ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 17799— 2005

Информационная технология

ПРАКТИЧЕСКИЕ ПРАВИЛА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ISO/IEC 17799:2000
Information technology — Code of practice for information security management
(IDT)

Издание официальное

БЗ 1—2006/420

Москва
Стандартинформ
2006

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИИ ПТЗИ ФСТЭК России»)

2 ВНЕСЕН Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 447-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 17799:2000 «Информационная технология. Практические правила управления информационной безопасностью» (ISO/IEC 17799:2000 «Information technology. Code of practice for security management»)

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2006

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения . . . 1
2 Термины и определения . . . 1
3 Политика безопасности . . . 1
3.1 Политика информационной безопасности . . . 1
4 Организационные вопросы безопасности . . . 2
4.1 Организационная инфраструктура информационной безопасности . . . 2
4.2 Обеспечение безопасности при наличии доступа к информационным системам сторонних организаций . . . 5
4.3 Привлечение сторонних организаций к обработке информации (аутсорсинг) . . . 7
5 Классификация и управление активами . . . 7
5.1 Учет активов . . . 7
5.2 Классификация информации . . . 8
6 Вопросы безопасности, связанные с персоналом . . . 9
6.1 Учет вопросов безопасности в должностных обязанностях и при найме персонала . . . 9
6.2 Обучение пользователей . . . 10
6.3 Реагирование на инциденты нарушения информационной безопасности и сбои . . . 10
7 Физическая защита и защита от воздействий окружающей среды . . . 11
7.1 Охраняемые зоны . . . 11
7.2 Безопасность оборудования . . . 14
7.3 Общие мероприятия по управлению информационной безопасностью . . . 16
8 Управление передачей данных и операционной деятельностью . . . 17
8.1 Операционные процедуры и обязанности . . . 17
8.2 Планирование нагрузки и приемка систем . . . 19
8.3 Защита от вредоносного программного обеспечения . . . 20
8.4 Вспомогательные операции . . . 21
8.5 Управление сетевыми ресурсами . . . 22
8.6 Безопасность носителей информации . . . 23
8.7 Обмен информацией и программным обеспечением . . . 24
9 Контроль доступа . . . 28
9.1 Требование бизнеса по обеспечению контроля в отношении логического доступа . . . 28
9.2 Контроль в отношении доступа пользователей . . . 28
9.3 Обязанности пользователей . . . 30
9.4 Контроль сетевого доступа . . . 31
9.5 Контроль доступа к операционной системе . . . 33
9.6 Контроль доступа к приложениям . . . 36
9.7 Мониторинг доступа и использования системы . . . 36
9.8 Работа с переносными устройствами и работа в дистанционном режиме . . . 38
10 Разработка и обслуживание систем . . . 39
10.1 Требования к безопасности систем . . . 39
10.2 Безопасность в прикладных системах . . . 40
10.3 Меры защиты информации, связанные с использованием криптографии . . . 42
10.4 Безопасность системных файлов . . . 44
10.5 Безопасность в процессах разработки и поддержки . . . 45
11 Управление непрерывностью бизнеса . . . 47
12 Соответствие требованиям . . . 50
12.1 Соответствие требованиям законодательства . . . 50
12.2 Пересмотр политики безопасности и техническое соответствие требованиям безопасности . 53
12.3 Меры безопасности при проведении аудита . . . 54

Введение

Что такое информационная безопасность?

Информация — это актив, который, подобно другим активам организации, имеет ценность и, следовательно, должен быть защищен надлежащим образом. Информационная безопасность защищает информацию от широкого диапазона угроз с целью обеспечения уверенности в непрерывности бизнеса, минимизации ущерба, получения максимальной отдачи от инвестиций, а также реализации потенциальных возможностей бизнеса.

Информация может существовать в различных формах. Она может быть напечатана или написана на бумаге, храниться в электронном виде, передаваться по почте или с использованием электронных средств связи, демонстрироваться на пленке или быть выражена устно. Безотносительно формы выражения информации, средств ее распространения или хранения она должна всегда быть адекватно защищена.

Информационная безопасность — механизм защиты, обеспечивающий:

- конфиденциальность: доступ к информации только авторизованных пользователей;
- целостность: достоверность и полноту информации и методов ее обработки;
- доступность: доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Информационная безопасность достигается путем реализации соответствующего комплекса мероприятий по управлению информационной безопасностью, которые могут быть представлены политиками, методами, процедурами, организационными структурами и функциями программного обеспечения. Указанные мероприятия должны обеспечить достижение целей информационной безопасности организации.

Необходимость информационной безопасности

Информация, поддерживающие ее процессы, информационные системы и сетевая инфраструктура являются существенными активами организации. Конфиденциальность, целостность и доступность информации могут существенно способствовать обеспечению конкурентоспособности, ликвидности, доходности, соответствия законодательству и деловой репутации организации.

Организации, их информационные системы и сети все чаще сталкиваются с различными угрозами безопасности, такими как компьютерное мошенничество, шпионаж, вредительство, вандализм, пожары или наводнения. Такие источники ущерба, как компьютерные вирусы, компьютерный взлом и атаки типа отказа в обслуживании, становятся более распространенными, более агрессивными и все более изощренными.

Зависимость от информационных систем и услуг означает, что организации становятся все более уязвимыми по отношению к угрозам безопасности. Взаимодействие сетей общего пользования и частных сетей, а также совместное использование информационных ресурсов затрудняет управление доступом к информации. Тенденция к использованию распределенной обработки данных ослабляет эффективность централизованного контроля.

При проектировании многих информационных систем вопросы безопасности не учитывались. Уровень безопасности, который может быть достигнут техническими средствами, имеет ряд ограничений и, следовательно, должен сопровождаться надлежащими организационными мерами. Выбор необходимых мероприятий по управлению информационной безопасностью требует тщательного планирования и внимания к деталям.

Управление информационной безопасностью нуждается, как минимум, в участии всех сотрудников организации. Также может потребоваться участие поставщиков, клиентов или акционеров. Кроме того, могут потребоваться консультации специалистов сторонних организаций.

Мероприятия по управлению в области информационной безопасности обойдутся значительно дешевле и окажутся более эффективными, если будут включены в спецификацию требований на стадии проектирования системы.

Как определить требования к информационной безопасности

Организация должна определить свои требования к информационной безопасности с учетом следующих трех факторов.

Во-первых, оценка рисков организации. Посредством оценки рисков происходит выявление угроз активам организации, оценка уязвимости соответствующих активов и вероятности возникновения угроз, а также оценка возможных последствий.

Во-вторых, юридические, законодательные, регулирующие и договорные требования, которым должны удовлетворять организация, ее торговые партнеры, подрядчики и поставщики услуг.

В-третьих, специфический набор принципов, целей и требований, разработанных организацией в отношении обработки информации.

Оценка рисков информационной безопасности

Требования к информационной безопасности определяются с помощью систематической оценки рисков. Решения о расходах на мероприятия по управлению информационной безопасностью должны приниматься, исходя из возможного ущерба, нанесенного бизнесу в результате нарушений информационной безопасности. Методы оценки риска могут применяться как для всей организации, так и для какой-либо ее части, отдельных информационных систем, определенных компонентов систем или услуг, а именно там, где это практически выполнимо и целесообразно.

Оценка риска — это систематический анализ:

- вероятного ущерба, наносимого бизнесу в результате нарушений информационной безопасности с учетом возможных последствий от потери конфиденциальности, целостности или доступности информации и других активов;
- вероятности наступления такого нарушения с учетом существующих угроз и уязвимостей, а также внедренных мероприятий по управлению информационной безопасностью.

Результаты этой оценки помогут в определении конкретных мер и приоритетов в области управления рисками, связанными с информационной безопасностью, а также внедрению мероприятий по управлению информационной безопасностью с целью минимизации этих рисков.

Может потребоваться неоднократное проведение оценки рисков и выбора мероприятий по управлению информационной безопасностью для того, чтобы охватить различные подразделения организации или отдельные информационные системы.

Важно периодически проводить анализ рисков в области информационной безопасности и внедренных мероприятий по управлению информационной безопасностью для того, чтобы учесть:

- изменения требований и приоритетов бизнеса;
- появление новых угроз и уязвимостей;
- снижение эффективности существующих мероприятий по управлению информационной безопасностью.

Уровень детализации такого анализа следует определять в зависимости от результатов предыдущих проверок и изменяющегося уровня приемлемого риска. Оценка рисков обычно проводится сначала на верхнем уровне, при этом ресурсы направляются в области наибольшего риска, а затем на более детальном уровне, что позволяет рассмотреть специфические риски.

Выбор мероприятий по управлению информационной безопасностью

После того, как определены требования к информационной безопасности, следует выбрать и внедрить такие мероприятия по управлению информационной безопасностью, которые обеспечат снижение рисков до приемлемого уровня. Эти мероприятия могут быть выбраны из настоящего стандарта, других источников, а также могут быть разработаны собственные мероприятия по управлению информационной безопасностью, удовлетворяющие специфическим потребностям организации. Имеется множество различных подходов к управлению рисками; в настоящем стандарте приводятся примеры наиболее распространенных методов. Однако следует отметить, что некоторые из мероприятий по управлению информационной безопасностью неприменимы к отдельным информационным системам и средам и могут оказаться неприемлемыми для конкретных организаций. Например, в 8.1.4 приводится описание того, как могут быть распределены должностные обязанности, чтобы предотвратить ошибки и мошенничество. В небольших организациях может оказаться невозможным разделение всех должностных обязанностей; тогда для достижения той же цели может быть необходимо принятие альтернативных мероприятий по управлению информационной безопасностью. В качестве другого примера можно привести 9.7 и 12.1 — осуществление мониторинга использования системы и сбора доказательств. Указанные мероприятия по управлению информационной безопасностью, такие, как регистрация событий в системе, могут вступать в конфликт с законодательством, действующим, например, в отношении защиты от вторжения в личную жизнь клиентов или сотрудников.

Выбор мероприятий по управлению информационной безопасностью должен основываться на соотношении стоимости их реализации к эффекту от снижения рисков и возможным убыткам в случае нарушения безопасности. Также следует принимать во внимание факторы, которые не могут быть представлены в денежном выражении, например, потерю репутации.

Некоторые мероприятия по управлению информационной безопасностью, приведенные в настоящем стандарте, могут рассматриваться как руководящие принципы для управления информационной безопасностью и применяться для большинства организаций. Более подробно такие мероприятия рассматриваются ниже.

Отправная точка для внедрения информационной безопасности

Отдельные мероприятия по управлению информационной безопасностью могут рассматриваться как руководящие принципы для управления информационной безопасностью и служить отправной точкой для ее внедрения. Такие мероприятия либо основываются на ключевых требованиях законодательства, либо рассматриваются как общепринятая практика в области информационной безопасности.

Ключевыми мерами контроля с точки зрения законодательства являются:

- обеспечение конфиденциальности персональных данных (12.1.4);
- защита учетных данных организации (12.1.3);
- права на интеллектуальную собственность (12.1.2).

Мероприятия по управлению информационной безопасностью, рассматриваемые как общепринятая практика в области информационной безопасности, включают:

- наличие документа, описывающего политику информационной безопасности (3.1);
- распределение обязанностей по обеспечению информационной безопасности (4.1.3);
- обучение вопросам информационной безопасности (6.2.1);
- информирование об инцидентах, связанных с информационной безопасностью (6.3.1);
- управление непрерывностью бизнеса (11.1).

Перечисленные мероприятия применимы для большинства организаций и информационных сред. Следует отметить, что, хотя все приведенные в настоящем стандарте мероприятия являются важными, уместность какой-либо меры должна определяться в свете конкретных рисков, с которыми сталкивается организация. Следовательно, несмотря на то, что вышеописанный подход рассматривается как отправная точка для внедрения мероприятий по обеспечению информационной безопасности, он не заменяет выбор мероприятий по управлению информационной безопасностью, основанный на оценке рисков.

Важнейшие факторы успеха

Практика показывает, что для успешного внедрения информационной безопасности в организации решающими являются следующие факторы:

- соответствие целей, политик и процедур информационной безопасности целям бизнеса;
- согласованность подхода к внедрению системы безопасности с корпоративной культурой;
- видимая поддержка и заинтересованность со стороны руководства;
- четкое понимание требований безопасности, оценка рисков и управление рисками;
- обеспечение понимания необходимости применения мер информационной безопасности руководством и сотрудниками организации;
- передача инструкций в отношении политики информационной безопасности и соответствующих стандартов всем сотрудникам и контрагентам;
- обеспечение необходимого обучения и подготовки;
- всесторонняя и сбалансированная система измеряемых показателей, используемых для оценки эффективности управления информационной безопасностью и предложений по ее улучшению, поступивших от исполнителей.

Разработка собственных руководств организации

Настоящий стандарт должен расцениваться как отправная точка для разработки руководства под конкретные нужды организации. Не все инструкции и мероприятия, приведенные в настоящем стандарте, могут быть применимыми.

Более того, могут потребоваться дополнительные меры, не включенные в настоящий стандарт. В этом случае может быть полезным сохранение перекрестных ссылок, которые облегчат проверку соответствия, проводимую аудиторами и партнерами по бизнесу.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

ПРАКТИЧЕСКИЕ ПРАВИЛА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Information technology. Code of practice for information security management

Дата введения — 2007—01—01

1 Область применения

Настоящий стандарт устанавливает рекомендации по управлению информационной безопасностью лицам, ответственным за планирование, реализацию или поддержку решений безопасности в организации. Он предназначен для обеспечения общих основ для разработки стандартов безопасности и выбора практических мероприятий по управлению безопасностью в организации, а также в интересах обеспечения доверия в деловых отношениях между организациями. Рекомендации настоящего стандарта следует выбирать и использовать в соответствии с действующим законодательством.

2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

2.1 **информационная безопасность:** Защита конфиденциальности, целостности и доступности информации.

Примечания

1 **конфиденциальность:** Обеспечение доступа к информации только авторизованным пользователям.

2 **целостность:** Обеспечение достоверности и полноты информации и методов ее обработки.

3 **доступность:** Обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

2.2 **оценка рисков:** Оценка угроз, их последствий, уязвимости информации и средств ее обработки, а также вероятности их возникновения.

2.3 **управление рисками:** Процесс выявления, контроля и минимизации или устранения рисков безопасности, оказывающих влияние на информационные системы, в рамках допустимых затрат.

3 Политика безопасности

3.1 Политика информационной безопасности

Цель: обеспечение решения вопросов информационной безопасности и вовлечение высшего руководства организации в данный процесс.

Разработка и реализация политики информационной безопасности организации осуществляется высшим руководством путем выработки четкой позиции в решении вопросов информационной безопасности.

3.1.1 Документальное оформление

Политика информационной безопасности должна быть утверждена, издана и надлежащим образом доведена до сведения всех сотрудников организации. Она должна устанавливать ответственность

Издание официальное

руководства, а также излагать подход организации к управлению информационной безопасностью. Как минимум, политика должна включать следующее:

а) определение информационной безопасности, ее общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации;

б) изложение целей и принципов информационной безопасности, сформулированных руководством;

в) краткое изложение наиболее существенных для организации политик безопасности, принципов, правил и требований, например:

1) соответствие законодательным требованиям и договорным обязательствам;

2) требования в отношении обучения вопросам безопасности;

3) предотвращение появления и обнаружение вирусов и другого вредоносного программного обеспечения;

4) управление непрерывностью бизнеса;

5) ответственность за нарушения политики безопасности;

г) определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности;

д) ссылки на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры безопасности для конкретных информационных систем, а также правила безопасности, которым должны следовать пользователи.

Такая политика должна быть доведена до сведения всех сотрудников организации в доступной и понятной форме.

3.1.2 Пересмотр и оценка

Необходимо, чтобы в организации назначалось ответственное за политику безопасности должностное лицо, которое отвечало бы за ее реализацию и пересмотр в соответствии с установленной процедурой. Указанная процедура должна обеспечивать осуществление пересмотра политики информационной безопасности в соответствии с изменениями, влияющими на основу первоначальной оценки риска, например, путем выявления существенных инцидентов нарушения информационной безопасности, появление новых уязвимостей или изменения организационной или технологической инфраструктуры. Периодические пересмотры должны осуществляться в соответствии с установленным графиком и включать:

- проверку эффективности политики, исходя из характера, числа и последствий зарегистрированных инцидентов нарушения информационной безопасности;
- определение стоимости мероприятий по управлению информационной безопасностью и их влияние на эффективность бизнеса;
- оценку влияния изменений в технологиях.

4 Организационные вопросы безопасности

4.1 Организационная инфраструктура информационной безопасности

Цель: управление информационной безопасностью в организации.

Структуру управления следует создавать так, чтобы она способствовала инициации и осуществлению контроля за внедрением информационной безопасности в организации.

Следует создавать соответствующие управляющие советы с участием высшего руководства для утверждения политики информационной безопасности, назначения ответственных лиц в области информационной безопасности, а также осуществления координации внедрения мероприятий по управлению информационной безопасностью в организации. При необходимости следует предусмотреть наличие специалиста по вопросам информационной безопасности внутри организации, к которому могут обращаться заинтересованные сотрудники. Следует налаживать контакты с внешними специалистами по безопасности для того, чтобы быть в курсе отраслевых тенденций, способов и методов ее оценки, а также с целью адекватного реагирования на инциденты нарушения информационной безопасности. Следует поощрять многопрофильный подход к информационной безопасности, например, путем налаживания сотрудничества между менеджерами, пользователями, администраторами, разработчиками приложений, аудиторами и сотрудниками безопасности, а также специалистами в области страхования и управления рисками.

4.1.1 Управляющий совет по вопросам информационной безопасности

Обеспечение информационной безопасности — это ответственность высшего руководства организации, разделяемая всеми ее членами. Поэтому при формировании совета по вопросам информационной безопасности должны обеспечиваться четкое управление и реальная поддержка со стороны руководства инициатив в области безопасности. Такой совет должен способствовать укреплению безопасности в организации путем непосредственного участия руководства и выделения необходимых ресурсов. Он может быть частью существующего органа управления. Как правило, такой совет выполняет следующие функции:

- утверждение и пересмотр политики информационной безопасности и соответствующих обязанностей по ее выполнению;
- отслеживание существенных изменений в воздействиях основных угроз информационным активам;
- анализ и мониторинг инцидентов нарушения информационной безопасности;
- утверждение основных проектов в области информационной безопасности.

Кроме этого, должен быть назначен руководитель, отвечающий за все вопросы, связанные с информационной безопасностью.

4.1.2 Координация вопросов информационной безопасности

Для координации внедрения мероприятий по управлению информационной безопасностью в большой организации может потребоваться создание комитета, включающего представителей руководства заинтересованных подразделений организации.

Как правило, такой комитет:

- согласовывает конкретные функции и обязанности в области информационной безопасности в рамках всей организации;
- согласовывает конкретные методики и процедуры информационной безопасности, например, такие как оценка рисков, классификация информации с точки зрения требований безопасности;
- согласовывает и обеспечивает поддержку инициатив и проектов в области информационной безопасности в рамках всей организации, например, таких как разработка программы повышения осведомленности сотрудников в области безопасности;
- обеспечивает учет включения требований безопасности во все проекты, связанные с обработкой и использованием информации;
- оценивает адекватность и координирует внедрение конкретных мероприятий по управлению информационной безопасностью для новых систем или услуг;
- проводит анализ инцидентов нарушения информационной безопасности;
- способствует демонстрации поддержки информационной безопасности со стороны высшего руководства организации.

4.1.3 Распределение обязанностей по обеспечению информационной безопасности

Следует определить обязанности по защите отдельных активов и по выполнению конкретных процедур, связанных с информационной безопасностью.

Политика информационной безопасности (раздел 3) должна устанавливать общие принципы и правила распределения функций и обязанностей, связанных с обеспечением информационной безопасности в организации. Политику следует дополнить, где необходимо, более детальными руководствами для конкретных областей, систем или услуг. Кроме этого, должна быть четко определена конкретная ответственность в отношении отдельных материальных и информационных активов и процессов, связанных с информационной безопасностью, например, таких как планирование непрерывности бизнеса.

Во многих организациях на руководителя службы информационной безопасности возлагается общая ответственность за разработку и внедрение системы информационной безопасности, а также за оказание содействия в определении мероприятий по управлению информационной безопасностью.

В то же время ответственность за определение подлежащих защите ресурсов и реализацию мероприятий по управлению информационной безопасностью в большинстве случаев возлагается на руководителей среднего звена. Общепринятой практикой является назначение ответственного лица (администратора) для каждого информационного актива, в чьи повседневные обязанности входит обеспечение безопасности данного актива.

Администратор информационных активов может передавать свои полномочия по обеспечению безопасности какому-либо руководителю среднего звена или поставщикам услуг. Тем не менее, администратор остается ответственным за обеспечение безопасности актива и должен быть в состоянии определить, что любые переданные полномочия реализуются должным образом.

Следует устанавливать границы ответственности каждого руководителя и выполнять следующие правила:

- различные активы и процессы (процедуры) безопасности, связанные с каждой отдельной системой, должны быть выделены и четко определены;

- необходимо назначить ответственных (администраторов) за каждый актив или процедуру безопасности, и детали этой ответственности должны быть документированы;

- уровни полномочий (авторизации) должны быть ясно определены и документированы.

Примечание — Под авторизацией понимается определение уровней доступа пользователя к определенным массивам информации; в более широком смысле — разрешение определенных действий.

4.1.4 Процесс получения разрешения на использование средств обработки информации

Необходимо определить процедуры получения разрешения на использование новых средств обработки информации.

При этом могут осуществляться следующие мероприятия по управлению информационной безопасностью:

- новые средства должны быть соответствующим образом одобрены со стороны руководства пользователей и администраторов средств управления, авторизующих их цель использования. Одобрение следует также получать от менеджера, ответственного за поддержание среды безопасности локальной информационной системы, чтобы обеспечить уверенность в том, что все соответствующие политики безопасности и требования соблюдены;

- аппаратные средства и программное обеспечение следует проверять на совместимость с другими компонентами системы.

Примечания

1 Одобрение может потребоваться для соединений некоторых типов.

2 Использование личных средств обработки информации для обработки служебной информации и любых необходимых мероприятий по управлению информационной безопасностью должно быть авторизовано.

3 Использование личных средств обработки информации на рабочем месте может быть причиной новых уязвимостей и, следовательно, должно быть оценено и авторизовано.

Эти мероприятия по управлению информационной безопасностью особенно важны в сетевой среде.

4.1.5 Консультации специалистов по вопросам информационной безопасности

Консультации специалистов по вопросам безопасности требуются многим организациям. В идеале, их должен обеспечивать опытный консультант по информационной безопасности, являющийся сотрудником организации. Но не все организации могут иметь в своем штате профессионала-консультанта. В таких случаях рекомендуется назначение выделенного сотрудника (администратора) для обобщения знаний и опыта внутри организации с целью обеспечения согласованности и поддержки в принятии решений по безопасности. Этот сотрудник должен также иметь доступ к необходимым внешним консультантам для получения профессиональных консультаций по вопросам, выходящим за рамки его собственной компетенции.

Перед консультантами по информационной безопасности или администраторами должна быть поставлена задача по обеспечению консультаций по всем аспектам информационной безопасности, в том числе и с привлечением внешних консультантов. От качества их оценки угроз безопасности и разработки рекомендаций относительно мероприятий по управлению информационной безопасностью существенным образом зависит ее эффективность в организации. Для обеспечения максимальной эффективности и результативности деятельности консультантов (администраторов) им должна быть предоставлена возможность непосредственного доступа к высшему руководству организации.

С консультантом по информационной безопасности или администратором следует советоваться, по возможности, незамедлительно, в случае подозрения на выявление инцидента нарушения информационной безопасности или уязвимости безопасности для обеспечения получения квалифицированного совета или выделения ресурсов. Несмотря на то, что большинство внутренних расследований в отношении безопасности обычно выполняют под контролем руководства, может быть целесообразным обращение к консультанту (администратору) по информационной безопасности с целью разработки рекомендаций, а также его участия в расследовании или в его руководстве.

4.1.6 Сотрудничество между организациями в области информационной безопасности

Соответствующие контакты с органами, отвечающими за соблюдение законов, с регулирующими органами, поставщиками информационных услуг и операторами связи следует поддерживать для того, чтобы гарантировать, что и в случае нарушения информационной безопасности можно быстро предпринять соответствующие действия и получить правильный совет. С аналогичной целью следует рассматривать участие в профессиональных сообществах и в отраслевых мероприятиях в области безопасности.

При обменах информацией по вопросам информационной безопасности следует обеспечивать защиту конфиденциальной информации организации от несанкционированного доступа.

4.1.7 Независимая проверка (аудит) информационной безопасности

Документ политики информационной безопасности (подраздел 3.1) устанавливает цели и обязанности в области информационной безопасности. Его выполнение должно проверяться в интересах обеспечения уверенности в том, что разработанные в организации мероприятия должным образом отражают политику и что она является выполнимой и эффективной (подраздел 12.2).

