МЕЖДУНАРОДНЫЙ СТАНДАРТ

ISO/IEC 17799

Первое издание

2000-12-01

Информационные технологии – практические правила управления информационной безопасностью

Шифр документа

ISO/IEC 17799:2000(E)

Содержание

Предисловие

Международная организация по стандартизации (ISO) и Международная электротехническая комиссия (IEC) образуют специализированную систему международной стандартизации. Государственные организации, являющиеся членами ISO или IEC, участвуют в разработке международных стандартов посредством технических комитетов, созданных соответствующими организациями для работы в определенных технических областях. Международные технические комитеты ISO и IEC сотрудничают в областях, представляющих интерес для обеих организаций. Кроме того, совместно с ISO и IEC в работе участвуют другие государственные и негосударственные международные организации.

Подготовка международных стандартов ведется согласно правилам, изложенным в части 3 Директив ISO/IEC.

В области информационных технологий организациями ISO и IEC создан объединенный технический комитет, ISO/IEC JTC 1. Разработанные варианты международных стандартов, принятые объединенным техническим комитетом, передаются организациям-участникам для голосования. Для публикации в качестве международного стандарта необходимо одобрение как минимум 75% организаций, участвующих в голосовании.

Необходимо обратить внимание на то, что некоторые элементы данного международного стандарта могут попадать под действие патентных прав. Организации ISO и IEC не должны нести ответственности за определение каких-либо из этих патентных прав.

Международный стандарт ISO/IEC 17799 был разработан Британским институтом стандартов (в качестве стандарта BS 7799) и принят Объединенным техническим комитетом ISO/IEC JTC 1 по информационным технологиям согласно специально «ускоренной процедуре» параллельно с утверждением в организациях-членах ISO и IEC.

Введение

Что такое информационная безопасность?

Информация – это ресурс, который, как и другие важные бизнес-ресурсы, имеет определенную ценность для организации и, следовательно, нуждается в соответствующей защите. Информационная безопасность предполагает защиту информации от разнообразных угроз для поддержки непрерывности бизнеса, сокращения убытков, увеличения прибылей на инвестированный капитал и расширения возможностей для бизнеса.

Информация может существовать в самых разных формах. Ее можно печатать или писать на бумаге, сохранять на электронных носителях, пересылать по традиционной или электронной почте, показывать в фильмах или передавать в устной беседе. Какую бы форму ни принимала информация и какие бы средства не использовались для ее передачи и хранения, необходимо всегда обеспечивать соответствующий уровень ее защиты. Под информационной безопасностью здесь подразумевается сохранение следующих характеристик:

a) конфиденциальность: предоставление доступа к информации только тем, у кого есть право на доступ к ней;

b) целостность: защита точности и полноты информации и методов обработки;

c) доступность: обеспечение доступа к информации и связанным с ней ресурсам авторизованным пользователям по мере необходимости.

Информационная безопасность достигается путем внедрения совокупности необходимых средств защиты, в число которых могут входить политики, рекомендации, инструкции, организационные структуры и программные функции. Эти средства необходимо реализовать для того, чтобы гарантировать выполнение требований к безопасности в конкретной организации.

Зачем нужна информационная безопасность

Информация и связанные с ней процессы, системы и сети являются важными бизнес-ресурсами. Конфиденциальность, целостность и доступность информации могут быть необходимы для поддержания конкурентоспособности, прибыльности, соответствия законодательству и коммерческой репутации.

Различные организации и принадлежащие им информационные системы и сети все чаще сталкиваются с угрозами для безопасности, причины которых могут быть самыми разными – компьютерное мошенничество, шпионаж, саботаж, вандализм, пожары и наводнения. Такие источники угроз как компьютерные вирусы, хакерские атаки и атаки типа «отказ в обслуживании» (Denial of Service), получают все большее распространение и становятся все более претенциозными и технически сложными.

Зависимость от информационных систем и сервисов означает, что организации становятся более уязвимыми. Объединение общедоступных и частных сетей и совместное использование информационных ресурсов увеличивает сложность реализации контроля доступа. Тенденция перехода к распределенной обработке данных уменьшила эффективность средств централизованного контроля.

При разработке многих информационных систем безопасность не принималась во внимание. Технические средства обеспечивают лишь ограниченный уровень безопасности. Для поддержки безопасности необходимо использовать также и организационные методы. Определение перечня средств, которые необходимо внедрить, требует тщательного планирования и внимания к деталям. Для поддержки информационной безопасности как минимум необходимо участие всех сотрудников организации. В дополнение к этому может

потребоваться участие поставщиков, клиентов и акционеров. Кроме того, может возникнуть необходимость в консультациях специалистов из других организаций.

Средства управления информационной безопасностью, вводимые на этапах формулировки требований и разработки, оказываются эффективнее и значительно дешевле.

Определение требований к безопасности

Любая организация должна определить свои требования к безопасности. При оценке требований используются три основных показателя.

Первым показателем служит оценка рисков, с которыми сталкивается организация. Путем оценки рисков определяется угрозы для ресурсов, их уязвимость и вероятность возникновения угроз, а также возможный ущерб.

Второй показатель – это законодательные, нормативные и договорные требования, которые должна соблюдать организация, ее партнеры по бизнесу, подрядчики и поставщики услуг.

Третий показатель – это определенный набор принципов, целей и требований к обработке информации, разработанных организацией для поддержки своей деятельности.

Оценка рисков, связанных с информационной безопасностью

Определение требований к безопасности производится путем методической оценки рисков. Расходы на поддержку безопасности необходимо сбалансировать с ущербом для бизнеса, который может возникнуть при нарушении безопасности. Методы оценки рисков могут применяться ко всей организации или лишь к ее частям, а также к отдельным информационным системам, системным компонентам и сервисам, в зависимости от того, что окажется наиболее практичным, реалистичным и полезным.

Оценка рисков – это систематический анализ следующих показателей:

a) ущерб для бизнеса, который может возникнуть при нарушении безопасности. При этом следует учитывать возможные последствия утраты конфиденциальности, целостности или доступности информации и других ресурсов;

b) оценка вероятности такого нарушения с учетом известных опасностей, уязвимостей и реализованных средств защиты.

Результаты такой оценки помогут определить необходимые действия и приоритеты для управления рисками, связанными с информационной безопасностью, и для реализации выбранных средств защиты от этих рисков. Процесс оценки рисков и выбора средств защиты может потребоваться выполнить несколько раз, чтобы охватить различные части организации или отдельные информационные системы.

