2013. 384 с.

Забегайло Л.А., Назарова И.А. Актуальные вопросы охраны коммерческой тайны в отношениях с органами государства // Современное право. 2011. № 7.

Загузов Г.В. Административно-правовые средства обеспечения информационной безопасности и защиты информации в Российской Федерации // Административное и муниципальное право. 2010. № 5.

Кузнецова Т.В. Организация работы с персональными данными // Трудовое право. 2011. № 5.

Маркарьян Р.В. Об основных направлениях совершенствования законодательства о развитии Интернета в Российской Федерации // Международное публичное и частное право. 2011. № 4.

Палехова Е.А. Конфиденциальная информация и институт персональных данных в банковской деятельности // Предпринимательское право. 2010. № 3.

Партыка Т.Л., Попов И.И. Информационная безопасность. М.: Форум, 2012. 432 с.

Петренко С.А., Курбатов В.А. Политики информационной безопасности. М.: Компания АйТи. 2006. 400 с.

Петров С.В., Слинькова И.П., Гафнер В.В. Информационная безопасность. АРТА, 2012. 296 с.

Савчишкин Д.Б. Административная ответственность как средство обеспечения информационной безопасности // Административное и муниципальное право. 2011. № 6.

Семененко В.А. Информационная безопасность. М. 2010. 277 с.

Станскова У.М. Правовой анализ локальных нормативных актов работодателя по защите информации ограниченного доступа // Трудовое право в России и за рубежом. 2011. № 2.

Терещенко Л.К. О соблюдении баланса интересов при установлении мер защиты персональных данных // Журн. российского права. 2011. № 5.

Чеботарева А.А. Электронное государственное управление как новая форма взаимоотношений личности, общества и государства // Государственная власть и местное самоуправление. 2011. № 6.

Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. М.: ИД «ФОРУМ, ИНФРА-М», 2013. 416 с.

Ярочкин В.И. Информационная безопасность. М.: Акад. Проект, Гаудеамус, 2008. 544 с.

[Электронный ресурс] Internet Security Glossary, Version 2 (http://www.ietf.org/rfc/rfc4949.txt)

[Электронный ресурс] Benchmarking Terminology for Firewall Performance (http://www.ietf.org/rfc/rfc2647.txt)

[Электронный ресурс] Behavior of and Requirements for Internet Firewalls (http://www.ietf.org/rfc/rfc2979.txt)

[Электронный ресурс] http://aluigi.altervista.org/adv/termdd_1-adv.txt

ПРИЛОЖЕНИЕ

НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные законы

Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.).

О Декларации прав и свобод человека и гражданина (принята Постановлением Верховного Совета РСФСР от 22 ноября 1991 № 1920-1).

Доктрина информационной безопасности Российской Федерации» (утв. Президентом РФ 09 сентября 2000 г. №Пр-1895).

Уголовный кодекс Российской Федерации (принят Федеральным законом от 13 июня 1996 г. № 63-ФЗ).

Кодекс Российской Федерации об административных правонарушениях (принят Федеральным законом от 30 декабря 2001 г. №195-ФЗ).

Гражданский кодекс Российской Федерации (принят Федеральным законом от 18 декабря 2006 г. № 230-ФЗ).

Трудовой кодекс Российской Федерации (принят Федеральным законом от 30 декабря 2001 г. № 197-ФЗ).

Воздушный кодекс Российской Федерации (принят Федеральным законом от 19 марта 1997 г. № 60-ФЗ).

Федеральные законы

Закон Российской Федерации от 02 декабря 1990 г. № 395-1 «О банках и банковской деятельности».

Закон Российской Федерации «Об организации страхового дела в Российской Федерации» от 27 ноября 1992 г. № 4015-I.

Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г. № 5485-1.

Федеральный закон «О Федеральной службе безопасности» от 03 апреля 1995 г. № 40-ФЗ .

Федеральный закон «Об оперативно-розыскной деятельности» от 12 августа 1995 г. №144-ФЗ.

Федеральный закон «О техническом регулировании» от 27 декабря 2002 г. № 184-ФЗ.

Федеральный закон «О связи» от 07 июля 2003 г. № 126-ФЗ .

Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ.

Федеральный закон «О государственной гражданской службе Российской Федерации» от 27 июля 2004 г. № 79-ФЗ.

Федеральный закон «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» от 19 декабря 2005 г. № 160-ФЗ.

Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ.

Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ .

Федеральный закон «О муниципальной службе в Российской Федерации» от 02 марта 2007 г. № 25-ФЗ. (Ст. 29. Персональные данные муниципального служащего).

Федеральный закон «О безопасности» от 28 декабря 2010 г. № 390-ФЗ .

Федеральный закон «Об электронной подписи» от 6 апреля 2011 г. № 63-ФЗ.