Такая проверка (аудит) может быть выполнена внутренним аудитом, независимым менеджером или сторонней организацией, специализирующейся на таких проверках, при этом специалисты, привлекаемые к проверке, должны обладать соответствующими навыками и опытом.

4.2 Обеспечение безопасности при наличии доступа к информационным системам сторонних организаций

Цель: поддерживать безопасность средств обработки информации организации и информационных активов при доступе третьих сторон.

Доступ к средствам обработки информации организации третьих сторон должен контролироваться.

Там, где есть потребность бизнеса в таком доступе третьей стороны, следует производить оценку риска, определять последствия для безопасности и устанавливать требования к мероприятиям по управлению информационной безопасностью. Такие мероприятия следует согласовывать и определять в контракте с третьей стороной.

Контракты, разрешающие доступ третьей стороне, должны включать процедуру определения прав и условий доступа других участников.

Настоящий стандарт может использоваться как основа для составления таких контрактов, а также при рассмотрении и привлечении сторонних организаций для обработки информации (outsourcing).

4.2.1 Определение рисков, связанных с наличием доступа сторонних лиц и организаций к информационным системам

4.2.1.1 Типы доступа

Определение типа доступа, предоставленного третьей стороне, имеет особое значение. Например, риски доступа через сетевое соединение отличаются от рисков, связанных с физическим доступом.

Типами доступа, которые следует рассматривать, являются:

- физический — к офисным помещениям, компьютерным комнатам, серверным;
- логический — к базам данных, информационным системам организации.

4.2.1.2 Обоснования для доступа

Третьей стороне может быть предоставлен доступ по ряду причин. Например, сторонним компаниям, оказывающим услуги организациям, но не расположенным территориально в том же месте, может быть предоставлен физический и логический доступ, как, например:

- сотрудникам третьей стороны, отвечающим за обслуживание аппаратных средств и программного обеспечения, которым необходим доступ на уровне систем или более низком уровне прикладной функциональности;
- торговым и деловым партнерам, которым может потребоваться обмен информацией, доступ к информационным системам или общим базам данных.

Информация организации может быть подвержена риску нарушения безопасности при доступе третьих сторон с неадекватным управлением безопасностью. Там, где есть производственная необходимость контактов с третьей стороной, следует проводить оценку риска, чтобы идентифицировать требования и определить мероприятия по управлению информационной безопасностью. При этом следует принимать во внимание тип требуемого доступа, ценность информации, мероприятия по управлению информационной безопасностью, используемые третьей стороной, и последствия этого доступа для информационной безопасности организации.

4.2.1.3 Подрядчики, выполняющие работы в помещениях в организации

Третьи стороны, размещенные в помещениях организации более срока, определенного в их контракте, могут ослабить безопасность. Категории сотрудников третьей стороны, размещаемых в помещениях организации:

- сотрудники, осуществляющие поддержку и сопровождение аппаратных средств и программного обеспечения;
- сотрудники, осуществляющие уборку, обеспечивающие питание, охрану и другие услуги;
- студенты и лица, работающие по трудовым соглашениям;
- консультанты.

Важно предусмотреть мероприятия по управлению информационной безопасностью, необходимые для управления доступом к средствам обработки информации третьей стороны. Все требования безопасности, связанные с доступом третьей стороны или мероприятиями по управлению информационной безопасностью, следует отражать в контракте с третьей стороной (4.2.2). Например, если существует специальная потребность в обеспечении конфиденциальности информации, следует заключить соглашение о ее неразглашении (6.1.3).

Недопустимо предоставлять третьей стороне доступ к информации и средствам ее обработки до тех пор, пока не установлены соответствующие мероприятия по управлению информационной безопасностью и не подписан контракт, определяющий условия предоставления связи или доступа.

4.2.2 Включение требований безопасности в договоры со сторонними лицами и организациями

Все действия, связанные с привлечением третьей стороны к средствам обработки информации организации, должны быть основаны на официальном контракте, содержащем или ссылающемся на них, и должны обеспечиваться в соответствии с политикой и стандартами безопасности организации. Контракт должен обеспечивать уверенность в том, что нет никакого недопонимания между сторонами. Организации также должны предусмотреть возмещение своих возможных убытков со стороны контрагента. В контракт включаются следующие положения:

а) общая политика информационной безопасности;

б) защита активов, включая:

1) процедуры по защите активов организации, в том числе информации и программного обеспечения;

2) процедуры для определения компрометации активов, например, вследствие потери или модификации данных;

3) мероприятия по обеспечению возвращения или уничтожения информации и активов по окончании контракта или в установленное время в течение действия контракта;

4) целостность и доступность активов;

5) ограничения на копирование и раскрытие информации;

в) описание каждой предоставляемой услуги;

г) определение необходимого и неприемлемого уровня обслуживания;

д) условия доставки сотрудников к месту работы, при необходимости;

е) соответствующие обязательства сторон в рамках контракта;

ж) обязательства относительно юридических вопросов, например, законодательства о защите данных с учетом различных национальных законодательств, особенно если контракт относится к сотрудничеству с организациями в других странах (12.1);

з) права интеллектуальной собственности (IPRs) и авторские права (12.1.2), а также правовая защита любой совместной работы (6.1.3);

и) соглашения по управлению доступом, охватывающие:

1) разрешенные методы доступа, а также управление и использование уникальных идентификаторов, типа пользовательских ID и паролей;

2) процесс авторизации в отношении доступа и привилегий пользователей;

3) требование актуализации списка лиц, имеющих право использовать предоставляемые услуги, а также соответствующего списка прав и привилегий;

к) определение измеряемых показателей эффективности, а также их мониторинг и предоставление отчетности;

л) право мониторинга действий пользователей и блокировки доступа;

м) право проводить проверки (аудит) договорных обязанностей или делегировать проведение такого аудита третьей стороне;

н) определение процесса информирования о возникающих проблемах в случае непредвиденных обстоятельств;

о) обязанности, касающиеся установки и сопровождения аппаратных средств и программного обеспечения;

п) четкая структура подотчетности и согласованные форматы представления отчетов;

р) ясный и определенный процесс управления изменениями;

с) любые необходимые способы ограничения физического доступа и процедуры для обеспечения уверенности в том, что эти меры эффективны;

т) обучение пользователя и администратора методам и процедурам безопасности;

у) мероприятия по управлению информационной безопасностью для обеспечения защиты от вредоносного программного обеспечения (см. 8.3);

ф) процедуры отчетности, уведомления и расследования инцидентов нарушения информационной безопасности и выявления слабых звеньев системы безопасности;

х) привлечение третьей стороны вместе с субподрядчиками.

4.3 Привлечение сторонних организаций к обработке информации (аутсорсинг)

Цель: обеспечение информационной безопасности, когда ответственность за обработку информации передана другой организации.

Договоренности, связанные с привлечением третьих сторон, должны учитывать оценки рисков, мероприятия по управлению информационной безопасностью и процедуры в отношении информационных систем, сетей и/или настольных компьютеров и должны быть отражены в контракте.

4.3.1 Включение требований безопасности в договоры на оказание услуг по обработке информации сторонними организациями (аутсорсингу)

Требования безопасности в случае, когда организация передает для управления и контроля все или некоторые из своих информационных систем, сетей и/или персональных компьютеров, следует указать в контракте, согласованном между сторонами и учитывающем:

- выполнение требований законодательства, например, в отношении защиты данных;
- достижение договоренностей, обеспечивающих уверенность в том, что все стороны, включая субподрядчиков, осведомлены о своих обязанностях, касающихся безопасности;
- как будут обеспечиваться и тестироваться параметры целостности и конфиденциальности бизнес-активов организации;
- типы физических и логических методов по управлению информационной безопасностью, используемых при предоставлении необходимого доступа к чувствительной служебной информации организации сторонним пользователям;
- обеспечение доступности сервисов в случае бедствия;
- уровни физической безопасности, которые должны быть обеспечены в отношении оборудования, используемого в рамках аутсорсинга;
- право на проведение аудита.

Условия, приведенные в пункте 4.2.2, следует также рассматривать как часть контракта. Необходимо, чтобы контрактом была предусмотрена возможность дальнейшей детализации и реализации требований и процедур безопасности в согласованном между сторонами плане мероприятий в области безопасности.

Несмотря на то, что контракты по привлечению третьих сторон могут включать ряд сложных вопросов, правила и рекомендации по управлению информационной безопасностью, включенные в настоящий стандарт, должны служить отправной точкой при согласовании структуры и содержания плана по управлению безопасностью.

5 Классификация и управление активами

5.1 Учет активов

Цель: обеспечение соответствующей защиты активов организации.

Все основные информационные активы должны быть учтены и закреплены за ответственными владельцами.

Учет активов помогает обеспечивать уверенность в их надлежащей защите. Необходимо идентифицировать владельцев всех основных активов и определить их ответственность за поддержание соответствующих мероприятий по управлению информационной безопасностью. Осуществление мероприятий по управлению информационной безопасностью может быть делегировано, но ответственность должна оставаться за назначенным владельцем актива.

5.1.1 Инвентаризация активов

Описание активов дает уверенность в том, что обеспечивается эффективная защита активов, и оно может также потребоваться для целей обеспечения безопасности труда, страхования или решения финансовых вопросов (управление активами). Процесс составления описи активов — важный аспект управления риском. Организация должна быть в состоянии идентифицировать свои активы с учетом их относительной ценности и важности. Основываясь на этой информации, организация может обеспечивать заданные уровни защиты, соответствующие ценности и важности активов. Описи следует составлять и поддерживать для важных активов, связанных с каждой информационной системой. Каждый актив должен быть четко идентифицирован и классифицирован с точки зрения безопасности (5.2), его владельцы должны быть авторизованы, а данные о них документированы. Кроме того, должно быть ука-

зано фактическое местоположение актива (это важно в случае восстановления активов при потере или повреждении). Примерами активов, связанных с информационными системами, являются:

- информационные активы: базы данных и файлы данных, системная документация, руководства пользователя, учебные материалы, процедуры эксплуатации или поддержки (обслуживания), планы по обеспечению непрерывности функционирования информационного обеспечения, процедуры действий при сбоях, архивированная информация;
- активы программного обеспечения: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства разработки и утилиты;
- физические активы: компьютерное оборудование (процессоры, мониторы, переносные компьютеры, модемы), оборудование связи (маршрутизаторы, частные автоматические телефонные станции с выходом в сеть общего пользования, факсы, автоответчики), магнитные носители (ленты и диски), другое техническое оборудование (электропитание, кондиционеры), мебель, помещения;
- услуги: вычислительные услуги и услуги связи, основные коммунальные услуги, например, отопление, освещение, электроэнергия, кондиционирование.

5.2 Классификация информации

Цель: обеспечение уверенности в том, что информационные активы защищены на надлежащем уровне.

Информацию следует классифицировать, чтобы определить ее приоритетность, необходимость и степень ее защиты.

Информация имеет различные степени чувствительности и критичности. Некоторые виды информации могут требовать дополнительного уровня защиты или специальных методов обработки. Систему классификации информации следует использовать для определения соответствующего множества уровней защиты и потребности в специальных методах обработки.

5.2.1 Основные принципы классификации

При классификации информации и связанных с ней мероприятий по управлению информационной безопасностью следует учитывать требования бизнеса в совместном использовании или ограничении доступа к информации, а также последствия для бизнеса, связанные с такими требованиями, например, неавторизованный доступ или повреждение информации. Классификация информации позволяет определить, как эта информация должна быть обработана и защищена.

Информацию и выходные отчеты систем, обрабатывающих классифицированные данные, следует отнести к какой-либо категории с точки зрения ее ценности и чувствительности для организации. Можно также оценить соответствующую информацию с учетом того, насколько она критична для организации, например, с точки зрения обеспечения ее целостности и доступности.

Информация обычно перестает быть чувствительной или критичной к компрометации по истечении некоторого периода времени, например, когда она становится общедоступной. Эти аспекты следует принимать во внимание, поскольку присвоение повышенной категории может вести к ненужным дополнительным расходам. В руководящих принципах классификации следует предвидеть и учитывать, что категория любого вида информации необязательно должна быть постоянной в течение всего времени — она может изменяться в соответствии с некоторой принятой политикой безопасности в организации (9.1).

Чрезмерно сложные схемы категорирования информации могут стать обременительными и неэкономичными для использования или оказываются неосуществимыми. Следует проявлять осмотрительность при интерпретации категорий (грифов) классификации на документах от других организаций, которые могут иметь другие определения или содержание для тех же самых или подобных категорий.

Ответственность за определение категории информации (например, документа, записи данных файла или дискеты с данными) и периодичность пересмотра этой категории должны оставаться за создателем, назначенным владельцем или собственником информации.

5.2.2 Маркировка и обработка информации

Важно, чтобы был определен соответствующий набор процедур для маркировки при обработке информации в соответствии с системой классификации, принятой организацией. Эти процедуры должны относиться к информационным активам, представленным как в физической, так и в электронной форме. Для каждой классификации следует определять процедуры маркировки для того, чтобы учесть следующие типы обработки информации:

- копирование;
- хранение;
- передачу по почте, факсом и электронной почтой;
- передачу голосом, включая мобильный телефон, голосовую почту, автоответчики;

- уничтожение.

При осуществлении вывода данных из систем, содержащих информацию, которая классифицирована как чувствительная или критичная, следует использовать соответствующую метку классификации (при выводе). В маркировке следует отражать классификацию согласно 5.2.1. Следует маркировать напечатанные отчеты, экранные формы, носители информации (ленты, диски, компакт-диски, кассеты), электронные сообщения и передачу файлов.

Физические метки являются, в общем случае, наиболее подходящей формой маркировки. Однако некоторые информационные активы, такие как документы в электронной форме, физически не могут быть промаркированы, и поэтому необходимо использовать электронные аналоги маркировки.

6 Вопросы безопасности, связанные с персоналом

6.1 Учет вопросов безопасности в должностных обязанностях и при найме персонала

Цель: минимизация рисков от ошибок, связанных с человеческим фактором, воровства, мошенничества, кражи или неправильного использования средств обработки информации.

Обязанности по соблюдению требований безопасности следует распределять на стадии подбора персонала, включать в трудовые договоры и проводить их мониторинг в течение всего периода работы сотрудника.

Следует осуществлять соответствующую проверку кандидатов на работу (6.1.2), особенно это касается должностей, предполагающих доступ к важной информации. Все сотрудники и представители третьей стороны, использующие средства обработки информации организации, должны подписывать соглашение о конфиденциальности (неразглашении).

6.1.1 Включение вопросов информационной безопасности в должностные обязанности

Функции (роли) и ответственность в области информационной безопасности, как установлено в политике информационной безопасности организации (3.1), следует документировать. В должностные инструкции следует включать как общие обязанности по внедрению или соблюдению политики безопасности, так и специфические особенности по защите определенных активов или действий, касающихся безопасности.

6.1.2 Проверка персонала при найме и соответствующая политика

Проверки сотрудников, принимаемых в постоянный штат, следует выполнять по мере подачи заявлений о приеме на работу. В них необходимо включать следующее:

- наличие положительных рекомендаций, в частности в отношении деловых и личных качеств претендента;
- проверка (на предмет полноты и точности) резюме претендента;
- подтверждение заявляемого образования и профессиональных квалификаций;
- независимая проверка подлинности документов, удостоверяющих личность (паспорта или заменяющего его документа).

В случаях, когда новому сотруднику непосредственно после приема на работу или в ее процессе предстоит доступ к средствам обработки важной информации, например финансовой или совершенно секретной информации организации, следует выполнить специальную «проверку на доверие». В отношении сотрудников, имеющих значительные полномочия, эта проверка должна проводиться периодически.

Аналогичный процесс проверки следует осуществлять для подрядчиков и временного персонала. В тех случаях, когда прием сотрудников осуществляется через кадровое агентство, контракт с агентством должен четко определять обязанности агентства по проверке претендентов и процедурам уведомления, которым оно должно следовать, если проверка не была закончена или если результаты дают основания для сомнения или беспокойства.

Руководству организации следует оценить необходимый уровень наблюдения за новыми и неопытными сотрудниками, обладающими правом доступа к важным системам. Необходимо внедрить процедуры по периодическому контролю и утверждению действий всех сотрудников со стороны вышестоящих руководителей.

Руководителям следует учитывать, что личные проблемы сотрудников могут сказываться на их работе. Личные или финансовые проблемы сотрудников, изменения в их поведении или образе жизни, периодическая рассеянность и признаки стресса или депрессии могут быть причинами мошенничества, воровства, ошибок или других нарушений безопасности. Эту информацию следует рассматривать в соответствии с действующим законодательством.

6.1.3 Соглашения о конфиденциальности

Соглашения о конфиденциальности или соглашения о неразглашении используются для уведомления сотрудников о том, что информация является конфиденциальной или секретной. Сотрудники обычно должны подписывать такое соглашение как неотъемлемую часть условий трудового договора.

Временные сотрудники и представители третьих сторон, не попадающие под стандартный трудовой договор (содержащий соглашение о соблюдении конфиденциальности), должны подписывать отдельно соглашение о соблюдении конфиденциальности до того, как им будет предоставлен доступ к средствам обработки информации.

Соглашения о соблюдении конфиденциальности следует пересматривать при изменении условий трудового договора, особенно в случае изменения обязанностей сотрудника или истечении сроков трудовых договоров.

6.1.4 Условия трудового соглашения

Условия трудового договора должны определять ответственность служащего в отношении информационной безопасности. Там, где необходимо, эта ответственность должна сохраняться и в течение определенного срока после увольнения с работы. Необходимо указать меры дисциплинарного воздействия, которые будут применимы в случае нарушения сотрудником требований безопасности.

Ответственность и права сотрудников, вытекающие из действующего законодательства, например в части законов об авторском праве или законодательства о защите персональных данных, должны быть разъяснены персоналу и включены в условия трудового договора. Также должна быть указана ответственность в отношении категорирования и управления данными организации-работодателя. Всякий раз, при необходимости, в условиях трудового договора следует указывать, что эта ответственность распространяется и на работу вне помещений организации, и внерабочее время, например, в случае исполнения работы на дому (7.2.5 и 9.8.1).

6.2 Обучение пользователей

Цель: обеспечение уверенности в осведомленности пользователей об угрозах и проблемах, связанных с информационной безопасностью, и их оснащенности всем необходимым для соблюдения требований политики безопасности организации при выполнении служебных обязанностей.

Пользователей необходимо обучать процедурам безопасности и правильному использованию средств обработки информации, чтобы свести к минимуму возможные риски безопасности.

6.2.1 Обучение и подготовка в области информационной безопасности

Все сотрудники организации и, при необходимости, пользователи третьей стороны должны пройти соответствующее обучение и получать на регулярной основе обновленные варианты политик и процедур информационной безопасности, принятых в организации. Обучение сотрудников должно обеспечить знание ими требований безопасности, ответственности в соответствии с законодательством, мероприятий по управлению информационной безопасностью, а также знание правильного использования средств обработки информации, например процедур регистрации в системах, использования пакетов программ, прежде чем им будет предоставлен доступ к информации или услугам.

6.3 Реагирование на инциденты нарушения информационной безопасности и сбои

Цель: сведение к минимуму ущерба от инцидентов нарушения информационной безопасности и сбоев, а также осуществление мониторинга и реагирование по случаям инцидентов.

Об инцидентах нарушения информационной безопасности следует информировать руководство в соответствии с установленным порядком, по возможности, незамедлительно.

Все сотрудники и подрядчики должны быть осведомлены о процедурах информирования о различных типах инцидентов нарушения информационной безопасности (нарушение безопасности, угроза, уязвимость системы или сбой), которые могли бы оказать негативное влияние на безопасность активов организации. Сотрудники и подрядчики должны немедленно сообщать о любых наблюдаемых или предполагаемых инцидентах определенному контактному лицу или администратору безопасности. В организации должны быть установлены меры дисциплинарной ответственности сотрудников, нарушающих требования безопасности. Для того чтобы иметь возможность реагировать на инциденты нарушения информационной безопасности должным образом, необходимо собирать свидетельства и доказательства возможно быстрее после обнаружения инцидента (12.1.7).

6.3.1 Информирование об инцидентах нарушения информационной безопасности

Об инцидентах нарушения информационной безопасности следует информировать руководство в соответствии с установленным порядком, по возможности, незамедлительно.

Необходимо внедрить формализованную процедуру информирования об инцидентах, а также процедуру реагирования на инциденты, устанавливающие действия, которые должны быть предприняты

после получения сообщения об инциденте. Все сотрудники и подрядчики должны быть ознакомлены с процедурой информирования об инцидентах нарушения информационной безопасности, а также проинформированы о необходимости незамедлительного сообщения об инцидентах. Необходимо также предусмотреть процедуры обратной связи по результатам реагирования на инциденты нарушения информационной безопасности. Информация об инцидентах может использоваться с целью повышения осведомленности пользователей (6.2), поскольку позволяет демонстрировать на конкретных примерах возможные последствия инцидентов, реагирование на них, а также способы их исключения в будущем (12.1.7).

6.3.2 Информирование о проблемах безопасности

От пользователей информационных сервисов необходимо требовать, чтобы они обращали внимание и сообщали о любых замеченных или предполагаемых недостатках и угрозах в области безопасности в системах или сервисах. Они должны немедленно сообщать об этих причинах для принятия решений своему руководству или непосредственно поставщику услуг. Необходимо информировать пользователей, что они не должны ни при каких обстоятельствах самостоятельно искать подтверждения подозреваемому недостатку в системе безопасности. Это требование предъявляется в интересах самих пользователей, поскольку тестирование слабых мест защиты может быть интерпретировано как неправомочное использование системы.

6.3.3 Информирование о сбоях программного обеспечения

Для информирования о сбоях программного обеспечения необходимы соответствующие процедуры. При этом должны предусматриваться следующие действия:

- симптомы проблемы и любые сообщения, появляющиеся на экране, должны фиксироваться;
- по возможности, компьютер необходимо изолировать и пользование им прекратить. О проблеме следует немедленно известить соответствующее контактное лицо или администратора. В случае необходимости провести исследования оборудования, которое должно быть отсоединено от всех сетей организации. Дискеты не следует передавать для использования в других компьютерах;
- о факте сбоя программного обеспечения следует немедленно извещать руководителя службы информационной безопасности.

Пользователи не должны пытаться самостоятельно удалить подозрительное программное обеспечение, если они не уполномочены на это. Ликвидировать последствия сбоев должен соответственно обученный персонал.

6.3.4 Извлечение уроков из инцидентов нарушения информационной безопасности

Необходимо установить порядок мониторинга и регистрации инцидентов и сбоев в отношении их числа, типов, параметров, а также связанных с этим затрат. Эту информацию следует использовать для идентификации повторяющихся или значительных инцидентов или сбоев. Данная информация может указывать на необходимость в совершенствовании существующих или внедрении дополнительных мероприятий по управлению информационной безопасностью с целью минимизации вероятности появления инцидентов нарушения информационной безопасности, снижения возможного ущерба и расходов в будущем, кроме того, данную информацию следует учитывать при пересмотре политики информационной безопасности (3.1.2).

6.3.5 Процесс установления дисциплинарной ответственности

Должны существовать формализованные процедуры, устанавливающие дисциплинарную ответственность сотрудников, нарушивших политику и процедуры безопасности организации (6.1.4 и, в отношении свидетельств, 12.1.7). Такие процедуры могут оказывать сдерживающее воздействие на сотрудников, которые склонны к игнорированию процедур обеспечения информационной безопасности. Кроме того, подобные процедуры призваны обеспечить корректное и справедливое рассмотрение дел сотрудников, которые подозреваются в серьезных или регулярных нарушениях требований безопасности.

7 Физическая защита и защита от воздействий окружающей среды

7.1 Охраняемые зоны

Цель: предотвращение неавторизованного доступа, повреждения и воздействия в отношении помещений и информации организации.

Средства обработки критичной или важной служебной информации необходимо размещать в зонах безопасности, обозначенных определенным периметром безопасности, обладающим соответствующими защитными барьерами и средствами контроля проникновения. Эти зоны должны быть физически защищены от неавторизованного доступа, повреждения и воздействия.

Уровень защищенности должен быть соразмерен с идентифицированными рисками. С целью минимизации риска неавторизованного доступа или повреждения бумажных документов, носителей данных и средств обработки информации, рекомендуется внедрить политику «чистого стола» и «чистого экрана».

7.1.1 Периметр охраняемой зоны

Физическая защита может быть достигнута созданием нескольких физических барьеров (преград) вокруг помещений компании и средств обработки информации. Барьеры устанавливают отдельные периметры безопасности, каждый из которых обеспечивает усиление защиты в целом. Организациям следует использовать периметры безопасности для защиты зон расположения средств обработки информации (7.1.3). Периметр безопасности — это граница, создающая барьер, например, проходная, оборудованная средствами контроля входа (въезда) по идентификационным карточкам или сотрудник на стойке регистрации. Расположение и уровень защиты (стойкости) каждого барьера зависят от результатов оценки рисков.