Время от времени следует заново анализировать риски и реализованные средства, чтобы:

a) учесть изменения бизнес-требований и приоритетов;

b) принять во внимание новые угрозы и уязвимости;

c) убедиться в том, что реализованные средства сохранили эффективность.

Уровень выполняемых проверок может различаться в зависимости от результатов предыдущей оценки и изменения приоритетов различных рисков. Часто оценка рисков производится в два этапа: сначала на высоком уровне, чтобы определить приоритеты ресурсов в областях повышенного риска, а затем с большей детализацией, чтобы проанализировать специфические риски.

Выбор средств защиты

После определения требований к безопасности необходимо выбрать и реализовать средства, которые помогут снизить риск до приемлемого уровня. Применять можно средства, описанные в данном документе и в других источниках; кроме того, при необходимости можно разработать новые средства, отвечающие конкретным целям. Существует множество различных способов управления рисками. В данном документе приведены примеры распространенных подходов. Однако следует помнить, что некоторые средства подходят не для всех информационных систем и сред и могут оказаться неприменимыми или непрактичными в некоторых организациях. Например, в разделе 8.1.4 описан метод разделения полномочий для предотвращения мошенничества и ошибок. В небольших организациях разделение всех полномочий может оказаться невозможным, и для реализации той же цели придется применить другие средства. Другой пример: в разделах 9.7 и 12.1 описаны способы наблюдения за использованием системы и сбора улик. Описанные методы (например, ведение журнала событий) могут противоречить действующему законодательству – например, правилам обеспечения неприкосновенности частной информации клиентов или рабочих мест.

Средства необходимо выбирать с учетом затрат на реализацию в отношении к уменьшаемым рискам и потенциальным убыткам при нарушении безопасности. Кроме того, следует учитывать и такие нефинансовые факторы, как потеря репутации.

Некоторые методы, описанные в данном документе, могут считаться основополагающими для управления информационной безопасностью. Они подойдут для большинства организаций. Эти методы более подробно описаны ниже в разделе «Основа информационной безопасности».

Основа информационной безопасности

Существуют методы, которые можно считать основополагающими, позволяющие создать надежную основу для реализации информационной безопасности. Эти методы либо основаны на важных законодательных требованиях, либо относятся к общепризнанным методам работы в области информационной безопасности.

С законодательной точки зрения важнейшими для организации считаются следующие меры:

a) защита данных и неразглашение личной информации (см. раздел 12.1.4);

b) защита организационных записей (см. раздел 12.1.3);

c) защита прав на интеллектуальную собственность (см. раздел 12.1.2).

К общепризнанным методам обеспечения информационной безопасности относятся следующие:

a) создание документа, определяющего политику информационной безопасности (см. раздел 3.1);

b) распределение ответственности за информационную безопасность (см. раздел 4.1.3);

c) обучение и подготовка в области информационной безопасности (см. раздел 6.2.1);

d) создание отчетов об инцидентах (см. раздел 6.3.1);

e) поддержка непрерывности бизнеса (см. раздел 11.1).

Эти методы могут применяться в большинстве организаций и в большинстве сред. Заметим, что несмотря на то, что все описанные в данном документе методы являются важными, значимость каждого метода следует определять в свете конкретных рисков, с которыми сталкивается организация. Таким образом, хотя описанный выше подход и может послужить

хорошей основой, он не заменит собой выбор средств, основанный на оценке рисков.

Ключевые факторы успеха

Опыт показывает, что перечисленные ниже факторы зачастую являются ключевыми для успешной реализации информационной безопасности в организации.

a) определение политики, целей и направлений деятельность по обеспечению безопасности, отражающие задачи организации;

b) подход к реализации безопасности, соответствующий традициям организации;

c) явная поддержка руководства;

d) хорошее понимание требований к безопасности, оценки рисков и методов управления рисками;

e) вовлечение всех руководителей и сотрудников организации в процессы обеспечения безопасности;

f) передача сведений о политике информационной безопасности и стандартах всем сотрудникам и подрядчикам;

g) обеспечение необходимого обучения и подготовки;

h) полномасштабная и сбалансированная система измерения, позволяющая определять эффективность управления информационной безопасностью и принимать рекомендации по усовершенствованию.

Разработка собственных правил

Данный свод правил можно считать основой для разработки перечня правил для конкретной организации. Часть описанных здесь правил и средств может не подойти для какой-то организации. Кроме того, могут потребоваться дополнительные меры, не описанные в данном документе. В подобном случае рекомендуется сохранять ссылки на документацию, применявшуюся при разработке – это поможет аудиторам и деловым партнерам при проверке соответствия.

Информационные технологии – Практические правила управления информационной безопасностью

1 Область применения

Данный стандарт включает в себя рекомендации по управлению информационной безопасностью, предназначенные для сотрудников, ответственных за создание, внедрение и поддержку мер, обеспечивающих безопасность в организации. Этот документ должен послужить основой для разработки стандартов безопасности и эффективных методов управления безопасностью в конкретной организации. Кроме того, он поможет поддержать взаимное доверие при контактах между организациями. Рекомендации, приведенные в данном стандарте, следует выполнять с учетом действующих законов и нормативных требований.

2 Термины и определения

В данном документе используются перечисленные ниже определения.

2.1 Информационная безопасность

Сохранение конфиденциальности, целостности и доступности информации.

- **Конфиденциальность**
  Обеспечение доступа к информации только для авторизованных пользователей, имеющих право на доступ к ней.
- **Целостность**
  Защита точности и полноты информации и методов ее обработки.
- **Доступность**
  Обеспечение доступности информации и связанных с ней ресурсов авторизованным пользователям при необходимости.

2.2 Оценка рисков

Оценка угроз для информации и средств ее обработки, возможного ущерба для них в случае нарушения безопасности, их уязвимостей а также возможности их возникновения.

2.3 Управление рисками

Процесс определения, контроля и уменьшения или полного устранения (с приемлемыми затратами) рисков для информационной безопасности, которые могут повлиять на информационные системы,.

3 Политика безопасности

3.1 Политика информационной безопасности

Цель: Обеспечение направления и поддержки информационной безопасности руководством.
Руководство организации должно четко сформулировать требования политики и проявить и поддержку требований информационной безопасности путем распространения политики информационной безопасности во всей организации.