Федеральный закон «О лицензировании отдельных видов деятельности» от 04 мая 2011 г. № 99-ФЗ .

Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «Об информации, информационных технологиях и о защите информации» от 11 июля 2011 г. № 200-ФЗ.

Федеральный закон «О бухгалтерском учете» от 06 декабря 2011 г. № 402-ФЗ.

Федеральный закон «О внесении изменений в части первую, вторую и четвертую Гражданского кодекса Российской Федерации и отдельные законодательные акты Российской Федерации» от 12 марта 2014 г. № 35-ФЗ.

Указы Президента Российской Федерации

Указ Президента Российской Федерации от 03 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации (с изм. Указа Президента Российской Федерации от 25 июля 2000 г. № 1358)».

Указ Президента Российской Федерации от 06 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с изм. от 23 сентября 2005 г. № 1111).

Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

Указ Президента Российской Федерации от 30 мая 2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».

Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Указ Президента Российской Федерации от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года».

Постановления Правительства Российской Федерации

Постановление Правительства РСФСР от 05 декабря 1991 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну».

Постановление Совета Министров – Правительства Российской Федерации от 15 сентября 1993 г. № 912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» (Извлечения).

Постановление Правительства Российской Федерации от 03 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».

Постановление Правительства Российской Федерации от 06 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Постановление Правительства Российской Федерации от 16 марта 2009 г. № 228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

Постановление Правительства Российской Федерации от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям».

Постановление Правительства Российской Федерации от 04 марта 2010 г. № 125 «О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию».

Постановление Правительства Российской Федерации от 21 апреля 2010 г. № 266 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг), и о внесении изменения в Положение о сертификации средств защиты информации».

Постановление Правительства Российской Федерации от 15 мая 2010 г. № 330 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг)».

Постановление Правительства Российской Федерации от 03 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

Постановление Правительства Российской Федерации от 03 марта 2012 г. № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации».

Постановление Правительства Российской Федерации от 21 марта 2012 г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

Постановление Правительства Российской Федерации от 16 апреля 2012 г. № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением

случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Иные информативные акты

Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. Государственной технической комиссией при Президенте РФ 25.11.1994).

Положение о сертификации средств защиты информации по требованиям безопасности информации (утв. Государственной технической комиссией при Президенте РФ 27.10.1995, приказ № 199).

Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) (утв. Государственной технической комиссией при Президенте РФ от 30.08.2002, приказом № 282).

Методические рекомендации управлениям ФСТЭК России по федеральным округам об организации работ по аттестации объектов информатизации по требованиям безопасности информации (утв. ФСТЭК России 25.04. 2006).

Методические рекомендации по технической защите информации, составляющей коммерческую тайну (утв. ФСТЭК России 25.12.2006).

Пособие по организации технической защиты информации, составляющей коммерческую тайну (утв. ФСТЭК России 25.12.2006).

Методические документы по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05.2007 и 19.11.2007).

Руководящие документы

Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения (утв. председателем Гостехкомиссии России от 30.03.1992).

Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации (утв. председателем Гостехкомиссии России от 30.03.1992).

Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (утв. председателем Гостехкомиссии России от 30.03.1992).

Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (утв. председателем Гостехкомиссии России от 30.03.1992).

Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники (утв. председателем Гостехкомиссии России от 30.03.1992).

Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации (утв. председателем Гостехкомиссии России от 25.07.1997).

Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования (утв. председателем Гостехкомиссии России от 25.07.1997).

Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (утв. приказом председателя Гостехкомиссии России от 04.06.1999 № 114).

Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (утв. Приказом Гостехкомиссии России от 19.06.2002 № 187).

Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05. 2007).

Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05.2007).

Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05.2007).

Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 19.11.2007).

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК России 14.02.2008).

Ведомственные приказы

Об утверждении Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (Приказ ФСБ России от 21.02.2008 № 149/54-144).

Об утверждении типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, со-

ставляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (Приказ ФСБ России от 21.02. 2008. № 149/6/6-622).

Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащих сведений, составляющих государственную тайну (Приказ ФАПСИ России от 13.06.2001 № 152).

Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Приказ ФСБ России от 09.02.2005 № 66).

Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (Приказ ФСТЭК России от 18.02.2013 № 21).

Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (Приказ ФСТЭК России от 11.02.2013 № 17).

Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности (Приказ ФСБ России от 10.07.2014 № 378).

Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (Приказ ФСТЭК России от 14.03.2014 № 31).

Национальные и международные стандарты

ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

ГОСТ 29099–91. Сети вычислительные локальные. Термины и определения.

ГОСТ Р 34.11–94. Информационная технология. Криптографическая защита информации. Функция хеширования.