Рекомендуется рассматривать и внедрять при необходимости следующие мероприятия по обеспечению информационной безопасности:

- периметр безопасности должен быть четко определен;

- периметр здания или помещений, где расположены средства обработки информации, должен быть физически сплошным (то есть не должно быть никаких промежутков в периметре или мест, через которые можно было бы легко проникнуть). Внешние стены помещений должны иметь достаточно прочную конструкцию, а все внешние двери должны быть соответствующим образом защищены от неавторизованного доступа, например, оснащены устройствами контроля доступа, шлагбаумами, сигнализацией, замками и т.п.;

- должна быть выделенная и укомплектованная персоналом зона регистрации посетителей или должны существовать другие мероприятия по управлению физическим доступом в помещения или здания. Доступ в помещения и здания должен быть предоставлен только авторизованному персоналу;

- физические барьеры, в случае необходимости, должны быть расширены от пола до потолка, для предотвращения неавторизованных проникновений, а также исключения загрязнения окружающей среды в случае пожара или затоплений;

- все противопожарные выходы в периметре безопасности должны быть оборудованы аварийной сигнализацией и плотно закрываться.

7.1.2 Контроль доступа в охраняемые зоны

Зоны информационной безопасности необходимо защищать с помощью соответствующих мер контроля входа для обеспечения уверенности в том, что доступ позволен только авторизованному персоналу. Необходимо рассматривать следующие меры контроля:

- посетители зон безопасности должны сопровождаться или обладать соответствующим допуском; дату и время входа и выхода следует регистрировать. Доступ следует предоставлять только для выполнения определенных авторизованных задач. Необходимо также знакомить посетителей с требованиями безопасности и действиями на случай аварийных ситуаций;

- доступ к важной информации и средствам ее обработки должен контролироваться и предоставляться только авторизованным лицам. Следует использовать средства аутентификации, например, карты доступа плюс PIN-код для авторизации и предоставления соответствующего доступа. Необходимо также надежным образом проводить аудит журналов регистрации доступа;

- необходимо требовать, чтобы весь персонал носил признаки видимой идентификации, следует поощрять его внимание к незнакомым несопровождаемым посетителям, не имеющим идентификационных карт сотрудников;

- права доступа сотрудников в зоны информационной безопасности следует регулярно анализировать и пересматривать.

7.1.3 Безопасность зданий, производственных помещений и оборудования

Зона информационной безопасности может быть защищена путем закрытия на замок самого офиса или нескольких помещений внутри физического периметра безопасности, которые могут быть заперты и иметь запираемые файл-кабинеты или сейфы. При выборе и проектировании безопасной зоны следует принимать во внимание возможные последствия от пожара, наводнения, взрыва, уличных беспорядков и других форм природного или искусственного бедствия. Также следует принимать в расчет соответствующие правила и стандарты в отношении охраны здоровья и безопасности труда. Необходимо рассматривать также любые угрозы безопасности от соседних помещений, например затоплений.

При этом следует предусматривать следующие меры:

- основное оборудование должно быть расположено в местах с ограничением доступа посторонних лиц;

- здания не должны выделяться на общем фоне и должны иметь минимальные признаки своего назначения — не должны иметь очевидных вывесок вне или внутри здания, по которым можно сделать вывод о выполняемых функциях обработки информации;

- подразделения поддержки и оборудование, например, фотокопировальные устройства и факсы, должны быть расположены соответствующим образом в пределах зоны безопасности во избежание доступа, который мог бы скомпрометировать информацию;

- двери и окна необходимо запирать, когда в помещениях нет сотрудников, а также следует предусмотреть внешнюю защиту окон — особенно, низко расположенных;

- необходимо также внедрять соответствующие системы обнаружения вторжений для внешних дверей и доступных для этого окон, которые должны быть профессионально установлены и регулярно тестироваться. Свободные помещения необходимо ставить на сигнализацию. Аналогично следует оборудовать другие помещения, в которых расположены средства коммуникаций;

- необходимо физически изолировать средства обработки информации, контролируемые организацией и используемые третьей стороной;

- справочники и внутренние телефонные книги, идентифицирующие местоположения средств обработки важной информации, не должны быть доступны посторонним лицам;

- следует обеспечивать надежное хранение опасных или горючих материалов на достаточном расстоянии от зоны информационной безопасности. Большие запасы бумаги для печатающих устройств не следует хранить в зоне безопасности без соответствующих мер пожарной безопасности;

- резервное оборудование и носители данных следует располагать на безопасном расстоянии во избежание повреждения от последствий стихийного бедствия в основном здании.

7.1.4 Выполнение работ в охраняемых зонах

Для повышения степени защиты зон информационной безопасности могут потребоваться дополнительные меры по управлению информационной безопасностью и соответствующие руководства. Они должны включать мероприятия в отношении персонала или представителей третьих сторон, работающих в зоне безопасности и состоять в следующем:

- о существовании зоны информационной безопасности и проводимых в ней работах должны быть осведомлены только лица, которым это необходимо в силу производственной необходимости;

- из соображений безопасности и предотвращения возможности злонамеренных действий в охраняемых зонах необходимо избегать случаев работы без надлежащего контроля со стороны уполномоченного персонала;

- пустующие зоны безопасности должны быть физически закрыты, и их состояние необходимо периодически проверять;

- персоналу третьих сторон ограниченный авторизованный и контролируемый доступ в зоны безопасности или к средствам обработки важной информации следует предоставлять только на время такой необходимости. Между зонами с различными уровнями безопасности внутри периметра безопасности могут потребоваться дополнительные барьеры и периметры ограничения физического доступа;

- использование фото, видео, аудио или другого записывающего оборудования должно быть разрешено только при получении специального разрешения.

7.1.5 Изолирование зон приемки и отгрузки материальных ценностей

Зоны приемки и отгрузки материальных ценностей должны находиться под контролем и, по возможности, быть изолированы от средств обработки информации во избежание неавторизованного доступа. Требования безопасности для таких зон должны быть определены на основе оценки рисков. В этих случаях рекомендуется предусматривать следующие мероприятия:

- доступ к зоне складирования с внешней стороны здания должен быть разрешен только определенному и авторизованному персоналу;

- зона складирования должна быть организована так, чтобы поступающие материальные ценности могли быть разгружены без предоставления персоналу поставщика доступа к другим частям здания;

- должна быть обеспечена безопасность внешней(их) двери(ей) помещения для складирования, когда внутренняя дверь открыта;

- поступающие материальные ценности должны быть осмотрены на предмет потенциальных опасностей (7.2.1 г) прежде, чем они будут перемещены из помещения для складирования к местам использования;

- поступающие материальные ценности должны быть зарегистрированы, если это необходимо (5.1).

7.2 Безопасность оборудования

Цель: предотвращение потерь, повреждений или компрометаций активов и нарушения непрерывности деятельности организации.

Оборудование необходимо защищать от угроз его безопасности и воздействий окружающей среды.

Необходимо обеспечивать безопасность оборудования (включая и то, что используется вне организации), чтобы уменьшить риск неавторизованного доступа к данным и защитить их от потери или повреждения. При этом необходимо принимать во внимание особенности, связанные с расположением оборудования и возможным его перемещением. Могут потребоваться специальные мероприятия защиты от опасных воздействий среды или неавторизованного доступа через инфраструктуры обеспечения, в частности, системы электропитания и кабельной разводки.

7.2.1 Расположение и защита оборудования

Оборудование должно быть расположено и защищено так, чтобы уменьшить риски от воздействий окружающей среды и возможности неавторизованного доступа. Необходимо рассматривать следующие мероприятия по управлению информационной безопасностью:

а) оборудование необходимо размещать таким образом, чтобы свести до минимума излишний доступ в места его расположения;

б) средства обработки и хранения важной информации следует размещать так, чтобы уменьшить риск несанкционированного наблюдения за их функционированием;

в) отдельные элементы оборудования, требующие специальной защиты, необходимо изолировать, чтобы повысить общий уровень необходимой защиты;

г) меры по управлению информационной безопасностью должны свести к минимуму риск потенциальных угроз, включая:

1) воровство;
2) пожар;
3) взрыв;
4) задымление;
5) затопление (или перебои в подаче воды);
6) пыль;
7) вибрацию;
8) химические эффекты;
9) помехи в электроснабжении;
10) электромагнитное излучение.

д) в организации необходимо определить порядок приема пищи, напитков и курения вблизи средств обработки информации;

е) следует проводить мониторинг состояния окружающей среды в целях выявления условий, которые могли бы неблагоприятно повлиять на функционирование средств обработки информации;

ж) следует использовать специальные средства защиты, оборудования, расположенного в производственных цехах, например, защитные пленки для клавиатуры;

з) необходимо разработать меры по ликвидации последствий бедствий, случающихся в близлежащих помещениях, например, пожар в соседнем здании, затопление в подвальных помещениях или протекание воды через крышу, взрыв на улице.

7.2.2 Подача электропитания

Оборудование необходимо защищать от перебоев в подаче электроэнергии и других сбоев, связанных с электричеством. Необходимо обеспечивать надлежащую подачу электропитания, соответствующую спецификациям производителя оборудования.

Варианты достижения непрерывности подачи электропитания включают:

- наличие нескольких источников электропитания, чтобы избежать последствий при нарушении его подачи от единственного источника;
- устройства бесперебойного электропитания (UPS);
- резервный генератор.

Чтобы обеспечить безопасное выключение и/или непрерывное функционирование устройств, поддерживающих критические бизнес-процессы, рекомендуется подключать оборудование через UPS. В планах обеспечения непрерывности следует предусматривать действия, которые должны быть предприняты при отказе UPS. Оборудование UPS следует регулярно проверять на наличие адекватной мощности, а также тестировать в соответствии с рекомендациями производителя.

Резервный генератор следует применять, если необходимо обеспечить функционирование оборудования в случае длительного отказа подачи электроэнергии от общего источника. Резервные генераторы следует регулярно проверять в соответствии с инструкциями производителя. Для обеспечения

работы генератора в течение длительного срока необходимо обеспечить соответствующую поставку топлива.

Кроме того, аварийные выключатели электропитания необходимо располагать около запасных выходов помещений, где расположено оборудование, чтобы ускорить отключение электропитания в случае критических ситуаций. Следует обеспечить работу аварийного освещения на случай отказа электропитания, потребляемого от сети. Все здания должны быть оснащены громоотводами, а все внешние линии связи оборудованы специальными грозозащитными фильтрами.

7.2.3 Безопасность кабельной сети

Силовые и телекоммуникационные кабельные сети, по которым передаются данные или осуществляются другие информационные услуги, необходимо защищать от перехвата информации или повреждения. Необходимо рассматривать следующие мероприятия:

а) силовые и телекоммуникационные линии, связывающие средства обработки информации, должны быть, по возможности, подземными или обладать адекватной альтернативной защитой;

б) сетевой кабель должен быть защищен от неавторизованных подключений или повреждения, например, посредством использования специального кожуха и/или выбора маршрутов прокладки кабеля в обход общедоступных участков;

в) силовые кабели должны быть отделены от коммуникационных, чтобы исключить помехи;

г) дополнительные мероприятия по управлению информационной безопасностью для чувствительных или критических систем включают:

1) использование бронированных кожухов, а также закрытых помещений/ящиков в промежуточных пунктах контроля и конечных точках;

2) использование дублирующих маршрутов прокладки кабеля или альтернативных способов передачи;

3) использование оптико-волоконных линий связи;

4) проверки на подключение неавторизованных устройств к кабельной сети.

7.2.4 Техническое обслуживание оборудования

В организации должно проводиться надлежащее техническое обслуживание оборудования для обеспечения его непрерывной работоспособности и целостности. В этих целях следует применять следующие мероприятия:

- оборудование следует обслуживать в соответствии с инструкциями и периодичностью, рекомендуемыми поставщиком;

- необходимо, чтобы техническое обслуживание и ремонт оборудования проводились только авторизованным персоналом;

- следует хранить записи обо всех случаях предполагаемых или фактических неисправностей и всех видах профилактического и восстановительного технического обслуживания;

- необходимо принимать соответствующие меры безопасности при отправке оборудования для технического обслуживания за пределы организации (7.2.6 в отношении удаленных, стертых и перезаписанных данных). Кроме этого должны соблюдаться все требования, устанавливаемые использующимися правилами страхования.

7.2.5 Обеспечение безопасности оборудования, используемого вне помещений организации

Независимо от принадлежности оборудования, его использование для обработки информации вне помещения организации должно быть авторизовано руководством. Уровень информационной безопасности при этом должен быть эквивалентен уровню безопасности в отношении оборудования, используемого с аналогичной целью в помещениях организации, а также с учетом рисков работы на стороне. Оборудование по обработке информации включает все типы персональных компьютеров, электронных записных книжек, мобильных телефонов, а также бумагу или иные материальные ценности, которые используются для работы на дому или транспортируются за пределы рабочих помещений. В этих условиях необходимо применять следующие мероприятия по управлению информационной безопасностью:

- оборудование и носители информации, взятые из помещений организации, не следует оставлять без присмотра в общедоступных местах. При перемещении компьютеры следует перевозить как ручную кладь и, по возможности, не афишировать ее содержимое;

- всегда необходимо соблюдать инструкции изготовителей по защите оборудования, например, от воздействия сильных электромагнитных полей;

- при работе дома следует применять подходящие мероприятия по управлению информационной безопасностью с учетом оценки рисков, например, использовать запираемые файл-кабинеты, соблюдать политику «чистого стола» и контролировать возможность доступа к компьютерам;

- должны иметь место адекватные меры по страхованию для защиты оборудования вне помещений организации.

Риски безопасности, например, связанные с повреждением, воровством и подслушиванием, могут в значительной степени зависеть от расположения оборудования в организации и должны учитываться при определении и выборе наиболее подходящих мероприятий по управлению информационной безопасностью. Более подробная информация о других аспектах защиты мобильного оборудования приведена в 9.8.1.

7.2.6 Безопасная утилизация (списание) или повторное использование оборудования

Служебная информация может быть скомпрометирована вследствие небрежной утилизации (списания) или повторного использования оборудования (8.6.4). Носители данных, содержащие важную информацию, необходимо физически разрушать или перезаписывать безопасным образом, а не использовать стандартные функции удаления. Все компоненты оборудования, содержащего носители данных (встроенные жесткие диски), следует проверять на предмет удаления всех важных данных и лицензионного программного обеспечения. В отношении носителей данных, содержащих важную информацию, может потребоваться оценка рисков с целью определения целесообразности их разрушения, восстановления или выбраковки.

7.3 Общие мероприятия по управлению информационной безопасностью

Цель: предотвращение компрометации или кражи информации и средств обработки информации.

Информацию и средства обработки информации необходимо защищать от раскрытия, кражи или модификации неавторизованными лицами; должны быть внедрены меры, обеспечивающие сведение к минимуму риска их потери или повреждения.

Процедуры обработки и хранения информации рассматриваются в 8.6.3.

7.3.1 Политика «чистого стола» и «чистого экрана»

Организациям следует применять политику «чистого стола» в отношении бумажных документов и сменных носителей данных, а также политику «чистого экрана» в отношении средств обработки информации с тем, чтобы уменьшить риски неавторизованного доступа, потери и повреждения информации как во время рабочего дня, так и при внеурочной работе. При применении этих политик следует учитывать категории информации с точки зрения безопасности (5.2) и соответствующие риски, а также корпоративную культуру организации.

Носители информации, оставленные на столах, также могут быть повреждены или разрушены при бедствии, например, при пожаре, наводнении или взрыве.

Следует применять следующие мероприятия по управлению информационной безопасностью:

- чтобы исключить компрометацию информации, целесообразно бумажные и электронные носители информации, когда они не используются, хранить в надлежащих запирающихся шкафах и/или в других защищенных предметах мебели, особенно в нерабочее время;

- носители с важной или критичной служебной информацией, когда они не требуются, следует убирать и запирать (например, в несгораемом сейфе или шкафу), особенно когда помещение пустует;

- персональные компьютеры, компьютерные терминалы и принтеры должны быть выключены по окончании работы; следует также применять кодовые замки, пароли или другие мероприятия в отношении устройств, находящихся без присмотра;

- необходимо обеспечить защиту пунктов отправки/приема корреспонденции, а также факсимильных и телексных аппаратов в случаях нахождения их без присмотра;

- в нерабочее время фотокопировальные устройства следует запирать на ключ (или защищать от неавторизованного использования другим способом);

- напечатанные документы с важной или конфиденциальной информацией необходимо изымать из принтеров немедленно.

7.3.2 Вынос имущества

Оборудование, информацию или программное обеспечение можно выносить из помещений организации только на основании соответствующего разрешения. Там, где необходимо и уместно, оборудование следует регистрировать при выносе и при вносе, а также делать отметку, когда оно возвращено. С целью выявления неавторизованных перемещений активов и оборудования следует проводить выборочную инвентаризацию. Сотрудники должны быть осведомлены о том, что подобные проверки могут иметь место.

8 Управление передачей данных и операционной деятельностью

8.1 Операционные процедуры и обязанности

Цель: обеспечение уверенности в надлежащем и безопасном функционировании средств обработки информации.

Должны быть установлены обязанности и процедуры по управлению и функционированию всех средств обработки информации. Они должны включать разработку соответствующих операционных инструкций и процедуры реагирования на инциденты.

С целью минимизации риска при неправильном использовании систем вследствие небрежности или злого умысла следует, по возможности, реализовывать принцип разделения полномочий (8.1.4).

8.1.1 Документальное оформление операционных процедур

Операционные процедуры, определяемые политикой безопасности, должны рассматриваться как официальные документы, документироваться и строго соблюдаться, а изменения к ним должны санкционироваться и утверждаться руководством.

Процедуры содержат детальную инструкцию выполнения конкретного задания (работы) и включают:

- обработку и управление информацией;
- определение требований в отношении графика выполнения заданий, включающих взаимосвязи между системами; время начала выполнения самого раннего задания и время завершения самого последнего задания;
- обработку ошибок или других исключительных ситуаций, которые могут возникнуть в течение выполнения заданий, включая ограничения на использование системных утилит (9.5.5);
- необходимые контакты на случай неожиданных операционных или технических проблем;
- специальные мероприятия по управлению выводом данных, например, использование специальной бумаги для печатающих устройств или особых процедур применительно к выводу конфиденциальной информации, включая процедуры для безопасной утилизации выходных данных, не завершенных в процессе выполнения заданий;
- перезапуск системы и процедуры восстановления в случае системных сбоев.

Документированные процедуры должны быть также разработаны в отношении обслуживания систем обработки и обмена информацией, в частности процедуры запуска и безопасного завершения работы компьютера(ов), процедуры резервирования, текущего обслуживания и ремонта оборудования, обеспечения надлежащей безопасности помещений с компьютерным и коммуникационным оборудованием.

8.1.2 Контроль изменений

Изменения конфигурации в средствах и системах обработки информации должны контролироваться надлежащим образом. Неадекватный контроль изменений средств и систем обработки информации — распространенная причина системных сбоев и инцидентов нарушения информационной безопасности. С целью обеспечения надлежащего контроля всех изменений в оборудовании, программном обеспечении или процедурах должны быть определены и внедрены формализованные роли, ответственности и процедуры. При изменении программного обеспечения вся необходимая информация должна фиксироваться и сохраняться в системном журнале аудита. Изменения операционной среды могут оказывать влияние на работу приложений. Везде, где это имеет практический смысл, процедуры управления изменениями в операционной среде и в приложениях должны быть интегрированы (см. также 10.5.1). В частности, необходимо рассматривать следующие мероприятия:

- определение и регистрация существенных изменений;
- оценка возможных последствий таких изменений;
- формализованная процедура утверждения предлагаемых изменений;
- подробное информирование об изменениях всех заинтересованных лиц;
- процедуры, определяющие обязанности по прерыванию и восстановлению работы средств и систем обработки информации, в случае неудачных изменений программного обеспечения.

8.1.3 Процедуры в отношении инцидентов нарушения информационной безопасности

Обязанности и процедуры по управлению в отношении инцидентов должны быть определены для обеспечения быстрой, эффективной и организованной реакции на эти нарушения информационной безопасности (6.3.1). При этом необходимо рассмотреть следующие мероприятия:

а) должны быть определены процедуры в отношении всех возможных типов инцидентов нарушения информационной безопасности, в том числе:

1) сбои информационных систем и утрата сервисов;
2) отказ в обслуживании;

3) ошибки вследствие неполных или неточных данных;

4) нарушения конфиденциальности;

б) в дополнение к обычным планам обеспечения непрерывности (предназначенных для скорейшего восстановления систем или услуг) должны существовать процедуры выполнения требований (6.3.4):

1) анализа и идентификации причины инцидента;

2) планирования и внедрения средств, предотвращающих повторное проявление инцидентов, при необходимости;

3) использования журналов аудита и аналогичных свидетельств;

4) взаимодействия с лицами, на которых инцидент оказал воздействие или участвующих в устранении последствий инцидента;

5) информирования о действиях соответствующих должностных лиц;

в) журналы аудита и аналогичные свидетельства должны быть собраны (12.1.7) и защищены соответствующим образом с целью:

1) внутреннего анализа проблемы;

2) использования как доказательство в отношении возможного нарушения условий контракта, нарушения требований законодательства или, в случае гражданских или уголовных судебных разбирательств, касающихся, например, защиты персональных данных или неправомочного использования компьютеров;

3) ведения переговоров относительно компенсации ущерба с поставщиками программного обеспечения и услуг;

г) действия по устранению сбоев систем и ликвидации последствий инцидентов нарушения информационной безопасности должны быть под тщательным и формализованным контролем. Необходимо наличие процедур с целью обеспечения уверенности в том, что:

1) только полностью идентифицированному и авторизованному персоналу предоставлен доступ к системам и данным в среде промышленной эксплуатации (4.2.2 в отношении доступа третьей стороны);

2) все действия, предпринятые при чрезвычайных обстоятельствах, подробно документально оформлены;

3) о действиях, предпринятых при чрезвычайных обстоятельствах, сообщено руководству организации, и они проанализированы в установленном порядке;

4) целостность бизнес-систем и систем контроля подтверждена в минимальные сроки.

8.1.4 Разграничение обязанностей

Разграничение обязанностей — это способ минимизации риска нештатного использования систем вследствие ошибочных или злонамеренных действий пользователей. Необходимо рассматривать принцип разграничения обязанностей в отношении функций управления, выполнения определенных задач и областей ответственности как способ уменьшения неавторизованной модификации или неправильного использования информации или сервисов.

Для небольших организаций эти мероприятия труднодостижимы, однако данный принцип должен быть применен насколько это возможно. В случаях, когда разделение обязанностей осуществить затруднительно, следует рассматривать использование других мероприятий по управлению информационной безопасностью, таких как мониторинг деятельности, использование журналов аудита, а также мер административного контроля. В то же время важно, чтобы аудит безопасности оставался независимой функцией.

Необходимо предпринимать меры предосторожности, чтобы сотрудник не мог совершить злоупотребления в области своей единоличной ответственности не будучи обнаруженным. Инициирование события должно быть отделено от его авторизации. Необходимо рассматривать следующие мероприятия по управлению информационной безопасностью:

- разграничение полномочий в отношении видов деятельности, которые создают возможность сговора для осуществления мошенничества, например, формирование заказов на закупку и подтверждения получения товаров;

- при наличии опасности сговора мероприятия должны быть продуманы так, чтобы в осуществлении операции участвовали два или более лица для снижения возможности сохранения тайны сговора.

8.1.5 Разграничение сред разработки и промышленной эксплуатации

При разделении сред разработки, тестирования и промышленной эксплуатации необходимо разделить роли и функции сотрудников. Правила перевода программного обеспечения из статуса разрабатываемого в статус принятого к эксплуатации должны быть определены и документально оформлены.

Деятельность, связанная с разработкой и тестированием, может быть причиной серьезных проблем, например нежелательных изменений файлов или системной среды, а также системных сбоев. При этом следует обеспечивать необходимый уровень разделения между средами промышленной эксплуатации по отношению к средам тестирования, а также для предотвращения операционных сбоев. Аналогичное разделение следует также реализовывать между функциями разработки и тестирования. В этом случае необходимо поддерживать в рабочем состоянии отдельную среду, в которой следует выполнять комплексное тестирование с известной стабильностью и предотвращать несанкционированный доступ со стороны разработчиков.

Там, где сотрудники, отвечающие за разработку и тестирование, имеют доступ к системе и данным среды промышленной эксплуатации, они имеют возможность установить неавторизованную и непротестированную программу или изменить данные в операционной среде. Применительно к ряду систем эта возможность могла бы быть использована с целью злоупотребления, а именно для совершения мошенничества или установки непротестированной или вредоносной программы. Непротестированное или вредоносное программное обеспечение может быть причиной серьезных проблем в операционной среде. Разработчики и специалисты, проводящие тестирование, могут также быть причиной угроз для безопасности операционной информации и системы.