3.1.1 Описание политики информационной безопасности

Документ, содержащий описание политики информационной безопасности, должен быть одобрен руководством, опубликован и, согласно необходимости, распространен среди всех сотрудников. Этот документ должен выражать поддержку руководства компании и определять подход к управлению информационной безопасностью, который будет применяться в организации. Как минимум, данный документ должен включать следующие сведения:

a) определение информационной безопасности, ее общие цели и область действия, а также сведения о важности безопасности в качестве механизма, делающего возможным совместное использование информации (см. введение);

b) заявление о намерениях руководства, освещающее цели и принципы управления информационной безопасностью;

c) краткое описание политики безопасности, принципов, стандартов и нормативных требований, имеющих определенное значение для организации, например:

   1) соответствие требованиям законодательства и условиям контрактов;

   2) требования к образовательной подготовке в области безопасности;

   3) защита от вирусов и других злонамеренных программ;

   4) поддержка непрерывности бизнеса;

   5) последствия нарушения политики безопасности;

d) определение общих и частных обязанностей по управлению информационной безопасностью, в том числе предоставление сведений об инцидентах;

e) ссылки на документацию, которая может дополнять описание политики, например, более подробные описания политик и инструкций для конкретных информационных систем или правила безопасности, которые должны соблюдаться пользователями.

Данное описание политики необходимо распространить среди пользователей во всей организации в подходящем и удобочитаемом для них виде.

3.1.2 Обновление и оценка

Необходимо назначить сотрудника, отвечающего за поддержку политики и ее обновление согласно принятой процедуре обновления. Данная процедура должна гарантировать пересмотр политики в ответ на любые изменения, влияющие на основу исходной оценки рисков – например, крупные инциденты, связанные с безопасностью, новые уязвимости или изменения в организационной или технической инфраструктуре. Кроме того, необходимо создать график периодической переоценки следующих критериев:

a) эффективность политики, демонстрируемая на основе типов, количества и ущерба от

зарегистрированных инцидентов;

b) стоимость и воздействие мер безопасности на эффективность деятельности организации;

c) воздействие технологических изменений.

4 Организационная безопасность

4.1 Инфраструктура информационной безопасности

Цель: Управление информационной безопасностью в организации.

Чтобы приступить к внедрению средств информационной безопасности в организации, необходимо создать структуру управления.

В составе руководства компании следует создать совет для принятия политики информационной безопасности, рапределения ролей по обеспечению безопасности, и координации внедрения средств безопасности во всей организации. При необходимости следует создать консультационный центр по вопросам безопасности, в который можно было бы обращаться из любой части организации. Необходимо наладить контакты со специалистами в области безопасности вне компании, чтобы не отставать от развития данной отрасли, следить за стандартами и методами оценки и находить подходящие точки соприкосновения при реакции на инциденты. Следует поощрять развитие многостороннего подхода к информационной безопасности (например, сотрудничество и совместную работу руководителей, пользователей, администраторов, разработчиков приложений, аудиторов и сотрудников, ответственных за безопасность) и приобретение познаний в таких областях, как страхование и управление рисками.

4.1.1 Совет по управлению информационной безопасностью

Ответственность за информационную безопасность лежит на всех членах руководящей группы. Поэтому рекомендуется создать совет, помогающий обеспечить четкое понимание и явную поддержку инициатив, связанных с безопасностью. Этот совет должен способствовать продвижению безопасности в организации путем выполнения соответствующих обязательств и тщательного подбора кадров. Совет может быть частью существующего управляющего органа. Как правило, деятельность такого совета включает в себя следующие задачи:

a) изучение и одобрение политики информационной безопасности и распределения обязанностей;

b) отслеживание значимых изменений в степени подверженности информационных ресурсов основным угрозам;

c) отслеживание и анализ инцидентов, связанных с информационной безопасностью;

d) поддержка инициатив, помогающих улучшить информационную безопасность.

За все задачи, связанные с безопасностью, должен нести ответственность один руководитель.

4.1.2 Координация в области информационной безопасности

В крупных организациях может потребоваться создание многоцелевого совета из представителей руководства соответствующих отделов организации для координирования внедрения средств информационной безопасности. Как правило, данный совет берет на себя следующие задачи:

a) согласование должностей и обязанностей, связанных с информационной безопасностью, во всей организации;

b) согласование методов и процедур, связанных с информационной безопасностью (например, оценки рисков и классификации инормации);

c) согласование и поддержка инициатив в области информационной безопасности в масштабах всей организации (например, программы ознакомления с требованиями безопасности);

d) включение мер по обеспечению безопасности в процесс планирования процедур, связанных с информацией;

e) оценка пригодности и координация внедрения конкретных средств информационной безопасности для новых систем и сервисов;

f) анализ инцидентов, связанных с информационной безопасностью;

g) содействие развитию поддержки информационной безопасности во всей организации.

4.1.3 Распределение обязанностей, связанных с информационной безопасностью

Необходимо четко определить ответственность за защиту отдельных ресурсов и за выполнение конкретных процедур, связанных с безопасностью.

Политика информационной безопасности (см. часть 3) должна включать в себя общие правила по распределению должностей и обязанностей, связанных с информационной безопасностью. В случае необходимости эту политику нужно дополнить более подробными правилами для конкретных отделов, систем или сервисов. Следует четко определить локальную ответственность за отдельные физические и информационные ресурсы и процессы, связанные с безопасностью, например, планирование непрерывности бизнеса.

Во многих организациях назначается руководитель подразделения информационной безопасности, который принимает на себя общую ответственность за разработку и внедрение средств безопасности и за руководство выбором этих средств.

Однако обязанности за набор персонала и реализацию конкретных средств зачастую сохраняются за другими сотрудниками. Распространенным методом является назначение владельца каждого информационного ресурса. Такой владелец несет ответственность за ежедневное обеспечение безопасности своего ресурса.

Владельцы информационных ресурсов могут передавать свои обязанности, связанные с безопасностью, отдельным сотрудникам или поставщикам услуг. Несмотря на это, владелец несет полную ответственность за безопасность ресурса. Он должен иметь возможность контролировать корректность освобождения других сотрудников от переданных им обязанностей, связанных с безопасностью.

Следует четко определить круг обязанностей каждого руководителя. В частности, необходимо соблюдать перечисленные ниже правила.

a) должны быть четко определены ресурсы и процессы, связанные с безопасностью каждой отдельно взятой системы,

b) должны быть определены руководители, ответственные за каждый ресурс или процесс, связанный с безопасностью. Обязанности каждого руководителя должны быть подробно сформулированы в соответствующем документе.

c) Необходимо четко определить и документировать уровни авторизации.

4.1.4 Процесс утверждения средств обработки информации

Требуется разработать процесс, согласно которому введение новых средств обработки информации будет утверждаться руководством.