ГОСТ 30373–95/ГОСТ 50414-92. Совместимость технических средств электромагнитная. Оборудование для испытаний. Камеры экранированные. Классы, основные параметры, технические требования и методы испытаний.

ГОСТ Р 50739–95. Средства вычислительной техники. Защита от НСД к информации. Общие технические требования.

ГОСТ Р 50752–95. Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Методы испытаний.

ISO/IEC 27001–2005 (2013). Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования.

ISO/IEC 27002–2005 (2012). Информационные технологии. Методы обеспечения безопасности. Практическое руководство по управлению информационной безопасностью.

ГОСТ Р В50170–2005. Противодействие иностранной технической разведке. Термины и определения.

ГОСТ Р 50922–2006. Защита информации. Основные термины и определения.

ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

ГОСТ Р ИСО/МЭК 27001–2006. Информационная технология. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. Требования.

ISO/IEC 27006–2007. Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью.

ГОСТ Р ИСО/МЭК 27006–2008. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности.

ГОСТ Р ИСО/МЭК 27005–2010. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

ГОСТ Р ИСО/МЭК 27004–2011. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения.

ГОСТ Р 34.10–2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

ГОСТ Р ИСО/МЭК 15408-1–2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий: в 3. Ч. 1. Введение и общая модель.

ГОСТ Р ИСО/МЭК 27002–2012. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

ГОСТ Р ИСО/МЭК 27003–2012. Информационные технологии. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности

ГОСТ Р ИСО/МЭК 15408-2–2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий: в 3. Ч. 2. Функциональные компоненты безопасности.

ГОСТ Р ИСО/МЭК 15408-3–2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий: в 3. Ч. 3. Компоненты доверия к безопасности.

ОГЛАВЛЕНИЕ

Предисловие 3

Р а з д е л I. Основы безопасности автоматизированных систем 5
Глава 1. Актуальность проблемы обеспечения безопасности автоматизированных систем 5
1.1. Место и роль автоматизированных систем в управлении бизнес-процессами 5
1.2. Обострение проблемы обеспечения безопасности автоматизированных систем на современном этапе 6
1.3. Защита автоматизированных систем как процесс управления рисками 9
1.4. Методы оценки целесообразности затрат на обеспечение безопасности 10
1.5. Особенности современных автоматизированных систем как объектов защиты 13
Глава 2. Основные понятия в области безопасности автоматизированных систем 15
2.1. Определение безопасности автоматизированных систем 15
2.2. Информация и информационные ресурсы 16
2.3. Субъекты информационных отношений, их безопасность 17
2.4. Цель защиты автоматизированной системы и циркулирующей в ней информации 19
Глава 3. Угрозы безопасности автоматизированных систем 20
3.1. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем 20
3.2. Угрозы безопасности информации, автоматизированных систем и субъектов информационных отношений 22
3.3. Классификация угроз безопасности 24
3.4. Классификация каналов проникновения в автоматизированную систему и утечки информации 27
3.5. Неформальная модель нарушителя 28
Глава 4. Меры и основные принципы обеспечения безопасности автоматизированных систем 33
4.1. Виды мер противодействия угрозам безопасности 33
4.2. Принципы построения системы обеспечения безопасности информации в автоматизированной системе 35

Глава 5. Правовые основы обеспечения безопасности автоматизированных систем 39
5.1. Защищаемая информация 41
5.2. Лицензирование 52
5.3. Сертификация средств защиты информации и аттестация объектов информатизации 57
5.4. Специальные требования и рекомендации по технической защите конфиденциальной информации 68
5.5. Юридическая значимость электронных документов с электронной подписью 69
5.6. Ответственность за нарушения в сфере защиты информации 71
Глава 6. Государственная система защиты информации 77
6.1. Главные направления работ по защите информации 77
6.2. Структура государственной системы защиты информации 78
6.3. Организация защиты информации в системах и средствах информатизации и связи 81
6.4. Контроль состояния защиты информации 83
6.5. Финансирование мероприятий по защите информации 84

Р а з д е л II. Обеспечение безопасности автоматизированных систем 85
Глава 7. Организационная структура системы обеспечения безопасности автоматизированных систем 85
7.1. Технология управления безопасностью информации и ресурсов в автоматизированной системе 85
7.2. Институт ответственных за обеспечение информационной безопасности 87
7.3. Регламентация действий пользователей и обслуживающего персонала автоматизированной системы 90
7.4. Политика безопасности организации 91
7.5. Мероприятия по созданию и обеспечению функционирования комплексной системы защиты 93
7.6. Распределение функций по обеспечению безопасности автоматизированных систем 95
7.7. Организационно-распорядительные документы по обеспечению безопасности автоматизированных систем 96
Глава 8. Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях 98
8.1. Проблема человеческого фактора 99
8.2. Общие правила обеспечения безопасности 99
8.3. Обязанности ответственного за обеспечение безопасности информации в подразделении 100
8.4. Ответственность за нарушения требований обеспечения безопасности 101
8.5. Порядок работы с носителями ключевой информации 102