Кроме того, если разработка и тестирование производятся в одной компьютерной среде, это может стать причиной непреднамеренных изменений программного обеспечения и информации. Разделение сред разработки, тестирования и эксплуатации является, следовательно, целесообразным для уменьшения риска случайного изменения или неавторизованного доступа к программному обеспечению и бизнес-данным среды промышленной эксплуатации. Необходимо рассматривать следующие мероприятия по управлению информационной безопасностью:

- программное обеспечение для разработки и эксплуатации, по возможности, должно работать на различных компьютерных процессорах или в различных доменах или директориях;
- действия по разработке и тестированию должны быть разделены, насколько это возможно;
- компиляторы, редакторы и другие системные утилиты не должны быть доступны в операционной среде без крайней необходимости;
- чтобы уменьшить риск ошибок, для операционных и тестовых систем должны использоваться различные процедуры регистрации (входа в систему). Пользователям следует рекомендовать применение различных паролей для этих систем, а в их экранных меню должны показываться соответствующие идентификационные сообщения;
- разработчики могут иметь доступ к паролям систем операционной среды только в том случае, если внедрены специальные мероприятия по порядку предоставления паролей для поддержки среды промышленной эксплуатации. Эти меры должны обеспечивать смену паролей после использования.

8.1.6 Управление средствами обработки информации сторонними лицами и/или организациями

Использование сторонних подрядчиков для управления средствами обработки информации является потенциальной угрозой для безопасности, поскольку возникает возможность компрометации, повреждения или потери данных в организации подрядчика. Такие риски должны быть идентифицированы заранее, а соответствующие мероприятия по управлению информационной безопасностью согласованы с подрядчиком и включены в контракт (4.2.2 и 4.3 в отношении руководств по контрактам с третьей стороной, предусматривающих доступ к средствам обработки информации организации и в отношении контрактов по аутсорсингу).

В этих условиях требуется решение специальных вопросов:

- идентификация важных или критических бизнес-приложений, которые лучше оставить в организации;
- получение одобрения владельцев коммерческих бизнес-приложений;
- оценка влияния на планы обеспечения непрерывности бизнеса;
- определение перечня стандартов безопасности, которые должны быть включены в контракты, и процедур проверки выполнения их требований;
- распределение конкретных обязанностей и процедур для эффективного мониторинга всех применяемых видов деятельности, связанных с информационной безопасностью;
- определение обязанностей и процедур в отношении информирования и управления процессами ликвидации последствий инцидентов нарушения информационной безопасности (8.1.3).

8.2 Планирование нагрузки и приемка систем

Цель: сведение к минимуму риска сбоев в работе систем.

Для обеспечения доступности данных, требуемой производительности и ресурсов систем необходимо провести предварительное планирование и подготовку.

Для снижения риска перегрузки систем необходимо проводить анализ предполагаемой ее нагрузки.

Требования к эксплуатации новых систем должны быть определены, документально оформлены и протестированы перед их приемкой и использованием.

8.2.1 Планирование производительности

Для обеспечения необходимых мощностей по обработке и хранению информации необходим анализ текущих требований к производительности, а также прогноз будущих. Эти прогнозы должны учитывать новые функциональные и системные требования, а также текущие планы и перспективные планы развития информационных технологий в организации.

Мэйнфреймы требуют особого внимания вследствие значительных финансовых и временных затрат на повышение их производительности. Руководители, отвечающие за предоставление мэйнфреймовых услуг, должны проводить мониторинг загрузки ключевых системных ресурсов, в том числе процессоров, оперативной и внешней памяти, принтеров и других устройств вывода, а также систем связи. Эти руководители должны определять общие потребности и тенденции в использовании компьютерных ресурсов, что особенно важно для поддержки бизнес-приложений или систем управления для руководства.

Руководителям следует использовать эту информацию с целью идентификации/избежания потенциально узких мест, представляющих угрозу безопасности системы или пользовательским сервисам, а также с целью планирования соответствующих мероприятий по обеспечению информационной безопасности.

8.2.2 Приемка систем

Перед приемкой систем должны быть определены критерии приемки новых информационных систем, новых версий и обновлений, а также должно проводиться необходимое их тестирование. Требования и критерии для принятия новых систем должны быть четко определены, согласованы, документально оформлены и опробованы. В этих целях необходимо предусматривать следующие мероприятия по управлению информационной безопасностью:

- оценка выполнения требований к мощности и производительности компьютера;
- определение процедур восстановления после сбоев и повторного запуска, а также формирование планов обеспечения непрерывной работы;
- подготовка и тестирование типовых операционных процессов на соответствие определенным стандартам;
- наличие необходимого набора средств контроля информационной безопасности;
- разработка эффективных руководств по процедурам;
- обеспечение непрерывности бизнеса в соответствии с требованиями 11.1;
- обязательная проверка отсутствия неблагоприятного влияния новых систем на существующие, особенно во время максимальных нагрузок, например, в конце месяца;
- контроль проведения анализа влияния, оказываемого новой системой на общую информационную безопасность организации;
- организация профессиональной подготовки персонала к эксплуатации и использованию новых систем.

Для консультаций на всех этапах разработки новых систем должны привлекаться службы поддержки (эксплуатации) и пользователи с целью обеспечения эффективной эксплуатации проектируемой системы. При этом должны проводиться соответствующие тесты для подтверждения того, что все критерии приемки удовлетворены полностью.

8.3 Защита от вредоносного программного обеспечения

Цель: обеспечение защиты целостности программного обеспечения и массивов информации.

Необходимо принимать меры предотвращения и обнаружения внедрения вредоносного программного обеспечения.

Программное обеспечение и средства обработки информации уязвимы к внедрению вредоносного программного обеспечения, такого как компьютерные вирусы, сетевые «черви», «троянские кони» (10.5.4) и логические бомбы. Пользователи должны быть осведомлены об опасности использования неавторизованного или вредоносного программного обеспечения, а соответствующие руководители должны обеспечить внедрение специальных средств контроля с целью обнаружения и/или предотвращения проникновения подобных программ. В частности, важно принятие мер предосторожности с целью обнаружения и предотвращения заражения компьютерными вирусами персональных компьютеров.

8.3.1 Мероприятия по управлению информационной безопасностью для борьбы с вредоносным программным обеспечением

С целью обнаружения и предотвращения проникновения вредоносного программного обеспечения необходимо планирование и реализация мероприятий по управлению информационной безопасностью, а также формирование процедур, обеспечивающих соответствующую осведомленность пользователей. Защита от вредоносного программного обеспечения должна основываться на понимании требований безопасности, соответствующих мерах контроля доступа к системам и надлежащем управлении изменениями. Необходимо рассматривать следующие мероприятия по управлению информационной безопасностью:

- документированную политику, требующую соблюдения лицензионных соглашений и устанавливающую запрет на использование неавторизованного программного обеспечения (12.1.2.2);

- документированную политику защиты от рисков, связанных с получением файлов и программного обеспечения из внешних сетей, через внешние сети или из любой другой среды. В этой политике должно содержаться указание о необходимости принятия защитных мер (10.5, 10.5.4, 10.5.5);

- установку и регулярное обновление антивирусного программного обеспечения для обнаружения и сканирования компьютеров и носителей информации, запускаемого в случае необходимости в качестве превентивной меры или рутинной процедуры;

- проведение регулярных инвентаризаций программного обеспечения и данных систем, поддерживающих критические бизнес-процессы. Необходима также формализованная процедура по расследованию причин появления любых неавторизованных или измененных файлов в системе;

- проверку всех файлов на носителях информации сомнительного или неавторизованного происхождения или файлов, полученных из общедоступных сетей, на наличие вирусов перед работой с этими файлами;

- проверку любых вложений электронной почты и скачиваемой информации на наличие вредоносного программного обеспечения до их использования.

Эта проверка может быть выполнена в разных точках, например, на электронной почте, персональных компьютерах или при входе в сеть организации;

- управленческие процедуры и обязанности, связанные с защитой от вирусов, обучение применению этих процедур, а также вопросы оповещения и восстановления после вирусных атак (6.3, 8.1.3);

- соответствующие планы по обеспечению непрерывности бизнеса в части восстановления после вирусных атак, включая все необходимые мероприятия по резервированию и восстановлению данных и программного обеспечения (раздел 11);

- процедуры по контролю всей информации, касающейся вредоносного программного обеспечения, обеспечение точности и информативности предупредительных сообщений. Для определения различия между ложными и реальными вирусами должны использоваться профессиональные источники, например, респектабельные журналы, заслуживающие доверия интернет-сайты или поставщики антивирусного программного обеспечения. Персонал должен быть осведомлен о проблеме ложных вирусов и действиях при их получении.

Эти мероприятия особенно важны в отношении сетевых файловых серверов, обслуживающих большое количество рабочих станций.

8.4 Вспомогательные операции

Цель: поддержание целостности и доступности услуг по обработке информации и связи.

В соответствии с утвержденной стратегией должны устанавливаться регулярные процедуры резервирования прикладного программного обеспечения (11.1), формирования копий данных и тестирования, их своевременного восстановления, регистрации событий и ошибок и, где необходимо, мониторинга состояния аппаратных средств.

8.4.1 Резервирование информации

Резервное копирование важной служебной информации и программного обеспечения должно выполняться на регулярной основе. Следует обеспечивать адекватные средства резервирования для обеспечения уверенности в том, что вся важная деловая информация и программное обеспечение смогут быть восстановлены после бедствия или сбоя оборудования. Мероприятия по резервированию для каждой отдельной системы должны регулярно тестироваться для обеспечения уверенности в том, что они удовлетворяют требованиям планов по обеспечению непрерывности бизнеса (раздел 11). В этих случаях целесообразно применять следующие мероприятия по управлению информационной безопасностью:

- минимально необходимый объем резервной информации, вместе с точными и полными регистрационными записями по содержанию резервных копий, а также документация по процедурам восста-

новления во избежание любого повреждения от стихийных бедствий должны храниться в достаточно отдаленном месте от основного здания. По крайней мере три поколения (цикла) резервной информации должны быть сохранены для важных бизнес-приложений:

- резервная информация должна быть обеспечена гарантированным уровнем физической защиты и защиты от воздействий окружающей среды (раздел 7) в соответствии с уровнем безопасности в основном здании. Мероприятия, применяемые к оборудованию в основном здании, должны распространяться на резервный пункт;

- резервное оборудование должно регулярно подвергаться тестированию для обеспечения уверенности в том, что в случае возникновения чрезвычайных ситуаций на его работу можно положиться;

- процедуры восстановления следует регулярно актуализировать и тестировать для обеспечения уверенности в их эффективности, а также в том, что для выполнения этих процедур потребуется не больше времени, чем определено операционными процедурами восстановления.

Следует определять периоды хранения важной служебной информации, а также учитывать требования к архивным копиям долговременного хранения (12.1.3).

8.4.2 Журналы действий оператора

Операторы должны вести журнал, в котором следует фиксировать:

- время начала и завершения работы системы;

- ошибки системы и предпринятые корректирующие действия;

- подтверждение правильной обработки данных файлов и выходных данных компьютера;

- личные данные (например, фамилия, должность) производящего записи в журнал специалиста.

Журналы оператора должны быть предметом постоянных независимых проверок на соответствие требованиям операционных процедур.

8.4.3 Регистрация ошибок

Об ошибках необходимо докладывать и принимать корректирующие действия в соответствии с установленным порядком. Необходимо регистрировать сообщения пользователей об ошибках, связанных с обработкой информации или системами связи. Должны существовать четкие правила обработки допущенных ошибок, включающие:

- анализ ошибок для обеспечения уверенности в том, что они были удовлетворительным образом устранены;

- анализ предпринятых корректирующих мер, обеспечивающих уверенность в том, что мероприятия по управлению информационной безопасностью не были скомпрометированы (нарушены) и предпринятые действия надлежащим образом авторизованы.

8.5 Управление сетевыми ресурсами

Цель: обеспечение безопасности информации в сетях и защиты поддерживающей инфраструктуры.

Управление безопасностью сетей, которые могут быть расположены за пределами границ организации, требует внимания.

Дополнительные мероприятия по управлению информационной безопасностью могут также потребоваться для защиты важных данных, передаваемых через общедоступные сети.

8.5.1 Средства контроля сетевых ресурсов

Для обеспечения требуемого уровня безопасности компьютерных сетей и его поддержки требуется комплекс средств контроля. Руководители, отвечающие за поддержку сетевых ресурсов, должны обеспечивать внедрение средств контроля безопасности данных в сетях и защиту подключенных сервисов от неавторизованного доступа. В частности, необходимо рассматривать следующие меры и средства управления информационной безопасностью:

- следует распределять ответственность за поддержание сетевых ресурсов и компьютерных операций (8.1.4);

- следует устанавливать процедуры и обязанности по управлению удаленным оборудованием, включая оборудование, установленное у конечных пользователей;

- если необходимо, специальные средства контроля следует внедрять для обеспечения конфиденциальности и целостности данных, проходящих по общедоступным сетям, а также для защиты подключенных систем (9.4 и 10.3). Могут также потребоваться специальные средства контроля для поддержания доступности сетевых серверов и рабочих станций;

- действия по управлению необходимо тщательно соизмерять как с требованиями к сервисам от бизнеса, так и с общими требованиями к обеспечению безопасности инфраструктуры обработки информации.

8.6 Безопасность носителей информации

Цель: предотвращение повреждений активов и прерываний бизнес-процессов. Использование носителей информации должно контролироваться, а также должна обеспечиваться их физическая безопасность.

Должны быть определены соответствующие процедуры защиты документов, компьютерных носителей информации (лент, дисков, кассет), данных ввода/вывода и системной документации от повреждений, воровства и неправомочного доступа.

8.6.1 Использование сменных носителей компьютерной информации

Должны существовать процедуры по использованию сменных носителей компьютерной информации (лент, дисков, кассет, а также печатных отчетов). В этих случаях необходимо рассматривать следующие мероприятия по управлению информационной безопасностью:

- если носители информации многократного использования больше не требуются и передаются за пределы организации, то их содержимое должно быть уничтожено;
- в отношении всех уничтожаемых носителей информации должно быть принято соответствующее решение, а также должна быть сделана запись в регистрационном журнале, который следует хранить (8.7.2);
- все носители информации следует хранить в надежном, безопасном месте в соответствии с требованиями изготовителей.

Все процедуры авторизации должны быть четко документированы.

8.6.2 Утилизация носителей информации

Носители информации по окончании использования следует надежно и безопасно утилизировать. Важная информация может попасть в руки посторонних лиц из-за небрежной утилизации носителей данных. Чтобы свести к минимуму такой риск, должны быть установлены формализованные процедуры безопасной утилизации носителей информации. Для этого необходимо предусматривать следующие мероприятия:

а) носители, содержащие важную информацию, следует хранить и утилизировать надежно и безопасно (например, посредством сжигания/измельчения). Если носители планируется использовать в пределах организации для других задач, то информация на них должна быть уничтожена;

б) ниже приведен перечень объектов, в отношении которых может потребоваться безопасная утилизация:

1) бумажные документы;
2) речевые или другие записи;
3) копировальная бумага;
4) выводимые отчеты;
5) одноразовые ленты для принтеров;
6) магнитные ленты;
7) сменные диски или кассеты;
8) оптические носители данных (все разновидности, в том числе носители, содержащие программное обеспечение, поставляемое производителями);
9) тексты программ;
10) тестовые данные;
11) системная документация;

в) может оказаться проще принимать меры безопасной утилизации в отношении всех носителей информации, чем пытаться сортировать носители по степени важности;

г) многие организации предлагают услуги по сбору и утилизации бумаги, оборудования и носителей информации. Следует тщательно выбирать подходящего подрядчика с учетом имеющегося у него опыта и обеспечения необходимого уровня информационной безопасности;

д) по возможности следует регистрировать утилизацию важных объектов с целью последующего аудита.

При накоплении носителей информации, подлежащих утилизации, следует принимать во внимание «эффект накопления», то есть большой объем открытой информации может сделать ее более важной.

8.6.3 Процедуры обработки информации

С целью обеспечения защиты информации от неавторизованного раскрытия или неправильного использования необходимо определить процедуры обработки и хранения информации. Эти процедуры должны быть разработаны с учетом категорирования информации (5.2), а также в отношении документов, вычислительных систем, сетей, переносных компьютеров, мобильных средств связи, почты, рече-

вой почты, речевой связи вообще, мультимедийных устройств, использования факсов и любых других важных объектов, например, бланков, чеков и счетов. Необходимо использовать следующие мероприятия по управлению информационной безопасностью (5.2 и 8.7.2):

- обработку и маркирование всех носителей информации (8.7.2а);
- ограничения доступа с целью идентификации неавторизованного персонала;
- обеспечение формализованной регистрации авторизованных получателей данных;
- обеспечение уверенности в том, что данные ввода являются полными, процесс обработки завершается должным образом и имеется подтверждение вывода данных;
- обеспечение защиты информации, находящейся в буфере данных и ожидающей вывода в соответствии с важностью этой информации;
- хранение носителей информации в соответствии с требованиями изготовителей;
- сведение рассылки данных к минимуму;
- четкую маркировку всех копий данных, предлагаемых вниманию авторизованного получателя;
- регулярный пересмотр списков рассылки и списков авторизованных получателей.

8.6.4 Безопасность системной документации

Системная документация может содержать определенную важную информацию, например, описания процессов работы бизнес-приложений, процедур, структур данных, процессов авторизации (9.1). В этих условиях с целью защиты системной документации от неавторизованного доступа необходимо применять следующие мероприятия:

- системную документацию следует хранить безопасным образом;
- список лиц, имеющих доступ к системной документации, следует сводить к минимуму; доступ должен быть авторизован владельцем бизнес-приложения;
- системную документацию, полученную/поддерживаемую через общедоступную сеть, следует защищать надлежащим образом.

8.7 Обмен информацией и программным обеспечением

Цель: предотвращение потери, модификации или неправильного использования информации при обмене ею между организациями.

Обмен информацией и программным обеспечением между организациями должен быть под контролем и соответствовать действующему законодательству (раздел 12).

Обмен информацией должен происходить на основе соглашений между организациями. Необходимо определить процедуры и мероприятия по защите информации и носителей при передаче. Необходимо учитывать последствия для деятельности и безопасности организации, связанные с электронным обменом данных, электронной торговлей и электронной почтой, а также требования к мероприятиям по управлению информационной безопасностью.

8.7.1 Соглашения по обмену информацией и программным обеспечением

Порядок обмена информацией и программным обеспечением (как электронным способом, так и вручную) между организациями, включая передачу на хранение исходных текстов программ третьей стороне, должен быть строго формализован и документирован. Требования безопасности в подобных соглашениях должны учитывать степень важности информации, являющейся предметом обмена. Необходимо, чтобы требования безопасности в подобных соглашениях учитывали:

- обязанности руководства по контролю и уведомлению о передаче, отправке и получении информации;
- процедуры для уведомления отправителя о передаче, отправке и получении информации;
- минимальные технические требования по формированию и передаче пакетов данных;
- требования к курьерской службе;
- ответственность и обязательства в случае потери данных;
- использование согласованной системы маркировки для важной или критичной информации, обеспечивающей уверенность в том, что значение этой маркировки будет сразу же понятно и информация будет соответственно защищена;
- определение владельцев информации и программного обеспечения, а также обязанностей по защите данных, учет авторских прав на программное обеспечение и аналогичных вопросов (12.1.2 и 12.1.4);
- технические требования в отношении записи и считывания информации и программного обеспечения;

- любые специальные средства контроля, которые могут потребоваться для защиты важных объектов, например криптографические ключи (10.3.5).

8.7.2 Безопасность носителей информации при пересылке

Информация может быть искажена или скомпрометирована вследствие неавторизованного доступа, неправильного использования или искажения во время физической транспортировки, например, при пересылке носителей информации по почте или через курьера. Для защиты информации, передаваемой между организациями, необходимо применять следующие меры:

а) следует использовать надежных перевозчиков или курьеров. Список авторизованных курьеров необходимо согласовывать с руководством, кроме того, следует внедрить процедуру проверки идентификации курьеров;

б) упаковка должна быть достаточной для защиты содержимого от любого физического повреждения, которое может иметь место при транспортировке, и соответствовать требованиям изготовителей носителей информации;

в) специальные средства контроля следует применять, при необходимости, для защиты важной информации от неавторизованного раскрытия или модификации. Например:

1) использование запертых контейнеров;

2) личную доставку;

3) использование упаковки, которую нельзя нарушить незаметно (на которой видна любая попытка вскрытия);

4) в исключительных случаях, разбивку отправления на несколько частей, пересылаемых различными маршрутами;

5) использование цифровых подписей и шифрования для обеспечения конфиденциальности (10.3).

8.7.3 Безопасность электронной торговли

В электронной торговле могут использоваться различные способы обмена данными, например, в электронном виде (EDI), через электронную почту и транзакции в режиме он-лайн через общедоступные сети, в частности, Интернет. Электронная торговля подвержена ряду сетевых угроз, которые могут привести к краже, оспариванию контрактов, а также раскрытию или модификации информации. Чтобы защитить электронную торговлю от таких угроз, необходимо применять соответствующие мероприятия по управлению информационной безопасностью. Для обеспечения безопасности электронной торговли необходимо проанализировать степень достоверности и обоснованности предлагаемых поставщиками мер обеспечения информационной безопасности:

- аутентификация. С какой степенью клиенту и продавцу следует проверять идентификацию друг друга?

- авторизация. Кто уполномочен устанавливать цены, подготавливать или подписывать ключевые коммерческие документы? Каким образом об этом может быть проинформирован торговый партнер?

- процессы в отношении контрактов и тендеров. Какие требования существуют в отношении конфиденциальности, целостности, подтверждения отправки и получения ключевых документов, а также в невозможности отказа от совершенных сделок?

- информация о ценах. Насколько можно доверять рекламе прайс-листов и конфиденциальности в отношении существенных скидок?

- обработка заказов. Как обеспечиваются конфиденциальность и целостность деталей заказа, условий оплаты и адреса поставки, а также подтверждение при его получении?

- контрольные проверки. Какая степень контроля является достаточной, чтобы проверить информацию об оплате, представленную клиентом?

- расчеты. Какая форма оплаты является наиболее защищенной от мошенничества?

- оформление заказов. Какая требуется защита, чтобы обеспечить конфиденциальность и целостность информации о заказах, а также избежать потери или дублирования сделок?

- ответственность. Кто несет ответственность за риск любых мошеннических сделок?

Многие из вышеупомянутых проблем могут быть решены с использованием криптографических методов, изложенных в 10.3, при этом необходимо обеспечивать соответствие требованиям законодательства (12.1, 12.1.6 относительно законодательства в области криптозащиты).

Соглашения между партнерами в области электронной торговли следует сопровождать документально оформленными договорами, которые устанавливают и документально оформляют между сторонами условия заключения сделок, включая детали авторизации. Могут потребоваться также дополнительные соглашения с поставщиками сетевых и информационных услуг.

Магазины (сети) электронной торговли, ориентированные на массового потребителя, должны обнародовать условия заключения сделок.

Необходимо обеспечивать устойчивость к вирусным атакам в процессе проведения электронной торговли, а также предусматривать последствия для безопасности всех сетевых взаимосвязей при ее осуществлении (9.4.7).

8.7.4 Безопасность электронной почты

8.7.4.1 Риски безопасности

Электронная почта используется для обмена служебной информацией, заменяя традиционные формы связи, такие как телекс и почта. Электронная почта отличается от традиционных форм бизнес-коммуникаций скоростью, структурой сообщений, определенной упрощенностью, а также уязвимостью к неавторизованным действиям. При этом необходимо учитывать потребность в средствах контроля для уменьшения рисков безопасности, связанных с электронной почтой. При оценке рисков безопасности необходимо учитывать, в частности:

- уязвимость сообщений по отношению к возможности неавторизованного доступа или модификации, а также к отказу в обслуживании;
- повышенную чувствительность к ошибкам, например указанию ошибочного или неверного адреса, а также к общей надежности и доступность данной услуги;
- влияние изменения средств передачи информации на бизнес-процессы, например эффект от увеличенной скорости доставки сообщений, а также эффект, связанный с обменом официальными сообщениями между людьми, а не между организациями;
- юридические вопросы, такие как возможная необходимость в доказательстве авторства сообщения, а также фактов ее отправки, доставки и получения;
- последствия, связанные с приданием гласности списка сотрудников, имеющих электронную почту;
- вопросы, связанные с управлением удаленным доступом к электронной почте.