Необходимо принимать во внимание следующее:

a) Новые средства должны пройти соответствующее утверждение среди руководства для однозначного определения их назначения и способа применения. Кроме того, руководитель, ответственный за поддержку безопасности локальной информационной системы, должен одобрить эти средства и подтвердить соблюдение всех необходимых условий и требований политики безопасности.

b) При необходимости оборудование и программное обеспечение следует проверить на совместимость с другими компонентами системы.

c) Примечание: для определенных подключений может потребоваться согласование типовых образцов.

d) Применение личных средств обработки информации для работы с информацией организации и применение всех необходимых средств управления информационной безопасностью должно быть санкционировано.

e) Применение личных средств обработки информации на рабочем месте может привести к появлению новых уязвимостей, поэтому в данном случае требуется их отдельная проверка и утверждение.

Эти соображения имеют особую важность при работе в сетевой среде.

4.1.5 Консультации специалистов по информационной безопасности

Как правило, консультации специалистов по безопасности требуются большинству организаций. В идеале следует пригласить опытного консультанта по информационной безопасности на постоянную работу. Однако не каждая организация имеет возможность включить в свой штат консультанта-специалиста. В подобных случаях рекомендуется назначить сотрудника, который будет координировать и согласовывать действия, связанные с вопросами безопасности в организации, и помогать при принятии решений в области безопасности. Такие сотрудники должны иметь возможность обращаться к сторонним консультантам для получения советов по вопросам, выходящим за рамки их компетенции.

В обязанности консультантов по информационной безопасности должны входить консультации по всем аспектам информационной безопасности – как на основе собственного опыта, так и с привлечением специалистов со стороны. Эффективность средств информационной безопасности в организации будет определяться способностью такого консультанта оценить угрозы для безопасности и предложить рекомендации по поводу необходимых мер. Чтобы обеспечить максимальную эффективность, консультанты должны иметь возможность напрямую обращаться ко всем руководителям в организации.

К консультанту по информационной безопасности следует обращаться как можно раньше в случае обнаружения уязвимостей или возникновения инцидентов, связанных с безопасностью, чтобы получить совет специалиста или помощь при изучении обстоятельств. Хотя в большинстве случаев внутренние расследования, связанные с безопасностью, проводятся представителями руководства, к ним можно привлечь и специалиста по информационной безопасности, который будет консультировать проводящих расследование сотрудников, руководить ими или осуществлять само расследование.

4.1.6 Сотрудничество между организациями

Необходимо поддерживать связь с правоохранительными и регулятивными органами, поставщиками информационных услуг и операторами телекоммуникационных служб, чтобы в случае инцидентов иметь возможность быстро принять соответствующие меры и получить консультации. По той же причине следует подумать об участии в группах обеспечения безопасности и отраслевых промышленных советах.

Обмен сведениями о мерах безопасности следует ограничить, чтобы не допустить утечки конфиденциальной информации из организации.

4.1.7 Независимая оценка информационной безопасности

В документе, описывающем политику информационной безопасности (см. раздел 3.1), определяется политика и ответственность за информационную безопасность. Реализация политики информационной безопасности должна быть оценена независимыми специалистами. Они должны проверить, насколько введенные в организации меры отражают требования политики и насколько они практичны и эффективны (см. раздел 12.2).

Такая оценка может быть произведена внутренними аудиторами, независимым специалистом или сторонней организацией, специализирующейся на таких проверках. Убедитесь, что кандидаты на эту роль обладают необходимыми навыками и опытом.

4.2 Безопасность доступа со стороны внешних пользователей

Цель: Обеспечить безопасность доступа к средствам обработки информации и информационным ресурсам организации со стороны внешних пользователей.

Доступ посторонних к принадлежащим организации средствам обработки информации необходимо контролировать.

Если необходимость такого доступа диктуется спецификой выполняемой задачи, следует провести оценку рисков и определить влияние на безопасность и требуемые средства контроля. Средства контроля следует согласовать со сторонней организацией и указать в договоре.

Доступ к информационным ресурсам организации могут получать и другие сторонние участники. Контракты, предполагающие доступ со стороны, должны включать в себя сведения о возможности назначения других участников и условиях их доступа.

Данный стандарт можно использовать в качестве основы для подобных контрактов; кроме того, его можно использовать при оценке необходимости привлечения других организаций к обработке информации.

4.2.1 Определение рисков, связанных с доступом со стороны внешних пользователей

4.2.1.1 Типы доступа

Тип доступа, предоставляемого сторонней организации, имеет особую важность. Например, риски при доступе через сетевое соединение отличаются от рисков при физическом доступе. Следует рассмотреть следующие типы доступа:

a) физический доступ – например, доступ к помещениям, компьютерным залам, шкафам с документацией;

b) логический доступ – например, доступ к базам данных и информационным системам организации.

4.2.1.2 Причины предоставления доступа

Доступ сторонним организациям может предоставляться по самым разным причинам. Например, существуют группы, которые не находятся на территории организации, однако имеют физический и логический доступ к ресурсам организации для выполнения определенных обязанностей, например:

a) группы поддержки оборудования и программного обеспечения, которым необходим доступ к системам и прикладным программам на низком уровне;

b) коммерческие партнеры и совместные предприятия, которые могут обмениваться информацией, работать с информационными системами или совместно использовать базы данных.

Доступ из сторонних организаций с недостаточно высоким уровнем информационной безопасности может представлять угрозу для безопасности информации. При возникновении необходимости подключения к сторонней организации следует провести оценку рисков и определить, какие меры безопасности следует ввести. При этом следует учитывать тип необходимого доступа, ценность информации, средства, реализованные сторонней организацией, и влияние такого доступа на безопасность информации в организации.

4.2.1.3 Подрядчики, работающие на территории организации

Сторонние группы, которые согласно условиям договора в течение определенного времени находятся на территории организации, также могут ослабить безопасность. Вот несколько примеров таких групп:

a) группы поддержки оборудования и программного обеспечения;

b) уборщики, снабженцы, охрана и другие вспомогательные службы, нанятые на стороне;

c) студенты и другие временные работники;

d) консультанты.

Необходимо понять, какие меры требуются для управления доступом посторонних к средствам обработки информации. Как правило, все требования к безопасности, связанные с доступом со стороны, и внутренние меры должны быть отражены в договоре со сторонней организацией (см. также раздел 4.2.2). Например, при необходимости сохранения конфиденциальности информации можно использовать соглашения о конфиденциальности (или о неразглашении конфиденциальной информации) (см. раздел 6.1.3).

Доступ к информации и средствам ее обработки должен предоставляться сторонним организациям только после реализации необходимых средств защиты и подписания договора, определяющего условия подключения или доступа.