Глава 9. Регламентация работ по обеспечению безопасности автоматизированных систем 106
9.1. Регламентация правил парольной и антивирусной защиты 107
9.2. Регламентация порядка допуска к работе и изменения полномочий пользователей автоматизированной системы 110
9.3. Регламентация порядка изменения конфигурации аппаратно-программных средств автоматизированной системы 112
9.4. Регламентация процессов разработки, испытания, опытной эксплуатации, внедрения и сопровождения задач 117
Глава 10. Категорирование и документирование защищаемых ресурсов 121
10.1. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов 121
10.2. Категорирование защищаемых ресурсов 123
10.3. Проведение информационных обследований и документирование защищаемых ресурсов 126
Глава 11. Концепция информационной безопасности. Планы защиты и обеспечения непрерывной работы и восстановления подсистем автоматизированной системы 128
11.1. Концепция информационной безопасности организации 129
11.2. План защиты информации 130
11.3. План обеспечения непрерывной работы и восстановления подсистем автоматизированной системы 131

Р а з д е л III. Средства защиты информации от несанкционированного доступа 138
Глава 12. Назначение и возможности средств защиты информации от несанкционированного доступа 138
12.1. Основные механизмы защиты автоматизированных систем 138
12.2. Защита периметра компьютерных сетей и управление механизмами защиты 151
12.3. Страхование информационных рисков 153
Глава 13. Аппаратно-программные средства защиты информации от несанкционированного доступа 156
13.1. Рекомендации по выбору средств защиты информации от несанкционированного доступа 156
13.2. Обзор существующих на рынке средств защиты информации от несанкционированного доступа 159
13.3. Средства аппаратной поддержки 166
13.4. Способы аутентификации 167
Глава 14. Применение штатных и дополнительных средств защиты информации от несанкционированного доступа 176
14.1. Стратегия безопасности Microsoft 177
14.2. Защита от вмешательства в процесс нормального функционирования автоматизированной системы 177

14.3. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы 179
14.4. Оперативное оповещение о зарегистрированных попытках несанкционированного доступа 185
14.5. Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования 187

Р а з д е л IV. Обеспечение безопасности компьютерных сетей 189
Глава 15. Проблемы обеспечения безопасности в компьютерных сетях 189
15.1. Типовая корпоративная сеть 189
15.2. Уровни информационной инфраструктуры корпоративной сети 190
15.3. Уязвимости и их классификация 190
15.4. Классификация атак 198
15.5. Средства защиты сетей 203
Глава 16. Защита периметра корпоративной сети 204
16.1. Угрозы, связанные с периметром корпоративной сети 205
16.2. Составляющие защиты периметра 206
16.3. Межсетевые экраны 207
16.4. Анализ содержимого почтового и веб-трафика 215
16.5. Виртуальные частные сети 216
Глава 17. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности 219
17.1. Управление уязвимостями 219
17.2. Архитектура систем управления уязвимостями 220
17.3. Особенности сетевых агентов сканирования 221
17.4. Средства анализа защищенности системного уровня 223
Глава 18. Мониторинг событий безопасности 224
18.1. Введение в управление журналами событий 224
18.2. Категории журналов событий 225
18.3. Инфраструктура управления журналами событий 225
18.4. Введение в технологию обнаружения атак 227
18.5. Классификация систем обнаружения атак 228
Глоссарий 230
Литература 237
Приложение. Нормативно-правовое обеспечение информационной безопасности 239

Учебное издание

Бондарев Валерий Васильевич

Введение в информационную безопасность автоматизированных систем

Редактор *Л.В. Честная*
Технический редактор *Э.А. Кулакова*
Художник *Я.М. Ильина*
Корректор *Ю.Н. Морозова*
Компьютерная графика *Т.Ю. Кутузовой*
Компьютерная верстка *Е.В. Ляшкевич*

В оформлении использованы шрифты
Студии Артемия Лебедева.

Оригинал-макет подготовлен
в Издательстве МГТУ им. Н.Э. Баумана.

Подписано в печать 12.05.2016. Формат 70×100/16.
Усл. печ. л. 15,75. Тираж 50 экз. Изд. № 523-2015. Заказ

Издательство МГТУ им. Н.Э. Баумана.
105005, Москва, 2-я Бауманская ул., д. 5, стр. 1.
press@bmstu.ru
www.baumanpress.ru

Отпечатано в типографии МГТУ им. Н.Э. Баумана.
105005, Москва, 2-я Бауманская ул., д. 5, стр. 1.
baumanprint@gmail.com