8.7.4.2 Политика в отношении электронной почты

Организациям следует внедрить четкие правила использования электронной почты, предусматривающие следующие аспекты:

- вероятность атаки на электронную почту (вирусы, перехват);
- защиту вложений в сообщения электронной почты;
- данные, при передаче которых не следует пользоваться электронной почтой;
- исключение возможности компрометации организации со стороны сотрудников, например, путем рассылки дискредитирующих и оскорбительных сообщений, использование корпоративной электронной почты с целью неавторизованных покупок;
- использование криптографических методов для защиты конфиденциальности и целостности электронных сообщений (10.3);
- хранение сообщений, которые, в этом случае, могли бы быть использованы в случае судебных разбирательств;
- дополнительные меры контроля обмена сообщениями, которые не могут быть аутентифицированы.

8.7.5 Безопасность электронных офисных систем

Необходимо разработать и внедрить политики безопасности и руководства с целью управления рисками бизнеса и информационной безопасностью, связанные с электронными офисными системами. Эти системы обеспечивают возможности для быстрого распространения и совместного использования служебной информации путем использования сочетания возможностей документов, компьютеров, переносных компьютеров, мобильных средств связи, почты, электронной почты, речевой связи вообще, мультимедийных систем, сервисов доставки почтовых отправлений и факсов.

Необходимо учитывать последствия для информационной безопасности и бизнес-процессов от взаимодействия вышеуказанных средств, в частности:

- уязвимость информации в офисных системах, связана, например, с записью телефонных разговоров или переговоров по конференц-связи, конфиденциальностью звонков, хранением факсов, вскрытием и рассылкой почты;
- уязвимость информации, предназначенной для совместного использования, например, при использовании корпоративных электронных досок объявления (9.1);
- исключение использования офисных систем в отношении категорий важной служебной информации, если эти системы не обеспечивают соответствующий уровень защиты (5.2);
- уязвимость доступа к данным личных ежедневников отдельных сотрудников, например, работающих на важных проектах;
- возможность или невозможность офисных систем поддерживать бизнес-приложения, например, в части передачи заказов или авторизации;

- категории сотрудников, подрядчиков или деловых партнеров, которым разрешено использовать систему и рабочие места, с которых может осуществляться к ней доступ (4.2);

- ограничение определенных возможностей системы для определенных категорий пользователей;

- идентификацию статуса пользователей, например служащих организации или подрядчиков, в отдельных директориях, для удобства других пользователей;

- сохранение и резервирование информации, содержащейся в системе (12.1.3, 8.4.1);

- требования по переходу на аварийный режим работы и перечень соответствующих мероприятий (11.1).

8.7.6 Системы публичного доступа

Следует уделять внимание защите целостности информации, опубликованной электронным способом, чтобы предотвратить неавторизованную модификацию, которая могла бы навредить репутации организации, поместившей эту информацию. Информацию системы публичного доступа, например информацию на Web-сайте, доступную через Интернет, возможно, потребуется привести в соответствие с законодательством и регулирующими нормами страны, под юрисдикцией которых находится система или осуществляется торговля. Необходим соответствующий формализованный процесс авторизации прежде, чем информация будет сделана общедоступной.

Программное обеспечение, данные и другую информацию, требующую высокого уровня целостности, доступ к которой осуществляется через системы публичного доступа, необходимо защищать адекватными способами, например, посредством цифровой подписи (10.3.3). Системы, предоставляющие возможность электронной публикации информации, обратной связи и непосредственного ввода информации, должны находиться под надлежащим контролем с тем, чтобы:

- полученная информация соответствовала всем законам по защите данных (12.1.4);

- информация, введенная в систему электронной публикации, обрабатывалась своевременно, полностью и точно;

- важная информация была защищена в процессе ее сбора и хранения;

- доступ к системе электронной публикации исключал бы возможность непреднамеренного доступа к сетям, с которыми она связана.

8.7.7 Другие формы обмена информацией

Необходимо предусмотреть наличие процедур и мероприятий по управлению информационной безопасностью с целью защиты процесса обмена информацией посредством речевых, факсимильных и видеосредств коммуникаций. Информация может быть скомпрометирована из-за недостаточной осведомленности сотрудников по использованию средств передачи информации. В частности, информация может быть подслушана при переговорах по мобильному телефону в общественном месте, а также с автоответчиков; информация может также быть скомпрометированной вследствие неавторизованного доступа к системе голосовой почты или случайной отсылки факсимильных сообщений неправильному адресату.

Бизнес-операции могут быть нарушены и информация может быть скомпрометирована в случае отказа, перегрузки или прерывания в работе средств взаимодействия (7.2 и раздел 11). Информация может быть скомпрометирована, если к ней имели место доступ неавторизованные пользователи (раздел 9).

Следует сформулировать четкие требования по соблюдению процедур, которым должны следовать сотрудники при использовании речевой, факсимильной и видеосвязи. В частности, необходимо предусмотреть следующее:

а) напоминание сотрудникам о необходимости принятия соответствующих мер предосторожности, например, для исключения подслушивания или перехвата информации при использовании телефонной связи:

1) лицами, находящимися в непосредственной близости, особенно при пользовании мобильными телефонами;

2) прослушивания телефонных переговоров путем физического доступа к трубке, телефонной линии или с использованием сканирующих приемников при применении аналоговых мобильных телефонов;

3) посторонними лицами со стороны адресата;

б) напоминание сотрудникам о том, что не следует вести конфиденциальные беседы в общественных местах, открытых офисах и в переговорных комнатах с тонкими стенами;

в) не оставлять сообщений на автоответчиках, переадресация на которые произошла вследствие ошибки соединения, или автоответчиках операторов связи, поскольку эти сообщения могут быть воспроизведены неавторизованными лицами;

г) напоминание сотрудникам о возможных рисках, присущих использованию факсимильных аппаратов, а именно:

1) неавторизованный доступ к встроенной памяти для поиска сообщений;

2) преднамеренное или случайное перепрограммирование аппаратов с целью передачи сообщений по определенным номерам;

3) отсылка документов и сообщений по неправильному номеру вследствие неправильного набора либо из-за использования неправильно сохраненного номера.

9 Контроль доступа

9.1 Требование бизнеса по обеспечению контроля в отношении логического доступа

Цель: контроль доступа к информации.

Доступ к информации и бизнес-процессам должен быть контролируемым с учетом требований бизнеса и безопасности.

Требования к контролю доступа должны быть отражены в политиках в отношении распространения и авторизации информации.

9.1.1 Политика в отношении логического доступа

9.1.1.1 Политика и требования бизнеса

Необходимо определять и документально оформлять требования бизнеса по обеспечению контроля в отношении логического доступа. Правила контроля доступа и права каждого пользователя или группы пользователей должны однозначно определяться политикой безопасности по отношению к логическому доступу. Пользователи и поставщики услуг должны быть оповещены о необходимости выполнения требований в отношении логического доступа.

Необходимо, чтобы в политике было учтено следующее:

- требования безопасности конкретных бизнес-приложений;
- идентификация всей информации, связанной с функционированием бизнес-приложений;
- условия распространения информации и авторизации доступа, например, применение принципа «need to know» (пользователь получает доступ только к данным, безусловно необходимым ему для выполнения конкретной функции), а также в отношении категорированной информации и требуемых уровней ее защиты;
- согласованность между политиками по контролю доступа и классификации информации применительно к различным системам и сетям;
- применяемое законодательство и любые договорные обязательства относительно защиты доступа к данным или сервисам (раздел 12);
- стандартные профили доступа пользователей для типовых обязанностей и функций;
- управление правами доступа в распределенной сети с учетом всех типов доступных соединений.

9.1.1.2 Правила контроля доступа

При определении правил контроля доступа следует принимать во внимание следующее:

- дифференциацию между правилами, обязательными для исполнения, и правилами, которые являются общими или применяемыми при определенных условиях;
- установление правил, основанных на предпосылке «все должно быть в общем случае запрещено, пока явно не разрешено», а не на более слабом принципе «все в общем случае разрешено, пока явно не запрещено»;
- изменения в признаках маркировки информации (см. 5.2) как генерируемых автоматически средствами обработки информации, так и инициируемых по усмотрению пользователей;
- изменения в правах пользователя как устанавливаемых автоматически информационной системой, так и определенных администратором;
- правила, которые требуют одобрения администратора или другого лица перед применением, а также те, которые не требуют специального одобрения.

9.2 Контроль в отношении доступа пользователей

Цель: предотвращение неавторизованного доступа к информационным системам.

Для контроля за предоставление права доступа к информационным системам и сервисам необходимо наличие формализованных процедур.

Необходимо, чтобы процедуры охватывали все стадии жизненного цикла пользовательского доступа от начальной регистрации новых пользователей до конечного снятия с регистрации пользователей, которым больше не требуется доступ к информационным системам и сервисам. Особое внимание сле-

дует уделять мероприятиям в отношении предоставления прав привилегированного доступа, с помощью которых пользователи могут обходить системные средства контроля.

9.2.1 Регистрация пользователей

Необходимо существование формализованной процедуры регистрации и снятия с регистрации пользователей в отношении предоставления доступа ко всем многопользовательским информационным системам и сервисам.

Доступ к многопользовательским информационным сервисам должен быть контролируемым посредством формализованного процесса регистрации пользователей, который должен включать:

- использование уникальных ID (идентификаторов или имен) пользователей таким образом, чтобы действия в системе можно было бы соотнести с пользователями и установить ответственных. Использование групповых ID следует разрешать только в тех случаях, где это необходимо, с учетом особенностей выполняемой работы;
- проверку того, что пользователь имеет авторизацию от владельца системы на пользование информационной системой или сервисов. Кроме того, может быть целесообразным наличие дополнительного разрешения на предоставление прав от руководства;
- проверку того, что уровень предоставленного доступа соответствует производственной необходимости (9.1), а также учитывает требования политики безопасности организации, например, не нарушает принципа разделения обязанностей (8.1.4);
- предоставление пользователям письменного документа, в котором указаны их права доступа;
- требование того, чтобы пользователи подписывали документ о том, что они понимают условия предоставления доступа;
- обеспечение уверенности в том, что поставщики услуг не предоставляют доступ, пока процедуры авторизации не завершены;
- ведение формализованного учета в отношении всех лиц, зарегистрированных для использования сервисов;
- немедленную отмену прав доступа пользователей, у которых изменились должностные обязанности или уволившихся из организации;
- периодическую проверку и удаление избыточных пользовательских ID и учетных записей;
- обеспечение того, чтобы избыточные пользовательские ID не были переданы другим пользователям.

Необходимо рассматривать возможность включения положений о применении соответствующих санкций в случае попыток неавторизованного доступа в трудовые договора сотрудников и контракты с поставщиками услуг (6.1.4 и 6.3.5).

9.2.2 Управление привилегиями

Предоставление и использование привилегий при применении средств многопользовательской информационной системы, которые позволяют пользователю обходить средства контроля системы или бизнес-приложения, необходимо ограничивать и держать под контролем. Неадекватное использование привилегий часто бывает главной причиной сбоев систем.

Необходимо, чтобы в многопользовательских системах, которые требуют защиты от неавторизованного доступа, предоставление привилегий контролировалось посредством формализованного процесса авторизации. При этом целесообразно применять следующие меры:

- идентифицировать привилегии в отношении каждого системного продукта, например, операционной системы, системы управления базами данных и каждого бизнес-приложения, а также категории сотрудников, которым эти привилегии должны быть предоставлены;
- привилегии должны предоставляться только тем сотрудникам, которым это необходимо для работы и только на время ее выполнения, например, предоставляя минимальные возможности по работе с системой для выполнения требуемых функций, только когда в этом возникает потребность;
- необходимо обеспечивать процесс авторизации и регистрации всех предоставленных привилегий. Привилегии не должны предоставляться до завершения процесса авторизации;
- следует проводить политику разработки и использования стандартных системных утилит (скриптов) для исключения необходимости в предоставлении дополнительных привилегий пользователям;
- следует использовать различные идентификаторы пользователей при работе в обычном режиме и с использованием привилегий.

9.2.3 Контроль в отношении паролей пользователей

Пароли являются наиболее распространенными средствами подтверждения идентификатора пользователя при доступе к информационной системе или сервису. Предоставление паролей должно контролироваться посредством формализованного процесса управления, который должен предусматривать:

- подписание пользователями документа о необходимости соблюдения полной конфиденциальности личных паролей, а в отношении групповых паролей — соблюдения конфиденциальности в пределах рабочей группы (это может быть включено в условия трудового договора, 6.1.4);

- в случаях, когда от пользователей требуется управление собственными паролями, необходимо обеспечивать предоставление безопасного первоначального временного пароля, который пользователя принуждают сменить при первой регистрации в системе. Временные пароли используются в тех случаях, когда пользователи забывают свой личный пароль, и должны выдаваться только после идентификации пользователя;

- обеспечение безопасного способа выдачи временных паролей пользователям. Следует избегать использования незащищенных (открытый текст) сообщений электронной почты или сообщений по электронной почте от третьей стороны. Пользователям необходимо подтверждать получение паролей.

Пароли никогда не следует хранить в компьютерной системе в незащищенной форме. При необходимости следует рассматривать возможности других технологий для идентификации и аутентификации пользователя, такие как биометрия (проверка отпечатков пальцев), проверка подписи, и использование аппаратных средств идентификации (чип-карт, микросхем).

9.2.4 Пересмотр прав доступа пользователей

Для поддержания эффективного контроля доступа к данным и информационным услугам руководство периодически должно осуществлять формализованный процесс пересмотра прав доступа пользователей, при этом:

- права доступа пользователей должны пересматриваться регулярно (рекомендуемый период — 6 месяцев) и после любых изменений (9.2.1);

- авторизация специальных привилегированных прав доступа (9.2.2) должна осуществляться через меньшие интервалы времени (рекомендуемый период — 3 месяца);

- предоставленные привилегии должны периодически проверяться для обеспечения уверенности в том, что не были получены неавторизованные привилегии.

9.3 Обязанности пользователей

Цель: предотвращение неавторизованного доступа пользователей к информации.

Взаимодействие авторизованных пользователей является важным аспектом эффективности безопасности.

Необходимо, чтобы пользователи были осведомлены о своих обязанностях по использованию эффективных мероприятий по управлению доступом, в частности, в отношении паролей и безопасности оборудования, с которым они работают.

9.3.1 Использование паролей

Пользователи должны соблюдать определенные правила обеспечения безопасности при выборе и использовании паролей.

С помощью паролей обеспечивается подтверждение идентификатора пользователя и, следовательно, получение доступа к средствам обработки информации или сервисам. Все пользователи должны быть осведомлены о необходимости:

а) сохранения конфиденциальности паролей;

б) запрещения записи паролей на бумаге, если только не обеспечено безопасное их хранение;

в) изменения паролей всякий раз, при наличии любого признака возможной компрометации системы или пароля;

г) выбора качественных паролей с минимальной длиной в шесть знаков, которые:

1) легко запомнить;

2) не подвержены легкому угадыванию или вычислению с использованием персональной информации, связанной с владельцем пароля, например, имен, номеров телефонов, дат рождения и т.д.;

3) не содержат последовательных идентичных символов и не состоят из полностью числовых или полностью буквенных групп;

д) изменения паролей через равные интервалы времени или после определенного числа доступов и исключения повторного или цикличного использования старых паролей (пароли для привилегированных учетных записей следует менять чаще, чем обычные пароли);

е) изменения временных паролей при первой регистрации в системе;

ж) запрещения включения паролей в автоматизированный процесс регистрации, например, с использованием хранимых макрокоманд или функциональных клавиш;

з) исключения коллективного использования индивидуальных паролей.

Если пользователи нуждаются в доступе к многочисленным услугам или бизнес-приложениям и вынуждены использовать многочисленные пароли, можно порекомендовать возможность использования одного качественного пароля (9.3.1.г) для всех сервисов, обеспечивающих разумный уровень защиты хранимого пароля.

9.3.2 Оборудование, оставленное пользователями без присмотра

Пользователи должны обеспечивать соответствующую защиту оборудования, оставленного без присмотра. Оборудование, установленное в рабочих зонах, например рабочие или файловые станции, требует специальной защиты от неавторизованного доступа в случае оставления их без присмотра на длительный период. Всем пользователям и подрядчикам необходимо знать требования безопасности и методы защиты оставленного без присмотра оборудования так же, как и свои обязанности по обеспечению такой защиты. Пользователям рекомендуется:

- завершать активные сеансы по окончании работы, если отсутствует механизм блокировки, например, хранитель экрана, защищенный паролем;
- отключаться от мэйнфрейма, когда сеанс закончен (то есть не только выключать PC или терминал);
- защищать PC или терминалы от неавторизованного использования посредством замка или эквивалентного средства контроля, например, защита доступа с помощью пароля, когда оборудование не используется.

9.4 Контроль сетевого доступа

Цель: защита сетевых сервисов.

Доступ как к внутренним, так и к внешним сетевым сервисам должен быть контролируемым. Это необходимо для уверенности в том, что пользователи, которые имеют доступ к сетям и сетевым сервисам, не компрометируют их безопасность, обеспечивая:

- соответствующие интерфейсы между сетью организации и сетями, принадлежащими другим организациям, или общедоступными сетями;
- соответствующие механизмы аутентификации в отношении пользователей и оборудования;
- контроль доступа пользователей к информационным сервисам.

9.4.1 Политика в отношении использования сетевых служб

Несанкционированные подключения к сетевым службам могут нарушать информационную безопасность целой организации. Пользователям следует обеспечивать непосредственный доступ только к тем сервисам, в которых они были авторизованы. Контроль доступа, в частности, является необходимым для сетевых подключений к важным или критичным бизнес-приложениям или для пользователей, находящихся в зонах высокого риска, например, в общественных местах или за пределами организации — вне сферы непосредственного управления и контроля безопасности со стороны организации.

Следует предусматривать меры безопасности в отношении использования сетей и сетевых сервисов. При этом должны быть определены:

- сети и сетевые услуги, к которым разрешен доступ;
- процедуры авторизации для определения кому, к каким сетям и сетевым сервисам разрешен доступ;
- мероприятия и процедуры по защите от несанкционированного подключения к сетевым сервисам.

Необходимо, чтобы эти меры согласовывались с требованиями бизнеса в отношении контроля доступа (9.1).

9.4.2 Предопределенный маршрут

Маршруты от пользовательского терминала до точек предоставления компьютерных сервисов требуют особого контроля. Сети проектируются с учетом обеспечения максимальных возможностей для совместного использования ресурсов и гибкости маршрутизации. Эти особенности повышают риск неавторизованного доступа к бизнес-приложениям или неавторизованного использования информационного оборудования. Мероприятия, которые ограничивают маршруты между пользовательским терминалом и компьютерными сервисами, к которым пользователь авторизован осуществлять доступ, например, путем создания оптимального маршрута, могут уменьшать такие риски.

Цель оптимизации маршрута состоит в том, чтобы исключить выбор пользователями иных маршрутов, кроме маршрута между пользовательским терминалом и сервисами, по которому пользователь авторизован осуществлять доступ.

Этот подход обычно требует внедрения набора средств контроля в различных точках маршрута. Принцип заключается в ограничении вариантов маршрутизации в каждой точке сети посредством определенных способов, например:

- распределения выделенных линий или номеров телефона;
- автоматического подключения портов к определенным системным приложениям или шлюзам безопасности;
- ограничения опций меню и подменю для индивидуальных пользователей;
- предотвращения неограниченного сетевого роуминга;
- использования определенных прикладных систем и/или шлюзов безопасности для внешних пользователей сети;
- активного контроля разрешенного источника с целью направления соединения через шлюзы безопасности, например, межсетевые экраны;
- ограничения доступа к сети посредством создания отдельных логических доменов, например виртуальных частных сетей для пользовательских групп в пределах организации (9.4.6).

Выбор конкретных способов должен основываться на требованиях бизнеса в отношении контроля доступа (9.1).

9.4.3 Аутентификация пользователей в случае внешних соединений

Внешние соединения обеспечивают потенциал для неавторизованного доступа к служебной информации, например, при использовании телефонной связи. Поэтому, при доступе удаленных пользователей, они должны быть аутентифицированы. Некоторые методы аутентификации обеспечивают больший уровень защиты, например, основанные на использовании средств криптографии, и могут обеспечить надежную аутентификацию. Исходя из оценки риска, важно определить требуемый уровень защиты для выбора соответствующего метода аутентификации.

Аутентификация удаленных пользователей может быть достигнута при использовании средств криптографии, средств идентификации аппаратуры или протоколов, поддерживающих метод «отклик-отзыв». Выделенные частные линии или средства проверки сетевого адреса пользователя могут также использоваться для обеспечения доверия к источнику подключений.

Процедуры и средства контроля обратного вызова, например использование модемов с обратным вызовом, могут обеспечивать защиту от неавторизованных и нежелательных подключений к средствам обработки информации организации, так как подтверждают право на доступ пользователей, пытающихся установить удаленную связь с сетью организации. При использовании этих способов организации не следует использовать сетевые сервисы, которые включают переадресацию вызова. Если же они используются, необходимо блокировать возможности переадресации, чтобы избежать связанных с этим рисков. Также важно, чтобы процесс обратного вызова обеспечивал уверенность в том, что фактическое разъединение на стороне организации осуществлено. В противном случае удаленный пользователь может держать линию занятой, фальсифицируя проверку обратного вызова. Для исключения подобных инцидентов процедуры и средства контроля обратного вызова следует тщательно тестировать.

9.4.4 Аутентификация узла

Средство автоматического подсоединения к удаленному компьютеру может предоставить способ получения неавторизованного доступа к бизнес-приложению. Следовательно, подключения к удаленным компьютерным системам необходимо аутентифицировать, что особенно важно, если подключение производится к сети, которая находится вне сферы контроля управления безопасностью организации. Примеры аутентификации и способы ее достижения рассматриваются в 9.4.3.

Аутентификация узла может служить альтернативным средством аутентификации групп удаленных пользователей там, где они подсоединены к безопасному компьютерному средству совместного использования (9.4.3).

9.4.5 Защита портов диагностики при удаленном доступе

Для обеспечения безопасности доступ к портам диагностики должен быть контролируемым. Многие компьютерные сети и системы связи имеют набор средств удаленной диагностики для использования инженерами по обслуживанию. Будучи незащищенными, эти диагностические порты являются источником риска неавторизованного доступа. Безопасность этих портов необходимо обеспечивать с помощью соответствующего защитного механизма безопасности, например, «замка», а также осуществлять доступ обслуживающего персонала к диагностическим портам только на основании договоренности между руководителем, отвечающим за обеспечение компьютерных сервисов, и персоналом по поддержке аппаратных/программных средств.

9.4.6 Принцип разделения в сетях

Компьютерные сети все более распространяются за пределы организации, поскольку создаются деловые партнерства, которые требуют общения между партнерами или совместного использования сетевой инфраструктуры и средств обработки информации. Такие расширения увеличивают риск неавторизованного доступа к информационным системам сети, причем в отношении некоторых из этих сис-

тем, вследствие их важности или критичности, может потребоваться защита от пользователей, получивших доступ к другим системам сети. В таких случаях необходимо рассматривать внедрение дополнительных мероприятий по управлению информационной безопасностью в пределах сети, чтобы разделять группы информационных сервисов, пользователей и информационные системы.

Одно из таких мероприятий состоит в том, чтобы разделять их на отдельные логические сетевые домены, например, внутренний сетевой домен организации и внешние сетевые домены, каждый из которых защищен определенным периметром безопасности. Такой периметр может быть реализован посредством внедрения шлюза безопасности между двумя связанными сетями для контроля доступа и информационного потока между ними. Этот шлюз следует конфигурировать для фильтрации трафика между доменами (9.4.7 и 9.4.8) и для блокирования неавторизованного доступа в соответствии с политикой контроля доступа организации (9.1). Примером такого шлюза является межсетевой экран.

Критерии для разделения сетей на домены следует формировать на основе анализа политики контроля доступа (9.1), а также учитывая влияние этого разделения на производительность в результате включения подходящей технологии маршрутизации сетей или шлюзов (9.4.7 и 9.4.8).

9.4.7 Контроль сетевых соединений

Требования политики контроля доступа для совместно используемых сетей, особенно тех, которые простираются за границы организации, могут потребовать внедрения дополнительных мероприятий по управлению информационной безопасностью, чтобы ограничивать возможности пользователей по подсоединению. Такие мероприятия могут быть реализованы посредством сетевых шлюзов, которые фильтруют трафик с помощью определенных таблиц или правил. Необходимо, чтобы применяемые ограничения основывались на политике и требованиях доступа к бизнес-приложениям (9.1), а также соответствующим образом поддерживались и обновлялись.

Примеры бизнес-приложений, к которым следует применять ограничения:

- электронная почта;
- передача файлов в одном направлении;
- передача файла в обоих направлениях;
- интерактивный доступ;
- доступ к сети, ограниченный определенным временем суток или датой.

9.4.8 Управление маршрутизацией сети

Сети совместного использования, особенно те, которые простираются за границы организации, могут требовать реализации мероприятий по обеспечению информационной безопасности, чтобы подсоединения компьютеров к информационным потокам не нарушали политику контроля доступа к бизнес-приложениям (9.1). Это является особенно важным для сетей, совместно используемых с пользователями третьей стороны (не сотрудниками организации).