4.2.2 Требования к безопасности при контрактах со сторонними организациями

Соглашения, подразумевающие доступ сторонних подрядчиков к принадлежащим организации средствам обработки информации, должны заключаться на основе формального контракта, включающего в себя все необходимые требования к безопасности или ссылки на них. Это поможет обеспечить соответствие стандартам и политике безопасности, принятой в организации. Такой контракт должен гарантировать отсутствие разногласий между организацией и сторонним подрядчиком. Организации должны иметь систему защиты от убытков, связанных с поставщиком. Следует рассмотреть включение в контракт следующих сведений:

a) общее описание политики информационной безопасности;

b) описание защиты ресурсов, в том числе:

1) процедуры защиты ресурсов организации, в том числе информации и программного обеспечения;

2) процедуры, позволяющие определить факты компрометации ресурсов, например, потерю или модификацию данных;

3) средства, гарантирующие возврат или уничтожение информации и ресурсов по истечении срока контракта или на оговоренном этапе;

4) целостность и доступность;

5) ограничения на копирование и раскрытие информации;

c) описание всех предоставляемых услуг;

d) целевой уровень услуг и неприемлемые уровни услуг;

e) порядок допуска персонала поставщика к информации и ресурсам;

f) е) соответствующие обязательства сторон, заключающих договор;

g) ж) ответственность, связанная с требованиями законодательства, например, законов о защите данных; в том случае, если контракт подразумевает сотрудничество с организациями в других странах, необходимо уделить особое внимание законодательным системам других стран (см. также раздел 12.1);

h) з) права на интеллектуальную собственность, присвоение авторских прав (см. раздел 12.1.2) и защита совместной работы (см. также раздел 6.1.3).

i) и) соглашения по контролю доступа, включая:

1) разрешенные методы доступа, а также контроль и использование уникальных идентификаторов, например, пользовательских идентификаторов и паролей;

2) процесс авторизации для получения пользовательского доступа и привилегий;

3) необходимость обязательной поддержки списка лиц, имеющих полномочия на использование предоставленных услуг, с указанием их прав и привилегий в отношении такого использования;

j) к) определение поддающихся проверке критериев эффективности, методов их мониторинга и отчетности;

k) л) право на мониторинг деятельности пользователей и прекращение доступа;

l) м) право на аудит обязанностей по контракту или выполнение этого аудита сторонней организацией;

m) н) установление процесса эскалации для решения проблем; при необходимости следует также предусмотреть возможность возникновения нештатных ситуаций;

n) о) обязанности по установке и обслуживанию оборудования и программного обеспечения;

o) п) четкая структура отчетности и согласованные форматы отчетов;

p) р) четкий и определенный процесс организации внесения изменений;

q) с) все необходимые средства физической защиты и механизмы, обеспечивающие соблюдение принятых мер;

r) т) подготовка пользователей и администраторов в области методов, процедур и безопасности;

s) у) средства защиты от злонамеренного программного обеспечения (см. раздел 8.3).

t) ф) соглашения о об оповещении об обнаружении, уведомлении о происшедших инцидентах и нарушений безопасности, а также их расследовании

u) х) участие субподрядчиков в деятельности сторонней организации.

4.3 Контракты на аутсорсинг

Цель: Обеспечить безопасность информации в том случае, когда ответственность за обработку информации возлагается на другую организацию.

Контракты на аутсорсинг должны разрабатываться с учетом рисков, мер безопасности и процедур для информационных систем, сетей и/или рабочих мест.

4.3.1 Требования к безопасности в контрактах на аутсорсинг

Требования к безопасности в организации, возлагающей на другую организацию обязанности по контролю всех или части своих информационных систем, сетей и/или рабочих мест, должны быть оговорены в контракте, заключенном между сторонами.

В частности, контракт должен включать следующие сведения:

a) как будет обеспечиваться соответствие требованиям законодательства (например, законам о защите данных);

b) какими мерами будет гарантироваться, что всем сторонам, участвующим в контракте на аутсорсинг, в том числе субподрядчикам, известны их обязанности, связанные с безопасностью;

c) методы обеспечения и проверки целостности и конфиденциальности бизнес-ресурсов организации;

d) физические и логические средства, которые должны использоваться для обеспечения доступа к конфиденциальной информации, связанной с деятельностью организации, только авторизованных пользователей;

e) методы поддержки доступности сервисов в чрезвычайных обстоятельствах;

f) уровни физической безопасности, которые должны быть обеспечены для оборудования, предоставляемого другой стороной;

g) право на аудит.

Кроме того, следует принять во внимание то, что условия, перечисленные в разделе 4.2.2., также должны быть включены в данный контракт. Контракт должен давать возможность более подробно описать требования к безопасности и процедуры в плане управления безопасностью, который будет принят обеими сторонами.

Хотя контракты на аутсорсинг могут привести к возникновению ряда сложных вопросов в области безопасности, описанные в данном своде правил рекомендации могут послужить основой для согласования структуры и содержания плана управления безопасностью.

5 Классификация и контроль ресурсов

5.1 Ответственность за ресурсы

Цель: Обеспечить необходимую защиту ресурсов организации.

Все основные информационные ресурсы должны находиться в чьем-либо ведении. Для каждого такого ресурса следует назначить владельца. Ответственность за ресурсы помогает обеспечить необходимую защиту. Для каждого из основных ресурсов следует назначить владельца и определить круг обязанностей по поддержке необходимых средств защиты. Обязанности по реализации средств защиты могут передаваться другим сотрудникам. Тем не менее, нести ответственность должен назначенный владелец ресурса.

5.1.1 Перечень ресурсов

Перечни ресурсов помогают поддерживать эффективную защиту ресурсов. Кроме того, они могут пригодиться и для других целей – например, для проверки техники безопасности, страхования и финансового контроля (управления ресурсами). Создание перечня ресурсов является важной частью процесса управления рисками. Организация должна иметь возможность получить информацию о своих ресурсах и об их относительной ценности и важности. Благодаря этой информации можно будет реализовать защиту, степень которой будет соразмерна ценности и важности ресурсов. Необходимо создать и поддерживать перечень важных ресурсов, связанных с каждой информационной системой. Следует четко описать каждый ресурс, согласовать и обозначить его владельца и категорию конфиденциальности (см. раздел 5.2), а также указать его текущее местоположение (эта информация потребуется при восстановлении в случае утраты или повреждения). Вот некоторые примеры ресурсов, связанных с информационными системами:

a) информационные ресурсы: базы данных и файлы данных, системная документация, руководства пользователей, учебные материалы, инструкции по эксплуатации и обслуживанию, планы действий по устранению неисправностей, планы обеспечения непрерывности бизнеса, архивированная информация;

b) программные ресурсы: прикладное программное обеспечение, системное программное обеспечение, средства разработки и утилиты;

c) физические ресурсы: компьютерное оборудование (системные блоки, мониторы, переносные компьютеры, модемы), коммуникационное оборудование (маршрутизаторы, офисные АТС, факсимильные аппараты, автоответчики), магнитные носители (ленты и диски), другое оборудование (источники питания, кондиционеры), мебель, помещения;

d) сервисы: компьютерные и коммуникационные службы, коммунальные услуги, например, отопление, освещение, электроэнергия, кондиционирование воздуха.