Обеспечение информационной безопасности при осуществлении маршрутизации основывается на надежном механизме контроля адресов источника и назначения сообщения. Преобразование сетевых адресов также очень полезно для изоляции сетей и предотвращения распространения маршрутов от сети одной организации в сеть другой. Этот подход может быть реализован как программным способом, так и аппаратно. Необходимо, чтобы специалисты, занимающиеся внедрением, были осведомлены о характеристиках используемых механизмов.

9.4.9 Безопасность использования сетевых служб

Общедоступные и частные сетевые службы предлагают широкий спектр дополнительных информационных услуг, обладающих характеристиками безопасности и обеспечивающих разные уровни защиты. Организации, пользующиеся этими услугами, должны быть уверены в том, что при этом обеспечивается необходимый уровень информационной безопасности и имеется четкое описание атрибутов безопасности всех используемых сервисов.

9.5 Контроль доступа к операционной системе

Цель: предотвращение неавторизованного доступа к компьютерам.

На уровне операционной системы следует использовать средства информационной безопасности для ограничения доступа к компьютерным ресурсам. Эти средства должны обеспечивать:

а) идентификацию и верификацию компьютера пользователя и, если необходимо, терминала и местоположение каждого авторизованного пользователя;

б) регистрацию успешных и неудавшихся доступов к системе;

в) аутентификацию соответствующего уровня. Если используется система парольной защиты, то она должна обеспечивать качественные пароли (9.3.1 г);

г) ограничение времени подсоединения пользователей, в случае необходимости.

Другие методы контроля доступа, такие как «отклик-отзыв», являются допустимыми, если они оправданы с точки зрения бизнес-рисков.

9.5.1 Автоматическая идентификация терминала

Следует рассматривать возможность использования автоматической идентификации терминала, чтобы аутентифицировать его подсоединение к определенным точкам системы. Автоматическая идентификация терминала — метод, который должен использоваться, если важно, чтобы сеанс мог быть инициирован только с определенного места или компьютерного терминала. Встроенный или подсоединенный к терминалу идентификатор может использоваться для определения, разрешено ли этому конкретному терминалу инициировать или получать определенные сообщения. Может быть необходимым применение физической защиты терминала для обеспечения безопасности его идентификатора. Существуют другие методы, которые можно использовать для аутентификации пользователей (9.4.3).

9.5.2 Процедуры регистрации с терминала

Доступ к информационным сервисам должен быть обеспечен путем использования безопасной процедуры входа в систему (способ регистрации). Процедуру регистрации в компьютерной системе следует проектировать так, чтобы свести к минимуму возможность неавторизованного доступа и не оказывать помощи неавторизованному пользователю. Правильно спланированная процедура регистрации должна обладать следующими свойствами:

а) не отображать наименований системы или приложений, пока процесс регистрации не будет успешно завершен;

б) отображать общее уведомление, предупреждающее, что доступ к компьютеру могут получить только авторизованные пользователи;

в) не предоставлять сообщений-подсказок в течение процедуры регистрации, которые могли бы помочь неавторизованному пользователю;

г) подтверждать информацию регистрации только по завершении ввода всех входных данных. В случае ошибочного ввода система не показывает, какая часть данных является правильной или неправильной;

д) ограничивать число разрешенных неудачных попыток регистрации (рекомендуется три) и предусматривать:

1) запись неудачных попыток;

2) включение временной задержки прежде, чем будут разрешены дальнейшие попытки регистрации, или отклонение любых дальнейших попыток регистрации без специальной авторизации;

3) разъединение сеанса связи при передаче данных;

е) ограничивать максимальное и минимальное время, разрешенное для процедуры регистрации. Если оно превышено, система должна прекратить регистрацию;

ж) фиксировать информацию в отношении успешно завершенной регистрации:

1) дату и время предыдущей успешной регистрации;

2) детали любых неудачных попыток регистрации, начиная с последней успешной регистрации.

9.5.3 Идентификация и аутентификация пользователя

Необходимо, чтобы все пользователи (включая персонал технической поддержки, т. е. операторов, администраторов сети, системных программистов и администраторов базы данных) имели уникальный идентификатор (пользовательский ID) для их единоличного использования с тем, чтобы их действия могли быть проанализированы ответственным лицом. Пользовательский ID не должен содержать признаков уровня привилегии пользователя (9.2.2), например, менеджера, контролера.

Для выполнения особо важных работ допускается использовать общий идентификатор для группы пользователей или для выполнения определенной работы. В таких случаях необходимо соответствующим образом оформленное разрешение руководства. Кроме того, для обеспечения безопасности системы от неавторизованного доступа в этих случаях может потребоваться применение дополнительных мер обеспечения информационной безопасности.

Существуют различные процедуры аутентификации, которые могут использоваться для доказательства заявленной идентичности пользователя. Пароли (9.3.1) — очень распространенный способ обеспечения идентификации и аутентификации (I&A), основанный на использовании пароля, который знает только пользователь. То же самое может быть достигнуто средствами криптографии и протоколами аутентификации.

Специальные физические устройства доступа с памятью (token) или микропроцессорные карты (смарт-карты), которыми пользуются сотрудники, могут также использоваться для идентификации и аутентификации. Биометрические методы аутентификации, которые основаны на уникальности харак-

теристик (особенностей) индивидуума, могут также использоваться для аутентификации пользователя. Сочетание различных технологий и методов обеспечивает более надежную аутентификацию.

9.5.4 Система управления паролями

Пароли — одно из главных средств подтверждения полномочия пользователя, осуществляющего доступ к компьютерным сервисам. В системах управления паролем должны быть предусмотрены эффективные интерактивные возможности поддержки необходимого их качества (9.3.1).

Для некоторых бизнес-приложений требуется назначение пользовательских паролей независимым должностным лицом. В большинстве же случаев пароли выбираются и поддерживаются пользователями.

Система управления паролями должна:

- предписывать использование индивидуальных паролей для обеспечения установления ответственности;
- позволять пользователям выбирать и изменять их собственные пароли, а также включать подтверждающую процедуру для учета ошибок ввода при необходимости;
- предписывать выбор высококачественных паролей в соответствии с 9.3.1;
- там, где пользователи отвечают за поддержку своих собственных паролей, принуждать их к изменению паролей (9.3.1);
- там, где пользователи выбирают пароли, обеспечивать изменение временных паролей при первой регистрации (9.2.3);
- поддерживать хранение истории предыдущих пользовательских паролей (за предыдущий год) и предотвращать их повторное использование;
- не отображать пароли на экране при их вводе;
- хранить файлы паролей отдельно от данных прикладных систем;
- хранить пароли в зашифрованной форме, используя односторонний алгоритм шифрования;
- обеспечивать смену паролей поставщика, установленных по умолчанию, после инсталляции программного обеспечения.

9.5.5 Использование системных утилит

На большинстве компьютеров устанавливается, по крайней мере, одна программа — системная утилита, которая позволяет обойти меры предотвращения неавторизованного доступа к операционным системам и бизнес-приложениям. Использование системных утилит должно быть ограничено и тщательным образом контролироваться. Для этого необходимо использование следующих мероприятий по управлению информационной безопасностью:

- использование процедур аутентификации системных утилит;
- отделение системных утилит от прикладных программ;
- ограничение использования системных утилит путем выбора минимального числа доверенных авторизованных пользователей, которым это необходимо;
- авторизация эпизодического использования системных утилит;
- ограничение доступности системных утилит (только на время внесения авторизованных изменений);
- регистрация использования всех системных утилит;
- определение и документирование уровней авторизации в отношении системных утилит;
- удаление всех ненужных утилит из системного программного обеспечения.

9.5.6 Сигнал тревоги для защиты пользователей на случай, когда они могут стать объектом насилия

Желательно предусматривать сигнал тревоги на случай, когда пользователь может стать объектом насилия. Решение об обеспечении такой сигнализацией следует принимать на основе оценки рисков. При этом необходимо определить обязанности и процедуры реагирования на сигнал такой тревоги.

9.5.7 Периоды бездействия терминалов

Терминалы, размещенные в местах повышенного риска, например в общедоступных местах или вне сферы контроля процесса управления безопасностью организации, обслуживающие системы высокого риска, должны отключаться после определенного периода их бездействия для предотвращения доступа неавторизованных лиц. Механизм блокировки по времени должен обеспечивать очистку экрана терминала, а также закрытие работы сеансов приложения и сетевого сеанса терминала после определенного периода времени его бездействия. Время срабатывания блокировки должно устанавливаться с учетом рисков безопасности, связанных с местом установки терминала. Следует иметь в виду, что некоторые персональные компьютеры обеспечивают ограниченную возможность блокировки терминала по времени путем очистки экрана и предотвращения неавторизованного доступа, не осуществляя при этом закрытия сеанса приложений или сетевого сеанса.

9.5.8 Ограничения подсоединения по времени

Ограничения подсоединения по времени должны обеспечивать дополнительную безопасность для приложений высокого риска. Ограничение периода времени, в течение которого разрешены подсоединения терминалов к компьютерным сервисам, уменьшает интервал времени, в течение которого возможен неавторизованный доступ. Эту меру обеспечения информационной безопасности необходимо применять для наиболее важных компьютерных приложений, особенно тех, которые связаны с терминалами, установленными в местах повышенного риска, например, в общедоступных местах или вне сферы контроля управления безопасностью организации. Примеры таких ограничений:

- использование заранее определенных отрезков времени для пакетной передачи файлов или регулярных интерактивных сеансов небольшой продолжительности;
- ограничение времени подключений часами работы организации, если нет необходимости сверхурочной или более продолжительной работы.

9.6 Контроль доступа к приложениям

Цель: предотвращение неавторизованного доступа к данным информационных систем.

Необходимо применять меры обеспечения информационной безопасности для ограничения доступа к прикладным системам.

Логический доступ к программному обеспечению и информации должен быть ограничен только авторизованными пользователями. Для этого необходимо обеспечивать:

- контроль доступа пользователей к информации и функциям бизнес-приложений в соответствии с определенной бизнесом политикой контроля доступа;
- защиту от неавторизованного доступа любой утилиты и системного программного обеспечения, которые позволяют обходить средства операционной системы или приложений;
- исключение компрометации безопасности других систем, с которыми совместно используются информационные ресурсы;
- доступ к информации только владельца, который соответствующим образом назначен из числа авторизованных лиц или определенных групп пользователей.

9.6.1 Ограничение доступа к информации

Пользователям бизнес-приложений, включая персонал поддержки и эксплуатации, следует обеспечивать доступ к информации и функциям этих приложений в соответствии с определенной политикой контроля доступа, основанной на требованиях к отдельным бизнес-приложениям (9.1). Необходимо рассматривать применение следующих мероприятий по управлению информационной безопасностью для обеспечения требований по ограничению доступа:

- поддержка меню для управления доступом к прикладным функциям системы;
- ограничения в предоставлении пользователям информации о данных и функциях бизнес-приложений, к которым они не авторизованы на доступ, путем соответствующего редактирования пользовательской документации;
- контроль прав доступа пользователей, например, чтение/запись/удаление/ выполнение;
- обеспечение уверенности в том, что выводимые данные из бизнес-приложений, обрабатывающих важную информацию, содержали только требуемую информацию и пересылались только в адреса авторизованных терминалов и по месту назначения. Следует проводить периодический анализ процесса вывода для проверки удаления избыточной информации.

9.6.2 Изоляция систем, обрабатывающих важную информацию

Системы, обрабатывающие важную информацию, должны быть обеспечены выделенной (изолированной) вычислительной средой. Некоторые прикладные системы имеют очень большое значение с точки зрения безопасности данных и поэтому требуют специальных условий эксплуатации. Важность обрабатываемой информации может или требовать работы системы на выделенном компьютере, или осуществлять совместное использование ресурсов только с безопасными бизнес-приложениями, или работать без каких-либо ограничений. При этом необходимо учитывать следующее:

- владельцу бизнес-приложений необходимо определить и документально оформить степень их важности (4.1.3);
- когда важное бизнес-приложение должно работать в среде совместного использования, необходимо выявить другие приложения, с которыми будет осуществляться совместное использование ресурсов, и согласовать это с владельцем важного бизнес-приложения.

9.7 Мониторинг доступа и использования системы

Цель: обнаружение неавторизованных действий.

Для обнаружения отклонения от требований политики контроля доступа и регистрации событий и обеспечения доказательства на случай выявления инцидентов нарушения информационной безопасности необходимо проводить мониторинг системы.

Мониторинг системы позволяет проверять эффективность применяемых мероприятий по обеспечению информационной безопасности и подтверждать соответствие модели политики доступа требованиям бизнеса (9.1).

9.7.1 Регистрация событий

Для записи инцидентов нарушения информационной безопасности и других связанных с безопасностью событий следует создавать журналы аудита и хранить их в течение согласованного периода времени с целью содействия в проведении будущих расследований и мониторинге управления доступом. Необходимо, чтобы записи аудита включали:

- ID пользователей;
- даты и время входа и выхода;
- идентификатор терминала или его местоположение, если возможно;
- записи успешных и отклоненных попыток доступа к системе;
- записи успешных и отклоненных попыток доступа к данным и другим ресурсам. Может потребоваться, чтобы определенные записи аудита были заархивированы для использования их при анализе и расследованиях инцидентов нарушения информационной безопасности, а также в интересах других целей (раздел 12).

9.7.2 Мониторинг использования систем

9.7.2.1 Процедуры и области риска

Для обеспечения уверенности в том, что пользователи выполняют только те действия, на которые они были явно авторизованы, необходимо определить процедуры мониторинга использования средств обработки информации. Уровень мониторинга конкретных средств обработки информации следует определять на основе оценки рисков. При мониторинге следует обращать внимание на:

а) авторизованный доступ, включая следующие детали:
   1) пользовательский ID;
   2) даты и время основных событий;
   3) типы событий;
   4) файлы, к которым был осуществлен доступ;
   5) используемые программы/утилиты;

б) все привилегированные действия, такие как:
   1) использование учетной записи супервизора;
   2) запуск и останов системы;
   3) подсоединение/отсоединение устройства ввода/вывода;

в) попытки неавторизованного доступа, такие как:
   1) неудавшиеся попытки;
   2) нарушения политики доступа и уведомления сетевых шлюзов и межсетевых экранов;
   3) предупреждения от собственных систем обнаружения вторжения;

г) предупреждения или отказы системы, такие как:
   1) консольные (терминальные) предупреждения или сообщения;
   2) исключения, записанные в системные журналы регистрации;
   3) предупредительные сигналы, связанные с управлением сетью.

9.7.2.2 Факторы риска

Результаты мониторинга следует регулярно анализировать. Периодичность анализов должна зависеть от результатов оценки риска. Факторы риска, которые необходимо при этом учитывать, включают:

- критичность процессов, которые поддерживаются бизнес-приложениями;
- стоимость, важность или критичность информации;
- анализ предшествующих случаев проникновения и неправильного использования системы;
- степень взаимосвязи информационных систем организации с другими (особенно с общедоступными) сетями.

9.7.2.3 Регистрация и анализ событий

Анализ (просмотр) журнала аудита подразумевает понимание угроз, которым подвержена система, и причин их возникновения. Примеры событий, которые могли бы потребовать дальнейшего исследования в случае инцидентов нарушения информационной безопасности, приведены в 9.7.1.

Системные журналы аудита часто содержат информацию, значительный объем которой не представляет интереса с точки зрения мониторинга безопасности. Для облегчения идентификации

существенных событий при мониторинге безопасности целесообразно рассмотреть возможность автоматического копирования соответствующих типов сообщений в отдельный журнал и/или использовать подходящие системные утилиты или инструментальные средства аудита для подготовки к анализу данных.

При распределении ответственности за анализ журнала аудита необходимо учитывать разделение ролей между лицом (лицами), проводящим (и) анализ, и теми, чьи действия подвергаются мониторингу.

Особое внимание следует уделять защите собственных средств регистрации, потому что при вмешательстве в их работу может быть получено искаженное представление о событиях безопасности. Мероприятия по управлению информационной безопасностью должны обеспечивать защиту от неавторизованных изменений и эксплуатационных сбоев, включая:

- отключение средств регистрации;
- изменение типов зарегистрированных сообщений;
- редактирование или удаление файлов, содержащихся в журналах аудита;
- регистрацию случаев полного заполнения носителей журнальных файлов, а также случаев невозможности записей событий вследствие сбоев либо случаев перезаписи новых данных поверх старых.

9.7.3 Синхронизация часов

Правильная установка компьютерных часов (таймера) важна для обеспечения точности заполнения журналов аудита, которые могут потребоваться для расследований или как доказательство при судебных или административных разбирательствах. Некорректные журналы аудита могут затруднять такие расследования, а также приводить к сомнению в достоверности собранных доказательств.

Там, где компьютер или устройство связи имеют возможность использовать часы в реальном времени, их следует устанавливать по Универсальному Скоординированному Времени (UCT) или местному стандартному времени. Так как некоторые часы, как известно, «уходят вперед» или «отстают», должна существовать процедура, которая проверяет и исправляет любое отклонение или его значимое изменение.

9.8 Работа с переносными устройствами и работа в дистанционном режиме

Цель: обеспечение информационной безопасности при использовании переносных устройств и средств, обеспечивающих работу в дистанционном режиме.

Следует соизмерять требуемую защиту со специфичными рисками работы в удаленном режиме. При использовании переносных устройств следует учитывать риски, связанные с работой в незащищенной среде, и применять соответствующие меры защиты. В случаях работы в дистанционном режиме организация должна предусматривать защиту как места работы, так и соответствующие меры по обеспечению информационной безопасности.

9.8.1 Работа с переносными устройствами

При использовании переносных устройств, например ноутбуков, карманных компьютеров, переносных компьютеров и мобильных телефонов, необходимо принимать специальные меры противодействия компрометации служебной информации. Необходимо принять формализованную политику, учитывающую риски, связанные с работой с переносными устройствами, в особенности в незащищенной среде. Такая политика должна включать требования по физической защите, контролю доступа, использованию средств и методов криптографии, резервированию и защите от вирусов. Необходимо, чтобы эта политика включала правила и рекомендации по подсоединению мобильных средств к сетям, а также разработку руководств по использованию этих средств в общедоступных местах.

Следует проявлять осторожность при использовании мобильных средств вычислительной техники и других сервисных средств в общедоступных местах, переговорных комнатах и незащищенных помещениях вне организации. Чтобы исключить неавторизованный доступ или раскрытие информации, хранимой и обрабатываемой этими средствами, необходимо использование средств и методов криптографии (10.3).

При использовании мобильных средств в общедоступных местах важно проявлять осторожность, чтобы уменьшить риск «подсмотра» паролей доступа неавторизованными лицами. Необходимо внедрять и поддерживать в актуализированном состоянии средства и способы защиты от вредоносного программного обеспечения (8.3). Следует также обеспечивать доступность оборудования для быстрого и удобного резервирования информации. Необходимо также обеспечивать адекватную защиту резервных копий от кражи или потери информации.

Соответствующую защиту необходимо обеспечивать мобильным средствам, подсоединенным к общедоступным сетям. Удаленный доступ к служебной информации через общедоступную сеть с

использованием мобильных средств вычислительной техники следует осуществлять только после успешной идентификации и аутентификации, а также при наличии соответствующих механизмов управления доступом (9.4).

Оборудование, на котором хранится важная и/или критическая коммерческая информация, не следует оставлять без присмотра и по возможности необходимо физически изолировать его в надежное место или использовать специальные защитные устройства на самом оборудовании, чтобы исключить его неавторизованное использование. Переносные устройства необходимо также физически защищать от краж, особенно когда их оставляют без присмотра, забывают в автомобилях или других видах транспорта, гостиничных номерах, конференц-залах и других местах встреч (7.2.5).

Необходимо информировать сотрудников, использующих переносные устройства, о дополнительных рисках и необходимых мероприятиях обеспечения информационной безопасности, связанных с этим способом работы.

9.8.2 Работа в дистанционном режиме

При работе в дистанционном режиме, а также для обеспечения работы сотрудников вне своей организации, в конкретном удаленном месте применяются коммуникационные технологии. При этом следует обеспечивать защиту мест дистанционной работы как от краж оборудования и информации, так и от неавторизованного раскрытия информации, неавторизованного удаленного доступа к внутренним системам организации или неправильного использования оборудования. Важно, чтобы при работе в дистанционном режиме были выполнены требования как по авторизации, так и по контролю со стороны руководства, а также был обеспечен соответствующий уровень информационной безопасности этого способа работы.

Организациям необходимо предусматривать разработку политики, процедуры и способы контроля за действиями, связанными с работой в дистанционном режиме. Организациям следует авторизовывать возможность работы в дистанционном режиме только в случае уверенности, что применяются соответствующие меры информационной безопасности, которые согласуются с политикой безопасности организации. Необходимо принимать во внимание:

- существующую физическую безопасность места работы в дистанционном режиме, с точки зрения безопасности здания и окружающей среды;
- предлагаемое оборудование мест дистанционной работы;
- требования к безопасности коммуникаций, исходя из потребности в удаленном доступе к внутренним системам организации, важности информации, к которой будет осуществляться доступ и которая будет передаваться по каналам связи, а также важность самих внутренних систем организации;
- угрозу неавторизованного доступа к информации или ресурсам со стороны других лиц, имеющих доступ к месту дистанционной работы, например, членов семьи и друзей.

Мероприятия по обеспечению информационной безопасности в этих условиях должны включать:

- обеспечение подходящим оборудованием и мебелью места дистанционной работы;
- определение видов разрешенной работы, времени работы, классификацию информации, которая может храниться, а также определение внутренних систем и услуг, доступ к которым авторизован лицу, работающему в дистанционном режиме;
- обеспечение подходящим телекоммуникационным оборудованием, в том числе средствами обеспечения безопасности удаленного доступа;
- физическую безопасность;
- правила и руководства в отношении доступа членов семьи и друзей к оборудованию и информации;
- обеспечение поддержки и обслуживания оборудования и программного обеспечения;
- процедуры в отношении резервирования данных и обеспечения непрерывности деятельности;
- аудит и мониторинг безопасности;
- аннулирование полномочий, отмену прав доступа и возвращение оборудования в случае прекращения работы в дистанционном режиме.

10 Разработка и обслуживание систем

10.1 Требования к безопасности систем

Цель: обеспечение учета требований безопасности при разработке информационных систем.

Эти требования касаются инфраструктуры, бизнес-приложений, а также приложений, разработанных пользователями. Процессы проектирования и внедрения бизнес-приложения или сервиса могут

быть критичными с точки зрения безопасности. Требования к безопасности следует идентифицировать и согласовывать до разработки информационных систем.

Все требования безопасности, включая необходимые мероприятия по переходу на аварийный режим, следует идентифицировать на стадии определения задач проекта, а также обосновывать, согласовывать и документировать в рамках общего проекта по внедрению информационной системы.

10.1.1 Анализ и спецификация требований безопасности

Необходимо, чтобы в формулировках требований бизнеса в отношении новых систем или усовершенствования существующих систем были учтены требования информационной безопасности. При этом следует учитывать как возможности встроенных в систему автоматизированных средств обеспечения информационной безопасности, так и необходимость применения организационных мероприятий по управлению информационной безопасностью или разработку специальных средств. Аналогично следует подходить к оценке пакетов прикладных программ. Как правило, руководство должно обеспечивать использование сертифицированных программных продуктов или продуктов, прошедших независимую оценку.

Требования безопасности и соответствующие мероприятия по обеспечению информационной безопасности должны учитывать ценность информационных активов, потенциальный ущерб бизнесу, который может стать результатом неэффективности или отсутствия мер безопасности. Оценка и управление рисками — основа для анализа требований к безопасности и определения необходимых мероприятий по управлению информационной безопасностью.

Планирование мероприятий по обеспечению информационной безопасности на стадии проектирования системы позволяет существенно снизить затраты на их внедрение и поддержку по сравнению с разработкой соответствующих мероприятий во время или после внедрения системы.

10.2 Безопасность в прикладных системах

Цель: предотвращение потерь, модификации или неправильного использования пользовательских данных в прикладных системах.

Соответствующие мероприятия по обеспечению информационной безопасности, включая функции аудита или протоколирование действий пользователя, необходимо предусматривать в прикладных системах, включая приложения, написанные самими пользователями. Эти меры должны включать в себя обеспечение функциональности подтверждения корректности ввода, обработки и вывода данных.

Дополнительные мероприятия по обеспечению информационной безопасности могут потребоваться для систем, которые обрабатывают или оказывают воздействие на важные, ценные или критические активы организации, и их необходимо определять на основе требований безопасности и оценки рисков.

10.2.1 Подтверждение корректности ввода данных

Необходимо обращать особое внимание на корректность входных данных для прикладных систем. При вводе бизнес-транзакций, постоянных данных (имена и адреса, кредитные лимиты, идентификационные номера клиентов) и таблиц параметров (цены продаж, курсы валют, ставки налогов) следует применять проверку корректности ввода для обеспечения уверенности в их соответствии исходным данным. Для этого целесообразно применение следующих мероприятий по обеспечению информационной безопасности:

а) проверки исключения двойного ввода или другие проверки ввода с целью обнаружения следующих ошибок:

1) значений, выходящих за допустимый диапазон;
2) недопустимых символов в полях данных;
3) отсутствующие или неполные данные;
4) превышение верхних и нижних пределов объема данных;
5) неавторизованные или противоречивые контрольные данные;

б) периодический анализ (просмотр) содержимого ключевых полей или файлов данных для подтверждения их достоверности и целостности;

в) сверка твердых (печатных) копий вводимых документов с вводимыми данными на предмет выявления любых неавторизованных изменений этих данных (необходимо, чтобы все изменения во вводимых документах были авторизованы);

г) процедуры реагирования на ошибки, связанные с подтверждением данных;

д) процедуры проверки правдоподобия вводимых данных;

е) определение обязанностей всех сотрудников, вовлеченных в процесс ввода данных.

10.2.2 Контроль обработки данных в системе

10.2.2.1 Области риска

Данные, которые были введены правильно, могут быть искажены вследствие ошибок обработки или преднамеренных действий. С целью обнаружения подобных искажений в функции систем следует включать требования, обеспечивающие выполнение контрольных проверок. Необходимо, чтобы дизайн приложений обеспечивал уверенность в том, что внедрены ограничения, направленные на минимизацию риска отказов, ведущих к потере целостности данных. Необходимо учитывать, в частности, следующее:

- использование места в программах для функций добавления и удаления данных;
- процедуры для предотвращения выполнения программ в неправильной последовательности или ее исполнения после сбоя на предыдущем этапе обработки данных (8.1.1);
- использование корректирующих программ для восстановления после сбоев и обеспечения правильной обработки данных.

10.2.2.2 Проверки и средства контроля

Выбор необходимых средств контроля зависит от характера бизнес-приложения и последствий для бизнеса любого искажения данных. Примеры встроенных средств обеспечения информационной безопасности могут быть:

а) средства контроля сеансовой или пакетной обработки с целью выверки контрольных данных (остатков/контрольных сумм) в файлах данных после транзакционных обновлений;

б) средства контроля входящих остатков с целью их проверки с предыдущими закрытыми остатками, а именно:

1) средства контроля «от выполнения — к выполнению»;
2) общие суммы измененных данных в файле;
3) средства контроля «от программы — к программе»;

в) подтверждение корректности данных, генерированных системой (10.2.1);

г) проверки целостности полученных или переданных данных (программного обеспечения) между центральным (главным) и удаленными компьютерами (10.3.3);

д) контрольные суммы записей и файлов;

е) проверки для обеспечения уверенности в том, что прикладные программы выполняются в нужное время;

ж) проверки для обеспечения уверенности в том, что программы выполняются в правильном порядке и прекращают работу в случае отказа, и что дальнейшая обработка приостанавливается до тех пор, пока проблема не будет разрешена.

10.2.3 Аутентификация сообщений

Аутентификация сообщений — это метод, используемый для обнаружения неавторизованных изменений или повреждений содержания переданного электронного сообщения. Аутентификация сообщений может быть реализована как аппаратным, так и программным путем в физическом устройстве аутентификации сообщений или в программном алгоритме.

Аутентификацию сообщений необходимо использовать для бизнес-приложений, где должна быть обеспечена защита целостности содержания сообщений, например при электронных переводах денежных средств, пересылке спецификаций, контрактов, коммерческих предложений и прочих документов, имеющих большую важность, или других подобных электронных обменов данными. Чтобы определить, требуется ли аутентификация сообщений, необходимо выполнять оценку рисков безопасности и выбирать наиболее подходящий метод ее реализации.

Аутентификация сообщений не предназначена для защиты содержания сообщения от неправомочного его раскрытия. Для этой цели при аутентификации сообщений могут использоваться криптографические методы (10.3.2 и 10.3.3).

10.2.4 Подтверждение корректности данных вывода

Данные, выводимые из прикладной системы, необходимо проверять на корректность, чтобы обеспечивать уверенность в том, что обработка информации выполнена правильно. Как правило, системы построены на предпосылке, что при наличии соответствующих подтверждений корректности, проверок и тестирования выводимые данные будут всегда правильны. Но это не всегда так. Подтверждение корректности данных вывода может включать:

- проверки на правдоподобие с целью определения, являются ли выходные данные приемлемыми;
- проверки контрольных счетчиков на предмет удостоверения, что все данные были обработаны;
- обеспечение достаточной информации для получателя результатов вывода или последующей системы обработки, чтобы определить корректность, законченность, точность и классификацию информации;

- процедуры по выполнению тестов на подтверждение выводимых данных;
- определение обязанностей всех сотрудников, вовлеченных в процесс вывода данных.

10.3 Меры защиты информации, связанные с использованием криптографии

Цель: защита конфиденциальности, аутентичности или целостности информации.

Криптографические системы и методы следует использовать для защиты конфиденциальной информации, когда другие средства контроля не обеспечивают адекватной защиты.

10.3.1 Политика в отношении использования криптографии

Решения относительно применения криптографических мер защиты следует рассматривать в рамках более общего процесса оценки рисков и выбора мероприятий по обеспечению информационной безопасности. Для определения необходимого уровня защиты информации следует проводить оценку рисков, которая должна использоваться для определения того, является ли криптографическое средство подходящим, какой тип средств необходим, с какой целью и в отношении каких бизнес-процессов его следует применять.

В организации следует разработать политику использования криптографических средств защиты информации. Такая политика необходима, чтобы максимизировать преимущества и минимизировать риски, связанные с использованием криптографических средств, а также избежать неадекватного или неправильного их использования. При этом необходимо определить:

а) методику использования криптографических средств в организации, включая общие принципы, в соответствии с которыми следует защищать служебную информацию;

б) принципы управления ключами, включая методы восстановления зашифрованной информации в случае потери, компрометации или повреждения ключей;

в) роли и обязанности должностных лиц за:

1) реализацию политики;

2) управление ключами;

г) соответствующий уровень криптографической защиты для различных данных;

д) перечень мероприятий, которые должны обеспечивать эффективность внедрения методов криптозащиты в организации.

10.3.2 Шифрование

Шифрование — это криптографический метод, который может использоваться для обеспечения защиты конфиденциальной, важной или критичной информации.

На основе оценки рисков необходимо определять требуемый уровень защиты, принимая во внимание тип и качество используемого алгоритма шифрования, а также длину криптографических ключей.

При разработке политики использования криптографических средств необходимо учитывать требования законодательства и ограничения, которые могут применяться в отношении использования криптографических методов в разных странах, а также вопросы, касающиеся объема потока зашифрованной информации, передаваемой через границы государств. Кроме того, следует учитывать требования законодательства в отношении экспорта и импорта криптографических технологий (12.1.6).

Для определения необходимого уровня защиты информации, выбора подходящих средств и методов защиты, которые должны обеспечивать требуемый уровень защиты и реализации безопасных способов управления ключами, целесообразно консультироваться со специалистами (10.3.5). Кроме того, может потребоваться консультация юриста относительно законов и нормативных актов, которые могут быть применимы в случае предполагаемого использования организацией методов и средств шифрования.

10.3.3 Цифровые подписи

Цифровые подписи обеспечивают защиту аутентификации и целостности электронных документов.

Например, электронные подписи могут использоваться при электронной торговле, где есть необходимость в контроле с целью удостовериться, кто подписал электронный документ, а также проверке, было ли содержание подписанного документа изменено.

Цифровые подписи могут применяться для любой формы документа, обрабатываемого электронным способом, например, при подписи электронных платежей, денежных переводов, контрактов и соглашений. Цифровые подписи могут быть реализованы при использовании криптографического метода, основывающегося на однозначно связанной паре ключей, где один ключ используется для создания подписи (секретный/личный ключ), а другой — для проверки подписи (открытый ключ).

Необходимо с особой тщательностью обеспечивать конфиденциальность личного ключа, который следует хранить в секрете, так как любой имеющий к нему доступ может подписывать документы (платежи, контракты), тем самым фальсифицируя подпись владельца ключа. Кроме того, очень важна защита

целостности открытого ключа, которая обеспечивается при использовании сертификата открытого ключа (10.3.5).

Следует уделять внимание выбору типа и качеству используемого алгоритма подписи и длине ключей. Необходимо, чтобы криптографические ключи, используемые для цифровых подписей, отличались от тех, которые используются для шифрования (10.3.2).

При использовании цифровых подписей, необходимо учитывать требования всех действующих законодательств, определяющих условия, при которых цифровая подпись имеет юридическую силу. Например, при электронной торговле важно знать юридический статус цифровых подписей. Может потребоваться наличие специальных контрактов или других соглашений, чтобы поддерживать использование цифровых подписей в случаях, когда законодательство в отношении цифровых подписей недостаточно развито. Необходимо воспользоваться консультацией юриста в отношении законов и нормативных актов, которые могут быть применимыми в отношении предполагаемого использования организацией цифровых подписей.

10.3.4 Сервисы неоспоримости

Сервисы неоспоримости следует использовать там, где может требоваться решать споры о наличии или отсутствии события или действия, например спор по использованию цифровой подписи на электронном контракте или платеже. Данные сервисы могут помочь доказать, имел ли место конкретный случай или действие, например отказ в отсылке инструкции, подписанной цифровой подписью, по электронной почте. Эти сервисы основываются на использовании методов шифрования и цифровой подписи (10.3.2 и 10.3.3).

10.3.5 Управление ключами

10.3.5.1 Защита криптографических ключей

Управление криптографическими ключами важно для эффективного использования криптографических средств.

Любая компрометация или потеря криптографических ключей может привести к компрометации конфиденциальности, подлинности и/или целостности информации. Следует применять систему защиты для обеспечения использования организацией следующих криптографических методов:

- методы в отношении секретных ключей, где две или более стороны совместно используют один и тот же ключ, и этот ключ применяется как для шифрования, так и дешифрования информации. Этот ключ должен храниться в секрете, так как любой, имеющий доступ к этому ключу, может дешифровать всю информацию, зашифрованную с помощью этого ключа, или ввести неавторизованную информацию;
- методы в отношении открытых ключей, где каждый пользователь имеет пару ключей, открытый ключ (который может быть показан любому) и личный ключ (который должен храниться в секрете). Методы с открытыми ключами могут использоваться для шифрования (10.3.2) и для генерации цифровых подписей (10.3.3).

Ключи необходимо защищать от изменения и разрушения, а секретным и личным ключам необходима защита от неавторизованного раскрытия. Криптографические методы могут также использоваться для этой цели. Физическую защиту следует применять для защиты оборудования, используемого для изготовления, хранения и архивирования ключей.

10.3.5.2 Способы, процедуры и методы защиты криптографических ключей

Необходимо, чтобы система обеспечения безопасности использования ключей основывалась на согласовании способов, процедур и безопасных методов для:

- генерации ключей при использовании различных криптографических систем и различных приложений;
- генерации и получения сертификатов открытых ключей;
- рассылки ключей предназначенным пользователям, включая инструкции по их активации при получении;
- хранения ключей; при этом необходимо наличие инструкции авторизованным пользователям для получения доступа к ключам;
- смены или обновления ключей, включая правила порядка и сроков смены ключей;
- порядка действий в отношении скомпрометированных ключей;
- аннулирования ключей, в том числе способы аннулирования или дезактивации ключей, если ключи были скомпрометированы или пользователь уволился из организации (в этом случае ключи необходимо архивировать);
- восстановления ключей, которые были утеряны или испорчены, для рассекречивания зашифрованной информации;
- архивирования ключей, например для архивированной или резервной информации;
- разрушения ключей;

- регистрации и аудита действий, связанных с управлением ключами.

Для уменьшения вероятности компрометации необходимо, чтобы ключи имели определенные даты активизации и дезактивации, чтобы их можно было бы использовать в течение ограниченного периода времени, который зависит от обстоятельств использования криптографических средств, контроля и от степени риска раскрытия информации.

Может потребоваться наличие процедур обработки юридических запросов, касающихся доступа к криптографическим ключам, например, чтобы зашифрованная информация стала доступной в незашифрованной форме для доказательств в суде.

В дополнение к вопросу безопасности управления секретными и личными ключами необходимо учитывать необходимость обеспечения защиты открытых ключей. Существует угроза подделывания цифровой подписи и замены открытого ключа пользователя своим. Эта проблема решается с помощью сертификата открытых ключей. Сертификаты необходимо изготовлять таким способом, который однозначно связывал бы информацию, относящуюся к владельцу пары открытого/секретного ключей, с открытым ключом. Поэтому важно, чтобы процессу управления, в рамках которого формируются эти сертификаты, можно было доверять. Этот процесс обычно выполняется органом сертификации, который должен быть признанной организацией, руководствующейся соответствующими правилами и процедурами информационной безопасности для обеспечения требуемой степени доверия к нему.

Необходимо, чтобы содержание соглашений с внешними поставщиками криптографических средств, например с органом сертификации, включало требования по ответственности, надежности средств и времени реагирования на запросы по их предоставлению (4.2.2).

10.4 Безопасность системных файлов

Цель: обеспечение модернизации информационных систем и действий по их поддержке безопасным способом.

В процессе эксплуатации бизнес-приложений необходимо контролировать доступ к системным файлам.

Пользователи или разработчики, которым принадлежит прикладная система или программное обеспечение, должны быть ответственными за целостность системы.

10.4.1 Контроль программного обеспечения, находящегося в промышленной эксплуатации

Необходимо обеспечивать контроль за процессом внедрения программного обеспечения в промышленную эксплуатацию. Чтобы свести к минимуму риск повреждения систем, находящихся в промышленной эксплуатации, целесообразно использовать следующие мероприятия по обеспечению информационной безопасности:

- обновление библиотек программ следует выполнять только назначенному специалисту — библиотекарю при соответствующей авторизации его обязанностей руководством (10.4.3);

- по возможности, системы, находящиеся в промышленной эксплуатации, должны состоять только из исполнимых программных кодов;

- исполняемую программу не следует внедрять в промышленную эксплуатацию до тех пор, пока не получены подтверждения ее успешного тестирования и принятия пользователями, а также не обновлены соответствующие библиотеки исходных текстов программ;

- необходимо, чтобы журнал аудита регистрировал все обновления библиотек программ, находящихся в промышленной эксплуатации;

- предыдущие версии программного обеспечения следует сохранять для восстановления системы в случае непредвиденных обстоятельств.

Необходимо, чтобы программное обеспечение, используемое в промышленной эксплуатации, поддерживалось на уровне, заданном разработчиком. При любом решении провести обновление до уровня новой версии следует принимать во внимание безопасность данной версии: какие новые функциональные возможности обеспечения информационной безопасности она имеет или имеются ли серьезные проблемы обеспечения безопасности, связанные с этой версией. Целесообразно использовать программные модификации (патчи), если они могут закрыть или снизить угрозы безопасности.

Физический или логический доступ предоставляется поставщикам (разработчикам), по мере необходимости, только для поддержки программного обеспечения при наличии разрешения руководства. При этом действия поставщика (разработчика) должны контролироваться.

10.4.2 Защита тестовых данных

Данные тестирования следует защищать и контролировать. Для осуществления системного и приемочного тестирования требуются существенные объемы тестовых данных, которые максимально приближены к операционным данным. Следует избегать использования баз данных, находящихся в промышленной эксплуатации и содержащих личную информацию. Если такая информация требуется

для тестирования, то перед использованием следует удалить личную информацию (деперсонифицировать ее). Для защиты операционных данных, когда они используются для целей тестирования, необходимо применять следующие мероприятия по обеспечению информационной безопасности:

- процедуры контроля доступа, применяемые для прикладных систем, находящихся в промышленной эксплуатации, следует также применять и к прикладным системам в среде тестирования;
- при каждом копировании операционной информации для прикладной системы тестирования предусматривать авторизацию этих действий;
- после того, как тестирование завершено, операционную информацию следует немедленно удалить из прикладной системы среды тестирования;
- копирование и использование операционной информации необходимо регистрировать в журнале аудита.

10.4.3 Контроль доступа к библиотекам исходных текстов программ

Для снижения риска искажения компьютерных программ необходимо обеспечивать строгий контроль доступа к библиотекам исходных текстов программ, для чего:

- по возможности, исходные библиотеки программ следует хранить отдельно от бизнес-приложений, находящихся в промышленной эксплуатации;
- назначать специалиста — библиотекаря программ для каждого бизнес-приложения;
- персоналу поддержки информационных технологий не следует предоставлять неограниченный доступ к исходным библиотекам программ;
- программы, находящиеся в процессе разработки или текущего обслуживания, не следует хранить в библиотеках с исходными текстами программ, находящихся в промышленной эксплуатации;
- обновление библиотек и обеспечение программистов исходными текстами следует осуществлять только назначенному специалисту — библиотекарю после авторизации, полученной от менеджера, отвечающего за поддержку конкретного бизнес-приложения;
- листинги программ следует хранить в безопасном месте (8.6.4);
- следует вести журнал аудита для всех доступов к исходным библиотекам;
- старые версии исходных текстов необходимо архивировать с указанием точных дат и времени, когда они находились в промышленной эксплуатации, вместе со всем программным обеспечением поддержки, управления заданиями, определениями данных и процедурами;
- поддержку и копирование исходных библиотек следует проводить под строгим контролем с целью предотвращения внесения неавторизованных изменений (10.4.1).

10.5 Безопасность в процессах разработки и поддержки

Цель: поддержание безопасности прикладных систем и информации.

Менеджеры, ответственные за прикладные системы, должны быть ответственными и за безопасность среды проектирования или поддержки. Они должны проводить анализ всех предложенных изменений системы и исключать возможность компрометации безопасности как системы, так и среды промышленной эксплуатации.

10.5.1 Процедуры контроля изменений

Чтобы свести к минимуму повреждения информационных систем, следует строго контролировать внедрение изменений — строго придерживаться формализованных процедур обеспечения информационной безопасности; осуществлять контроль за возможной компрометацией самих процедур; программистам, отвечающим за поддержку, предоставлять доступ только к тем частям системы, которые необходимы для их работы; обеспечивать формализацию и одобрение соответствующим руководством всех изменений. Изменения в прикладном программном обеспечении могут повлиять на информационную безопасность используемых бизнес-приложений. Там, где это возможно, следует объединять меры по обеспечению информационной безопасности используемых бизнес-приложений и изменений в прикладных программах (3.1.2). Необходимо, чтобы этот процесс включал:

- обеспечение протоколирования согласованных уровней авторизации;
- обеспечение уверенности в том, что запросы на изменения исходят от авторизованных соответствующим образом пользователей;
- анализ мер информационной безопасности и процедур, обеспечивающих целостность используемых систем;
- идентификацию всего программного обеспечения, информации, объектов, баз данных и аппаратных средств, требующих изменений;
- получение формализованного одобрения детальных запросов/предложений на изменения перед началом работы;

- разрешение внесения изменений в прикладные программы авторизованным пользователем до их непосредственной реализации;

- осуществление процесса внедрения изменений в прикладные программы с минимальными отрицательными последствиями для бизнеса;

- обеспечение обновления комплекта системной документации после завершения каждого изменения и архивирование или утилизация старой документации;

- поддержку контроля версий для всех обновлений программного обеспечения;

- регистрацию в журналах аудита всех запросов на изменение;

- коррекцию эксплуатационной документации (8.1.1) и пользовательских процедур в соответствии с внесенными изменениями;

- осуществление процесса внедрения изменений в согласованное время без нарушения затрагиваемых бизнес-процессов.

Во многих организациях используется среда, в которой пользователи тестируют новое программное обеспечение и которая отделена от среды разработки и среды промышленной эксплуатации. При этом обеспечивается возможность контроля нового программного обеспечения и дополнительная защита операционной информации, используемой в процессе тестирования.

10.5.2 Технический анализ изменений в операционных системах

Периодически возникает необходимость внести изменения в операционные системы, например, установить последнюю поддерживаемую версию программного обеспечения. В этих случаях необходимо провести анализ и протестировать прикладные системы с целью обеспечения уверенности в том, что не оказывается никакого неблагоприятного воздействия на их функционирование и безопасность. Необходимо, чтобы этот процесс учитывал:

- анализ средств контроля бизнес-приложений и процедур целостности, чтобы обеспечивать уверенность в том, что они не были скомпрометированы изменениями в операционной системе;

- обеспечение уверенности в том, что ежегодный план поддержки и бюджет предусматривает анализ и тестирование систем, которые необходимо осуществлять при изменениях в операционной системе;

- обеспечение своевременного поступления уведомлений об изменениях в операционной системе для возможности проведения соответствующего анализа их влияния на информационную безопасность перед установкой изменений в операционную систему;

- контроль документирования соответствующих изменений в планах обеспечения непрерывности бизнеса (раздел 11).

10.5.3 Ограничения на внесение изменений в пакеты программ

Модификаций пакетов программ следует избегать. Насколько это возможно и допустимо с практической точки зрения, поставляемые поставщиком пакеты программ следует использовать без внесения изменений. Там, где все-таки необходимо вносить изменения в пакет программ, следует учитывать:

- риск компрометации встроенных средств контроля и процесса обеспечения целостности;

- необходимость получения согласия поставщика;

- возможность получения требуемых изменений от поставщика в виде стандартного обновления программ;

- необходимость разработки дополнительных мер поддержки программного обеспечения, если организация в результате внесенных изменений станет ответственной за будущее сопровождение программного обеспечения.

В случае существенных изменений оригинальное программное обеспечение следует сохранять, а изменения следует вносить в четко идентифицированную копию. Все изменения необходимо полностью тестировать и документировать таким образом, чтобы их можно было повторно использовать, при необходимости, для будущих обновлений программного обеспечения.

10.5.4 Скрытые каналы утечки данных и «троянские» программы

Раскрытие информации через скрытые каналы может происходить косвенными и неавторизованными способами. Этот процесс может быть результатом активации изменений параметров доступа как к защищенным, так и к незащищенным элементам информационной системы, или посредством вложения информации в поток данных. «Троянские» программы предназначены для того, чтобы воздействовать на систему неавторизованным и незаметным способом, при этом данное воздействие осуществляется как на получателя данных, так и на пользователя программы. Скрытые каналы утечки и «троянские» программы редко возникают случайно. Там, где скрытые каналы или «троянские» программы являются проблемой, необходимо применять следующие мероприятия по обеспечению информационной безопасности:

- закупку программного обеспечения осуществлять только у доверенного источника;

- по возможности закупать программы в виде исходных текстов с целью их проверки;

- использовать программное обеспечение, прошедшее оценку на соответствие требованиям информационной безопасности;
- осуществлять проверку исходных текстов программ перед их эксплуатационным применением;
- осуществлять контроль доступа к установленным программам и их модификациям;
- использование проверенных сотрудников для работы с ключевыми системами.

10.5.5 Разработка программного обеспечения с привлечением сторонних организаций

В случаях, когда для разработки программного обеспечения привлекается сторонняя организация, необходимо применять следующие меры обеспечения информационной безопасности:

- контроль наличия лицензионных соглашений и определенности в вопросах собственности на программы и соблюдения прав интеллектуальной собственности (12.1.2);
- сертификацию качества и правильности выполненных работ;
- заключение «escrow» соглашения, предусматривающих депонирование исходного текста на случай невозможности третьей стороны выполнять свои обязательства;
- обеспечение прав доступа для аудита с целью проверки качества и точности выполненной работы;
- документирование требований к качеству программ в договорной форме;
- тестирование перед установкой программ на предмет обнаружения «Троянского коня».

11 Управление непрерывностью бизнеса

11.1 Вопросы управления непрерывностью бизнеса

Цель: противодействие прерываниям бизнеса и защита критических бизнес-процессов от последствий при значительных сбоях или бедствиях.

Необходимо обеспечивать управление непрерывностью бизнеса с целью минимизации отрицательных последствий, вызванных бедствиями и нарушениями безопасности (которые могут быть результатом природных бедствий, несчастных случаев, отказов оборудования и преднамеренных действий), до приемлемого уровня с помощью комбинирования профилактических и восстановительных мероприятий по управлению информационной безопасностью.

Последствия от бедствий, нарушений безопасности и отказов в обслуживании необходимо анализировать. Необходимо разрабатывать и внедрять планы обеспечения непрерывности бизнеса с целью восстановления бизнес-процессов в течение требуемого времени при их нарушении. Такие планы следует поддерживать и применять на практике, чтобы они стали составной частью всех процессов управления.

Необходимо, чтобы управление непрерывностью бизнеса включало мероприятия по управлению информационной безопасностью для идентификации и уменьшения рисков, ограничения последствий разрушительных инцидентов и обеспечения своевременного возобновления наиболее существенных бизнес-операций.