5.2 Классификация информации по уровню конфиденциальности

Цель: Обеспечить необходимый уровень защиты информационных ресурсов.

Классификация (категорирование) информации производится с целью определения необходимости, приоритетов и степени ее защиты. Уровень конфиденциальности может различаться. Некоторые виды информации могут требовать дополнительной защиты или особого обращения. Следует реализовать систему классификации информации, которая

поможет создать необходимый перечень уровней защиты и пояснить пользователям потребность в особом обращении.

5.2.1 Принципы классификации

При классификации и введении соответствующих мер защиты информации необходимо учитывать потребности организации в совместном использовании и ограничении доступа к информации, а также возможный ущерб, связанный с этими потребностями, например, в результате несанкционированного доступа или повреждения информации. Как правило, классификация информации помогает быстро установить, как следует обращаться с определенной информацией и какие меры защиты необходимо к ней применять.

Информацию и результаты работы систем, работающих с конфиденциальными данными, необходимо маркировать (указывать гриф) согласно ценности и важности для организации. Кроме того, маркирование информации может потребоваться и для того, чтобы определить ее важность для организации; например, можно категорировать информацию в терминах ее целостности и доступности. Зачастую информация теряет конфиденциальность или критичность по истечении определенного периода времени – например, после ее открытой публикации. Эти аспекты следует учитывать, поскольку присвоение слишком высоких уровней конфиденциальности может стать причиной неоправданных дополнительных расходов. Принципы классификации должны отражать тот факт, что категория любой единицы информации не обязательно будет фиксированной в течение всего времени и может изменяться согласно некоторой заранее определенной политике (см. раздел 9.1).

Необходимо определить требуемое количество категорий классификации и преимущества от их использования. Слишком высокая сложность схем может привести к тому, что классификация станет неудобной и неэкономичной или окажется неприменимой на практике. Будьте внимательны при интерпретации классификационных меток на документах, поступающих из других организаций, поскольку в них категории с теми же названиями могут иметь другое значение.

Ответственность за определение категории информации (например, документа, записи базы данных, файла или дискеты) и за периодическую проверку этой категории должна лежать на создателе или назначенном владельце этой информации.

5.2.2. Маркирование информации и обращение с маркированой информацией

Необходимо создать свод инструкций по маркированию информации и обращению с ней в соответствии с принятой в организации схемой классификации. Эти инструкции должны охватывать работу с информационными ресурсами в физическом и электронном виде. Для каждой категории необходимо разработать инструкции, относящиеся к следующим операциям с информацией:

a) копирование;

b) хранение;

c) передача по почте, факсу и электронной почте;

d) передача в устной форме, включая разговоры по мобильному телефону, голосовую почту и автоответчики;

e) уничтожение.

Результаты работы систем, содержащих информацию, которая считается конфиденциальной или критичной, должны включать соответствующую пометку (гриф). Пометка должна отражать категорию информации, определенную согласно правилам, которые изложены в

разделе 5.2.1. Сюда относятся печатные отчеты, результаты вывода на экран, носители с записью (ленты, дискеты, компакт-диски, кассеты), электронные сообщения и передаваемые файлы.

Как правило, наиболее удобными оказываются физические пометки. Однако некоторые информационные ресурсы, например, документы в электронной форме, нельзя снабдить физической пометкой, поэтому при работе с ними следует использовать электронные средства маркирования.

6 Вопросы безопасности, связанные с персоналом

6.1 Безопасность при формулировке заданий и наборе сотрудников

Цель: Снизить риск ошибок людей, кражи, мошенничества и неправомерного использования технических средств.

Обязанности, связанные с безопасностью, следует оговаривать на этапе приема на работу и включать в контракты. Во время работы сотрудников необходимо следить за выполнением этих обязанностей.

При приеме на работу необходимо внимательно отбирать кандидатов (см. раздел 6.1.2), особенно если речь идет о ключевых должностях. Все сотрудники и сторонние пользователи средств обработки информации должны подписать соглашение о конфиденциальности (неразглашении).

6.1.1 Включение безопасности в круг должностных обязанностей

Права и обязанности в отношении информационной безопасности, описанные в соответствии с политикой информационной безопасности организации (см. раздел 3.1), должны быть внесены в должностные обязанности. Сюда должны входить сведения об общих обязанностях по реализации и поддержке политики безопасности, а также о конкретных обязанностях по защите отдельных ресурсов и по выполнению конкретных операций, связанных с безопасностью.

6.1.2 Отбор персонала и политика приема на работу

При приеме на постоянную работу необходимо проводить проверку кандидатов. Эта проверка должна включать следующее:

a) наличие у кандидата удовлетворительных рекомендаций, например, одной деловой и одной личной;

b) проверка резюме кандидата (на предмет полноты и точности);

c) подтверждение наличия заявленного академического и профессионального образования;

d) независимая проверка личности (с помощью паспорта или заменяющего его документа).

Если работа (при начальном приеме или при продвижении по службе) предполагает доступ сотрудника к средствам обработки информации, в частности, к тем, которые обрабатывают

конфиденциальную информацию, например, финансовую информацию или сведения с высокой степенью конфиденциальности, необходимо проверить также и кредитную историю сотрудника. Для сотрудников, работающих на руководящих должностях, такую проверку необходимо периодически повторять.

Подобную процедуру отбора следует проводить для подрядчиков и временных работников. Если поиск таких работников осуществляется агентством по трудоустройству, в контракте с агентством должны быть четко сформулированы обязанности агентства по проверке кандидатов и процедуры уведомления, которые должны быть выполнены в том случае, если проверка не была проведена или если ее результаты подают почву для сомнений.

Руководство должно утвердить методы контроля новых и неопытных сотрудников, имеющих право доступа к конфиденциальным системам. Работа всего персонала должна периодически подвергаться оценке и одобрению руководством соответствующих отделений.