11.1.1 Процесс управления непрерывностью бизнеса

Необходимо, чтобы существовал управляемый процесс развития и поддержания непрерывности бизнеса для всей организации. Этот процесс должен объединять ключевые элементы управления непрерывностью бизнеса:

- понимание рисков, с которыми сталкивается организация, с точки зрения вероятности возникновения и последствий, включая идентификацию и определение приоритетов критических бизнес-процессов;
- понимание возможных последствий нарушения бизнес-процессов в случае незначительных или существенных инцидентов, потенциально угрожающих жизнедеятельности организации, а также выбора средств и способов обработки информации, которые соответствовали бы целям бизнеса;
- организацию оптимального страхования результатов обработки информации, которое должно быть частью процесса обеспечения непрерывности бизнеса;
- формулирование и документирование стратегии непрерывности бизнеса в соответствии с согласованными бизнес-целями и приоритетами;
- формулирование и документирование планов обеспечения непрерывности бизнеса в соответствии с согласованной стратегией;
- регулярное тестирование и обновление планов развития информационных технологий и существующих процессов;
- обеспечение органичного включения в процессы и структуру организации планов управления непрерывностью бизнеса. Ответственность за координацию процесса управления непрерывностью

бизнеса следует возлагать на орган, обладающий соответствующими полномочиями в организации, например на управляющий совет по информационной безопасности (4.1.1).

11.1.2 Непрерывность бизнеса и анализ последствий

Необходимо, чтобы планирование непрерывности бизнеса начиналось с идентификации событий, которые могут быть причиной прерывания бизнес-процессов, например отказ оборудования, наводнение или пожар. Планирование должно сопровождаться оценкой рисков с целью определения последствий этих прерываний (как с точки зрения масштаба повреждения, так и периода восстановления). Оценку рисков необходимо осуществлять при непосредственном участии владельцев бизнес-ресурсов и участников бизнес-процессов. Оценка риска должна распространяться на все бизнес-процессы и не ограничиваться только средствами обработки информации.

В зависимости от результатов оценки рисков необходимо разработать стратегию для определения общего подхода к обеспечению непрерывности бизнеса. Разработанный план должен быть утвержден руководством организации.

11.1.3 Разработка и внедрение планов обеспечения непрерывности бизнеса

Следует разрабатывать планы по поддержке или восстановлению бизнес-операций в требуемые периоды времени после прерывания или отказа критических бизнес-процессов. Необходимо, чтобы план обеспечения непрерывности бизнеса предусматривал следующие мероприятия по обеспечению информационной безопасности:

- определение и согласование всех обязанностей должностных лиц и процедур на случай чрезвычайных ситуаций;

- внедрение в случае чрезвычайных ситуаций процедур, обеспечивающих возможность восстановления бизнес-процессов в течение требуемого времени. Особое внимание следует уделять оценке зависимости бизнеса от внешних факторов и существующих контрактов;

- документирование согласованных процедур и процессов;

- соответствующее обучение сотрудников действиям при возникновении чрезвычайных ситуаций, включая кризисное управление;

- тестирование и обновление планов обеспечения непрерывности бизнеса.

Необходимо, чтобы план обеспечения непрерывности бизнеса соответствовал требуемым целям бизнеса, например восстановлению определенных сервисов для клиентов за приемлемый промежуток времени. Следует учитывать потребности в необходимых для этого сервиса ресурсов, включая укомплектование персоналом, альтернативными ресурсами для средств обработки информации, а также меры по переходу на аварийный режим работы для этих средств .

11.1.4 Структура планов обеспечения непрерывности бизнеса

Следует поддерживать единую структуру планов обеспечения непрерывности бизнеса в целях обеспечения непротиворечивости всех планов и определения приоритетов для тестирования и обслуживания средств и систем обработки информации. Необходимо, чтобы каждый план обеспечения непрерывности бизнеса четко определял условия его реализации, а также должностных лиц, ответственных за выполнение каждого его пункта. При выявлении новых требований необходимо вносить соответствующие корректировки в процедуры на случай чрезвычайных ситуаций, например в планы эвакуации или в любые существующие планы по переходу на аварийный режим работы.

Необходимо, чтобы в структуре планов обеспечения непрерывности бизнеса предусматривалось следующее:

- условия реализации планов, которые определяют порядок действий должностных лиц, которому необходимо следовать (как оценивать ситуацию, кто должен принимать участие, и т. д.) перед введением в действие каждого пункта плана;

- процедуры на случай чрезвычайных ситуаций, которые должны быть предприняты после инцидента, подвергающего опасности бизнес-операции и/или человеческую жизнь. Необходимо, чтобы они включали также меры по управлению связями с общественностью и эффективное взаимодействие с соответствующими государственными органами, например с милицией, пожарной охраной и местными органами власти;

- процедуры перехода на аварийный режим работы, которые описывают необходимые действия по переносу важных бизнес-операций или сервисов-поддержки в альтернативное временное место размещения и по восстановлению бизнес-процессов в требуемые периоды времени;

- процедуры возобновления работы, которые описывают необходимые действия для возвращения к нормальному режиму ведения бизнеса;

- график поддержки плана, который определяет сроки и методы тестирования, а также описание процесса поддержки плана;

- мероприятия по обучению персонала, которые направлены на понимание процессов обеспечения непрерывности бизнеса сотрудниками, и поддержание постоянной эффективности этих процессов;

- обязанности должностных лиц, ответственных за выполнение каждого пункта плана. При необходимости должны быть указаны альтернативные ответственные.

Необходимо, чтобы за каждый план отвечал конкретный руководитель (сотрудник). Чрезвычайные меры, планы по переходу на аварийный режим ручной обработки, планы по возобновлению работы следует включать в сферу ответственности владельцев соответствующих бизнес-ресурсов или участников затрагиваемых процессов. За меры по переходу на аварийный режим работы с использованием альтернативных технических средств, таких как средства обработки информации и связи, ответственность несут поставщики услуг.

11.1.5 Тестирование, поддержка и пересмотр планов по обеспечению непрерывности бизнеса

11.1.5.1 Тестирование планов

Планы по обеспечению непрерывности бизнеса могут оказаться несостоятельными при тестировании из-за неправильных предпосылок разработки, недосмотру или вследствие изменений, связанных с заменой оборудования или персонала. Поэтому планы необходимо регулярно тестировать для обеспечения уверенности в их актуальности и эффективности. Такие тесты необходимы также для обеспечения знания своих обязанностей всеми членами команды восстановления и другим персоналом, имеющим к этому отношение.

Необходимо, чтобы в графике тестирования плана по обеспечению непрерывности бизнеса указывалось, как и когда следует проверять каждый пункт плана. Периодичность и методы тестирования отдельных пунктов плана могут быть различными. При этом могут использоваться следующие методы:

- тестирование («имитация прогона») различных сценариев (обсуждение мер по восстановлению бизнеса на различных примерах прерываний);

- моделирование (особенно для тренировки персонала по выполнению своих функций после инцидента и перехода к кризисному управлению);

- тестирование технического восстановления (обеспечение уверенности в эффективном восстановлении информационных систем);

- проверка восстановления в альтернативном месте (бизнес-процессы осуществляются параллельно с операциями по восстановлению в удаленном альтернативном месте);

- тестирование средств и сервисов-поставщиков (обеспечение уверенности в том, что предоставленные сторонними организациями сервисы и программные продукты удовлетворяют контрактным обязательствам);

- «генеральные репетиции» (тестирование того, что организация, персонал, оборудование, средства и процессы могут справляться с прерываниями).

Методы тестирования могут использоваться любой организацией и необходимо, чтобы они отражали специфику конкретного плана по восстановлению.

11.1.5.2 Поддержка и пересмотр планов

Планы по обеспечению непрерывности бизнеса необходимо поддерживать в актуальном состоянии путем проведения регулярных пересмотров и обновлений с целью обеспечения уверенности в их постоянной эффективности (11.1.5.1). В рамках программы развития организации необходимо предусматривать соответствующие процедуры, обеспечивающие непрерывность бизнеса.

Необходимо назначать ответственных за проведение регулярных пересмотров плана по обеспечению непрерывности бизнеса; идентифицированные изменения в бизнес-процессах, еще не отраженные в планах по обеспечению непрерывности бизнеса, должны быть учтены путем соответствующих обновлений планов. Формализованный процесс управления изменениями должен обеспечивать рассылку и ввод в действие обновленных планов в рамках их регулярных пересмотров.

Примеры ситуаций, которые могли бы потребовать обновления планов, включают приобретение нового оборудования или обновление операционных систем, а также изменения, связанные с:

- персоналом;
- адресами или номерами телефонов;
- стратегией бизнеса;
- местоположением, средствами и ресурсами;
- законодательством;
- подрядчиками, поставщиками и основными клиентами;
- процессами (как новыми, так и изъятыми);
- рисками (операционными и финансовыми).

12 Соответствие требованиям

12.1 Соответствие требованиям законодательства

Цель: предотвращение любых нарушений норм уголовного и гражданского права, обязательных предписаний и регулирующих требований или договорных обязательств, а также требований безопасности.

Проектирование и функционирование информационных систем, их использование и управление ими могут быть предметом обязательных предписаний, регулирующих требований, а также требований безопасности в договорных обязательствах.

Следует консультироваться с юристами организации или с практикующими юристами, имеющими соответствующую квалификацию, в отношении конкретных юридических вопросов. Следует иметь в виду, что законодательные требования в отношении информации, созданной в одной стране и переданной в другую страну (например, информационный поток, передаваемый за границу государства), различаются в разных странах.

12.1.1 Определение применимого законодательства

Все применяемые нормы законодательства, обязательные предписания, регулирующие требования и договорные обязательства, следует четко определять и документировать для каждой информационной системы. Конкретные мероприятия по обеспечению информационной безопасности и индивидуальные обязанности должностных лиц по выполнению этих требований необходимо соответствующим образом определять и документировать.

12.1.2 Права интеллектуальной собственности

12.1.2.1 Авторское право

Необходимо внедрять процедуры, обеспечивающие соответствие законодательным ограничениям на использование материала, в отношении которого могут существовать права на интеллектуальную собственность, такие как авторское право, права на проект, торговые марки. Нарушение авторского права может привести к судебным процессам, предполагающим возможность уголовной ответственности.

Законодательные, регулирующие и договорные требования могут вводить ограничения на копирование материалов, являющихся предметом собственности. В частности, эти ограничения могут содержать требования к использованию только тех материалов, которые или разработаны организацией, или лицензированы, или предоставляются разработчиком для организации.

12.1.2.2 Авторское право на программное обеспечение

Программные продукты, являющиеся предметом чьей-то собственности, обычно поставляются в рамках лицензионного соглашения, которое ограничивает использование продуктов определенными компьютерами, а также может ограничивать копирование их с целью создания резервных копий. В этих случаях для обеспечения информационной безопасности следует предусматривать применение следующих мероприятий:

- строгое следование требованиям авторского права на программное обеспечение, которое определяет законное использование программных и информационных продуктов;
- определение порядка и правил приобретения программных продуктов;
- обеспечение осведомленности сотрудников по вопросам авторского права на программное обеспечение принятых правил в отношении закупок, а также уведомление о применении дисциплинарных санкций к нарушителям;
- ведение соответствующих регистров активов;
- ведение подтверждений и доказательств собственности на лицензии, дистрибутивные диски, руководства и т.д.;
- контроль за соблюдением ограничений максимального числа разрешенных пользователей программными продуктами;
- регулярные проверки применения только авторизованного программного обеспечения и лицензированных продуктов;
- реализация политики по обеспечению выполнения условий соответствующих лицензионных соглашений;
- выполнение правил утилизации или передачи программного обеспечения в другие организации;
- организация регулярного аудита;
- соблюдение условий получения из общедоступных сетей программного обеспечения и информации (8.7.6).

12.1.3 Защита учетных записей организации

Важные данные организации необходимо защищать от утраты, разрушения и фальсификации. В отношении некоторых данных может потребоваться обеспечение безопасности хранения с целью выполнения законодательных или регулирующих требований, а также поддержки важных бизнес-приложений. В качестве примеров можно привести данные, которые могут потребоваться для доказательства того, что организация работает в рамках установленных законом норм или регулирующих требований, или с целью адекватной защиты от гражданского или уголовного преследования, а также подтверждения финансового состояния организации для акционеров, партнеров и аудиторов. Период времени хранения и содержание данных могут быть установлены в соответствии с государственными законами или регулирующими требованиями.

Данные необходимо классифицировать по типам, например, бухгалтерские записи, записи баз данных, журналы транзакций, журналы аудита и операционных процедур, каждый с указанием периодов хранения и типов носителей хранимых данных (бумага, микрофильм, магнитные или оптические носители). Любые криптографические ключи, связанные с зашифрованными архивами или цифровыми подписями (10.3.2 и 10.3.3), следует хранить безопасным способом и предоставлять к ним, при необходимости, доступ только авторизованным лицам.

Следует учитывать возможность снижения качества носителей, используемых для хранения данных, осуществлять процедуры по хранению и уходу за носителями данных в соответствии с рекомендациями изготовителя.

При использовании электронных носителей данных следует применять процедуры проверки возможности доступа к данным (например, читаемость как самих носителей, так и формата данных) в течение периода их хранения с целью защиты от потери вследствие будущих изменений в информационных технологиях.

Системы хранения данных следует выбирать таким образом, чтобы требуемые данные могли быть извлечены способом, приемлемым для суда, действующего по нормам гражданского или общего права, например, возможность вывода всех необходимых записей в приемлемый период времени и в приемлемом формате.

Необходимо, чтобы система хранения обеспечивала четкую идентификацию данных, а также период их хранения, установленных законом или регулирующими требованиями. Эта система должна предоставлять возможности по уничтожению данных после того периода, когда у организации отпадет потребность в их хранении.

С целью выполнения данных обязательств организации следует:

- разработать руководство в отношении сроков, порядка хранения и утилизации информации;
- составить график хранения наиболее важных данных;
- вести опись источников ключевой информации;
- внедрить соответствующие меры для защиты важной информации от потери, разрушения и фальсификации.

12.1.4 Защита данных и конфиденциальность персональной информации

В ряде стран введены нормы законодательства, в которых установлены ограничения в отношении обработки и передачи персональных данных (в основном, это касается информации о живущих людях, которые могут быть идентифицированы по этой информации). Такие ограничения могут налагать обязанности на тех, кто осуществляет сбор, обработку и распространение личной информации, а также могут ограничивать возможность передачи этих данных в другие страны.

Соответствие законодательству по защите данных требует соответствующей структуры управления информационной безопасностью. Лучше всего это достигается при назначении должностного лица, отвечающего за защиту данных путем соответствующего разъяснения менеджерам, пользователям и поставщикам услуг об их индивидуальной ответственности, а также обязательности выполнения соответствующих мероприятий по обеспечению информационной безопасности. Владельцы данных обязаны информировать это должностное лицо о любых предложениях о способах хранения персональной информации в структуре файла данных, а также знать применяемые нормы законодательства в отношении защиты личных данных.

12.1.5 Предотвращение нецелевого использования средств обработки информации

Средства обработки информации организации предназначены для обеспечения потребностей бизнеса.

Руководство должно определить уровни полномочий пользователей в отношении использования средств обработки информации. Любое использование этих средств для непроизводственных или неавторизованных целей, без одобрения руководства, следует расценивать как нецелевое. Если такая деятельность выявлена мониторингом или другими способами, то на это следует обратить внимание

непосредственного руководителя сотрудника для принятия соответствующих мер дисциплинарного воздействия.

Законность использования мониторинга зависит от действующего в стране законодательства и может потребоваться, чтобы сотрудники были осведомлены и дали документированное согласие на проведение мониторинга. Перед осуществлением мониторинга необходимо получить консультацию юриста.

Многие страны имеют или находятся в процессе введения законодательства по защите от неправильного использования компьютеров. Возможны случаи использования компьютера для неавторизованных целей с преступным умыслом. Поэтому важно, чтобы все пользователи были осведомлены о четких рамках разрешенного им доступа. Это может быть достигнуто, например, путем ознакомления пользователей с предоставленной им авторизацией в письменной форме под роспись, а организации следует безопасным способом хранить копию этого документа. Необходимо, чтобы сотрудники организации и пользователи третьей стороны были осведомлены о том, что во всех случаях они имеют право доступа только к тем данным, использование которых им разрешено.

Необходимо, чтобы при регистрации доступа к системе на экране компьютера было отражено предупреждающее сообщение, указывающее, что система, вход в которую пользователи пытаются осуществить, является системой с ограниченным доступом, и что неавторизованный доступ к ней запрещен. Пользователь должен подтвердить это прочтение и реагировать соответствующим образом на него, чтобы продолжить процесс регистрации.

12.1.6 Регулирование использования средств криптографии

В некоторых странах приняты соглашения, законы, регулирующие требования или другие инструменты, определяющие мероприятия по обеспечению безопасности доступа к криптографическим средствам и их использованию. Такие мероприятия обычно включают:

- ограничения импорта и/или экспорта аппаратных и программных средств для выполнения криптографических функций;

- ограничения импорта и/или экспорта аппаратных и программных средств, которые разработаны таким образом, что имеют, как дополнение, криптографические функции;

- обязательные или дискреционные методы доступа со стороны государства к информации, зашифрованной с помощью аппаратных или программных средств для обеспечения конфиденциальности ее содержания.

Для обеспечения уверенности в соответствии политики использования криптографических средств в организации национальному законодательству необходима консультация юриста. Прежде чем зашифрованная информация или криптографическое средство будут переданы в другую страну, необходимо также получить консультацию юриста.

12.1.7 Сбор доказательств

12.1.7.1 Правила использования и сбора доказательств

Необходимо иметь адекватные свидетельства, чтобы поддерживать иски или меры воздействия, направленные против физического лица или организации, которые нарушили правила управления информационной безопасностью.

Всякий раз, когда эти меры воздействия являются предметом внутреннего дисциплинарного процесса, свидетельства должны быть описаны в соответствии с внутренними процедурами.

Когда меры воздействия/иски затрагивают вопросы как гражданского, так и уголовного права, необходимо, чтобы представленные свидетельства соответствовали требованиям к сбору свидетельств, изложенными в соответствующих правовых нормах или требованиям конкретного суда, в котором будет рассматриваться данный вопрос. В общем случае, эти правила предусматривают:

- допустимость свидетельств: действительно ли свидетельства могут использоваться в суде или нет;

- весомость свидетельств: качество и полнота свидетельств;

- адекватное свидетельство того, что эти меры контроля (процесс сбора свидетельств) осуществлялись корректно и последовательно в течение всего периода, когда установленное свидетельство инцидента нарушения информационной безопасности было сохранено и обработано системой.

12.1.7.2 Допустимость доказательств

Чтобы достичь признания допустимости свидетельств, организациям необходимо обеспечить уверенность в том, что их информационные системы соответствуют всем юридическим требованиям и правилам в отношении допустимых свидетельств.

12.1.7.3 Качество и полнота доказательств

Чтобы достичь качества и полноты свидетельств, необходимо наличие убедительных подтверждений свидетельств. В общем случае, такие убедительные подтверждения могут быть достигнуты следующим образом:

- для бумажных документов: оригинал хранится безопасным способом и фиксируется, кто нашел его, где он был найден, когда он был найден и кто засвидетельствовал обнаружение. Необходимо, чтобы любое исследование подтвердило, что оригиналы никто не пытался исказить;

- для информации на компьютерных носителях: копии информации, для любых сменных носителей информации, для жестких дисков или из основной памяти компьютера, следует выполнять таким образом, чтобы обеспечить их доступность. Журнал всех действий, выполненных в течение процесса копирования, необходимо сохранять, а сам процесс копирования необходимо документировать. Одну копию носителей информации и журнал следует хранить безопасным способом.

Когда инцидент обнаруживается впервые, не очевидно, что он может привести к возможным судебным разбирательствам. Поэтому, существует опасность, что необходимое показание будет случайно разрушено прежде, чем осознана серьезность инцидента. Целесообразно на самом раннем этапе привлекать юриста или милицию в любом случае предполагаемых судебных разбирательств и получать консультацию относительно требуемых свидетельств.

12.2 Пересмотр политики безопасности и техническое соответствие требованиям безопасности

Цель: обеспечение соответствия систем политике безопасности организации и стандартам.

Безопасность информационных систем необходимо регулярно анализировать и оценивать.

Такой анализ (пересмотр) необходимо осуществлять в отношении соответствующих политик безопасности, а программные средства и информационные системы должны подвергаться аудиту на предмет соответствия этим политикам.

12.2.1 Соответствие политике безопасности

Руководители должны обеспечивать правильное выполнение всех процедур безопасности в пределах их зоны ответственности. Кроме того, все сферы деятельности организации необходимо подвергать регулярному пересмотру для обеспечения требований по обеспечению информационной безопасности. При этом, кроме функционирования информационных систем, анализу должна подвергаться также деятельность:

- поставщиков систем;
- владельцев информации и информационных активов;
- пользователей;
- руководства.

Владельцам информационных систем (5.1) следует проводить регулярные мониторинги их систем на соответствие принятым политикам безопасности и любым другим требованиям безопасности.

Вопросы мониторинга использования систем рассмотрены в 9.7.

12.2.2 Проверка технического соответствия требованиям безопасности

Проверка технического соответствия включает испытания операционных систем для обеспечения уверенности в том, что мероприятия по обеспечению информационной безопасности функционирования аппаратных и программных средств были внедрены правильно. Этот тип проверки соответствия требует технической помощи специалиста. Данную проверку следует осуществлять вручную (при помощи соответствующих инструментальных и программных средств, при необходимости) опытному системному инженеру или с помощью автоматизированного пакета программ, который генерирует технический отчет для последующего анализа техническим специалистом.

Проверка соответствия также включает тестирование на наличие попыток несанкционированного доступа к системе (проникновение), которое может быть выполнено независимыми экспертами, специально приглашенными по контракту для этого. Данное тестирование может быть полезным для обнаружения уязвимостей в системе и для проверки эффективности мер безопасности при предотвращении неавторизованного доступа вследствие этих уязвимостей. Особую осторожность следует проявлять в случаях, когда тест на проникновение может привести к компрометации безопасности системы и непреднамеренному использованию других уязвимостей.

Любая проверка технического соответствия должна выполняться только компетентными, авторизованными лицами либо под их наблюдением.

12.3 Меры безопасности при проведении аудита

Цель: максимизация эффективности и минимизация влияния на информационную безопасность в процессе аудита системы.

Необходимо предусматривать мероприятия по обеспечению информационной безопасности операционной среды и инструментальных средств аудита в процессе проведения аудита систем.

Защита также требуется для поддержания целостности информационной системы и предотвращения неправильного использования инструментальных средств аудита.

12.3.1 Мероприятия по обеспечению информационной безопасности при проведении аудита систем

Требования и действия аудита, включающие проверку операционных систем, необходимо тщательно планировать и согласовывать, чтобы свести к минимуму риск для бизнес-процессов. Необходимо учитывать следующее:

- требования аудита необходимо согласовать с соответствующим руководством;
- объем работ по проверкам следует согласовывать и контролировать;
- при проведении проверок необходимо использовать доступ только для чтения к программному обеспечению и данным;
- другие виды доступа могут быть разрешены только в отношении изолированных копий файлов системы, которые необходимо удалять по завершению аудита;
- необходимо четко идентифицировать и обеспечивать доступность необходимых ресурсов информационных систем для выполнения проверок;
- требования в отношении специальной или дополнительной обработки данных следует идентифицировать и согласовывать;
- весь доступ должен подвергаться мониторингу и регистрироваться с целью обеспечения протоколирования для последующих ссылок;
- все процедуры, требования и обязанности аудита следует документировать.

12.3.2 Защита инструментальных средств аудита систем

Доступ к инструментальным средствам аудита систем, то есть программному обеспечению или файлам данных, необходимо защищать, чтобы предотвратить любое возможное их неправильное использование или компрометацию. Такие инструментальные средства необходимо отделять от систем разработки и систем операционной среды, а также не хранить эти средства в библиотеках магнитных лент или пользовательских областях, если не обеспечен соответствующий уровень дополнительной защиты.

УДК 001.4:025.4:006.354 ОКС 01.040.01 Т00

Ключевые слова: информационная технология, информационная безопасность, риски, активы, охраняемая зона, контроль доступа, аудит

Редактор *М.В. Глушкова*
Технический редактор *В.Н. Прусакова*
Корректор *В.И. Варенцова*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 15.06.2006. Подписано в печать 08.08.2006. Формат 60 × 84 1/8. Бумага офсетная. Гарнитура Ариал.
Печать офсетная. Усл. печ. л. 6,98. Уч.-изд. л. 7,10. Тираж 400 экз. Зак. 534. С 3127.

ФГУП «Стандартинформ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано во ФГУП «Стандартинформ» на ПЭВМ.
Отпечатано в филиале ФГУП «Стандартинформ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

gost.e-ecolog.ru