Руководители должны понимать, что на работу сотрудника могут влиять обстоятельства его личной жизни. Проблемы личного и финансового характера, изменения в поведении и стиле жизни, частые отлучки и признаки стресса или депрессии могут вести к мошенничеству, кражам, ошибкам и другим случаям нарушения безопасности. Данную информацию следует использовать согласно законодательству, действующему в соответствующей юрисдикции.

6.1.3 Соглашения о конфиденциальности

Соглашения о конфиденциальности (или о неразглашении конфиденциальной информации) служат для уведомления о том, что информация является конфиденциальной или секретной. Как правило, сотрудники подписывают подобное соглашение в составе исходного контракта при приеме на работу.

Временные работники и сторонние пользователи, на которых не распространяются существующие контракты (содержащие соглашение о конфиденциальности), должны подписать соглашение о конфиденциальности перед тем, как они получат доступ к средствам обработки информации.

Соглашения о конфиденциальности следует просматривать заново при изменении условий контракта или найма, в частности, когда сотрудник собирается увольняться или когда срок действия контракта заканчивается.

6.1.4 Договор о приеме на работу

Договор о приеме на работу должен включать в себя сведения об ответственности сотрудника в области информационной безопасности. При необходимости эта ответственность должна распространяться и на определенный период по окончании срока работы. В договоре должны быть описаны меры, которые будут приняты в случае несоблюдения сотрудником требований к безопасности.

Необходимо установить и включить в договор о приеме на работу права и обязанности сотрудника, определяемые законодательством (например, законами об авторском праве и защите информации). Кроме того, необходимо включить сведения об обязанностях в отношении классификации данных работодателя и работе с ними. При необходимости в договоре о приеме на работу должно быть указано, что обязанности должны выполняться не только на территории организации и не только в обычные рабочие часы, например, в случае надомной работы (см. также разделы 7.2.5 и 9.8.1).

6.2 Обучение пользователей

Цель: Гарантировать, что пользователи сведущи в вопросах информационной безопасности и имеют необходимые навыки для поддержки политики безопасности организации в ходе обычной работы.

Пользователи должны быть обучены процедурам, связанным с безопасностью, и правильным методам работы со средствами обработки информации – это уменьшит вероятность нарушения безопасности.

6.2.1 Обучение и подготовка в области информационной безопасности

Все сотрудники организации (а при необходимости и сторонние пользователи) должны пройти соответствующую подготовку в области политики и процедур, принятых в организации. Периодически следует проводить переподготовку пользователей. Курс подготовки должен содержать сведения о требованиях к безопасности, ответственности перед законом и принятых в организации методах работы, а также инструкции по правильному использованию средств обработки информации, например, о процедуре входа в систему и работе с программным обеспечением. Такой курс необходимо проводить перед тем, как сотрудникам будет предоставлен доступ к информации или сервисам.

6.3 Реакция на инциденты и сбои в работе

Цель: Уменьшение ущерба от инцидентов и сбоев в работе; отслеживание подобных инцидентов и получение опыта на их основе.

Информацию об инцидентах, связанных с нарушением безопасности, следует максимально быстро распространять среди руководства по соответствующим каналам.

Все сотрудники и подрядчики должны быть знакомы с процедурами уведомления о различных типах инцидентов (уязвимостях, атаках и сбоях), которые могут повлиять на безопасность ресурсов организации. В их обязанности должна входить максимально быстрая передача информации о выявленных или подозреваемых инцидентах соответствующим лицам. В организации необходимо принять систему дисциплинарных взысканий, применяемых к лицам, по вине которых произошло нарушение безопасности. Для принятия необходимых мер может потребоваться как можно скорее собрать улики сразу же после инцидента (см. раздел 12.1.7).

6.3.1 Уведомление об инцидентах

Информацию об инцидентах следует максимально быстро распространять среди руководства по соответствующим каналам.

Необходимо утвердить формальную процедуру уведомления, а также процедуру реакции на инциденты, включающую в себя действия, которые должны выполняться при поступлении сообщения об инциденте. Все сотрудники и подрядчики должны быть знакомы с процедурой уведомления об инцидентах, а в их обязанности должна входить максимально быстрая передача информации о таких инцидентах. Необходимо также реализовать процесс обратной связи, позволяющий сотрудникам, сообщившим об инциденте, узнать о результатах после принятия соответствующих мер. Описание возникших инцидентов можно включить в программу подготовки пользователей (см. раздел 6.2), чтобы проиллюстрировать, что может произойти, как нужно реагировать на подобные инциденты и как избежать их в будущем (см. также раздел 12.1.7).

6.3.2 Уведомление недостатках в системе безопасности

Обязанности пользователей информационных сервисов должны включать уведомление о выявленных или подозреваемых уязвимостях или угрозах для систем и сервисов. Пользователи должны максимально быстро сообщать об этом либо своему руководителю, либо непосредственно поставщику услуг. Пользователям следует сообщить, что они ни при каких условиях не должны пытаться убедиться в наличии подозреваемой уязвимости. Это поможет им самим доказать свою непричастность, поскольку проверка на наличие уязвимости может быть принята за попытку неправомерного использования системы.

6.3.3 Уведомление о сбоях в программном обеспечении

Необходимо принять процедуру уведомления о сбоях в программном обеспечении. В процедуру рекомендуется включить следующие действия:

a) необходимо дать описание симптомов проблемы и записать сообщения, появляющиеся на экране.

b) необходимо изолировать компьютер, если это возможно, и прекратить работу с ним. Следует немедленно поставить в известность соответствующего сотрудника. При выполнении осмотра компьютера перед включением питания его следует отсоединить от сетей организации. Дискеты нельзя переносить на другие компьютеры.

c) о случившемся следует немедленно сообщить начальнику отдела информационной безопасности.

Пользователи не должны пытаться удалить вызывающую подозрение программу, не получив на это соответствующих санкций. Восстановление должно проводиться специалистами, имеющими соответствующую подготовку.

6.3.4 Изучение инцидентов

Необходимо создать механизмы, позволяющие оценивать и мониторить тип инцидентов или сбоев, их масштаб и связанные с ними затраты. Это может помочь в определении регулярно возникающих или серьезных инцидентов и сбоев. Полученная информация может указывать на необходимость ввести новые средства управления безопасностью или усовершенствовать существующие, чтобы сократить частоту, масштаб и ущерб от возникновения подобных инцидентов в будущем. Кроме того, эту информацию следует учитывать при анализе и обновлении политики безопасности (см. раздел 3.1.2).

6.3.5 Дисциплинарные взыскания

Необходимо формально утвердить дисциплинарные взыскания для сотрудников, нарушивших процедуры и политику безопасности, принятую в организации (см. раздел 6.1.4; сохранение улик описано в разделе 12.1.7). Подобные взыскания могут оказать сдерживающий эффект на сотрудников, которые в ином случае могли бы пренебречь процедурами, связанными с безопасностью. Кроме того, наличие утвержденных взысканий поможет гарантировать справедливое обращение с сотрудниками, подозреваемыми в серьезном или неоднократном нарушении безопасности.

7 Физическая безопасность и защита территорий

7.1 Защищенные территории

Цель: Предотвратить несанкционированный доступ к территории организации и принадлежащей ей информации, ее повреждение и вмешательство в работу.

Средства обработки критичной или конфиденциальной информации должны находиться на территории, защищенной созданным периметром безопасности с соответствующими преградами и ограничением доступа. Такие средства должны быть физически защищены от несанкционированного доступа, повреждения и вмешательства в работу.

Степень защиты должна быть соизмерима с выявленными рисками. Рекомендуется ввести правило убирать неиспользуемые документы с рабочих столов и экранов компьютеров (правила «чистого стола» и «чистого экрана»), чтобы снизить вероятность несанкционированного доступа и повреждения бумажных документов, носителей и средств обработки информации.

7.1.1 Физический периметр безопасности

Чтобы обеспечить физическую защиту, можно создать несколько физических барьеров вокруг территории организации и средств обработки информации. Каждый барьер является частью периметра безопасности и повышает общий уровень защиты. Периметры безопасности должны использоваться в организациях для защиты территорий, на которых находятся средства обработки информации (см. раздел 7.1.3). Периметр безопасности - это нечто, создающее барьер для прохода людей. В состав такого периметра могут входить стены, автоматизированные проходные и контрольно-пропускные пункты. Расположение и степень защиты каждого такого барьера должны зависеть от результатов оценки рисков.

При создании периметра рекомендуется соблюдать следующие правила:

a) Периметр безопасности должен быть четко определен.

b) Периметр здания или территории, где находятся средства обработки информации, должен быть физически прочным (т. е. в периметре не должно быть промежутков или участков, через которые легко прорваться). Внешние стены зданий должны быть монолитными, а все внешние двери должны иметь соответствующую защиту от несанкционированного доступа (контрольные механизмы, замки, засовы, сигнализацию и т. п.).

c) Необходимо создать контрольно-пропускной пункт или другое средство ограничения физического доступа на территорию или в здание. Доступ на территорию и в здание должен предоставляться только тем сотрудникам, которые имеют необходимое разрешение.

d) Физические барьеры при необходимости должны простираться от реального пола до реального потолка, чтобы предотвратить незаконное проникновение, а также загрязнение (например, в случае пожаров и наводнений).

e) Все пожарные выходы в периметре безопасности должны быть снабжены сигнализацией и плотно закрываться.

7.1.2 Управление физическим доступом

Вход на защищенную территорию должен быть должным образом ограничен, чтобы предоставлять доступ только авторизованным сотрудникам. Рекомендуется рассмотреть следующие меры:

a) Посетители защищенных территорий должны получать специальное разрешение на вход и выход с территории и находиться на них с сопровождением. Необходимо записывать дату и время их входа и выхода. Посетители должны получать доступ только для выполнения определенной санкционированной задачи. Посетители должны быть проинструктированы по поводу требований безопасности на данной территории и о действиях при возникновении чрезвычайной ситуации.

b) Доступ к конфиденциальной информации и средствам обработки такой информации должен контролироваться и предоставляться только сотрудникам, имеющим соответствующее разрешение. Для авторизации и подтверждения доступа должны использоваться средства аутентификации, например, смарт-карты с идентификационным кодом. Необходимо вести защищенные аудиторские записи обо всех сеансах доступа.

c) Все сотрудники должны обязательно носить какие-либо видимые идентификационные знаки и обращать внимание на незнакомых лиц без сопровождения и людей, у которых отсутствует идентификационный знак.

d) Необходимо регулярно проверять и обновлять права доступа к защищенным территориям.

7.1.3 Защита зданий, помещений и оборудования

Защищенной территорией может быть закрытое здание или несколько комнат внутри физического периметра безопасности. Комнаты могут запираться; в них могут находиться оборудованные замками шкафы и сейфы. При выборе и подготовке защищенной территории следует учитывать возможность повреждения в связи с пожаром, наводнением, взрывами, гражданскими беспорядками и другими бедствиями. Необходимо следить за соблюдением соответствующих норм и стандартов здравоохранения и техники безопасности. Кроме того, следует принять во внимание возможные угрозы, связанные с соседними территориями, например, утечку воды из прилегающих помещений.

Рекомендуется рассмотреть следующие меры:

a) Основные средства должны располагаться в местах с ограниченным доступом.

b) Строения должны быть неприметными и не иметь явных признаков своего назначения. На строениях и внутри них не должно быть знаков, указывающих на деятельность, связанную с обработкой информации.

c) Дополнительные средства и устройства, например, копировальные и факсимильные аппараты, должны располагаться в соответствующих местах защищенной территории, чтобы у посторонних не возникало желания воспользоваться ими, поскольку это может нарушить безопасность информации.

d) Двери и окна при отсутствии людей необходимо закрывать на замок. Следует подумать о внешней защите для окон (в частности, для расположенных на первом этаже).

e) Необходимо установить и регулярно тестировать сигнализацию, соответствующую профессиональным стандартам. Сигнализацией должны быть снабжены все внешние двери и доступные окна. В неиспользуемых помещениях сигнализация должна быть включена постоянно. Кроме того, необходимо обеспечить защиту других помещений,

в частности, тех, где находится компьютерное и коммуникационное оборудование.

f) Средства обработки информации, управляемые организацией, должны быть физически отделены от средств, управляемых другими организациями.

g) Доступ к телефонным справочникам и спискам телефонов с указанием местоположения средств обработки конфиденциальной информации должен быть ограничен.

h) Опасные и горючие вещества должны храниться с соблюдением мер предосторожности на безопасном расстоянии от защищенной территории. Расходные материалы (например, канцелярские принадлежности) не должны храниться на защищенной территории без необходимости.

i) Запасное оборудование и резервные носители должны находиться на безопасном расстоянии, чтобы избежать их повреждения при возникновении чрезвычайных ситуаций на основной территории.

7.1.4 Работа на защищенных территориях

Для повышения безопасности защищенной территории могут потребоваться дополнительные меры и средства. Сюда входят меры, связанные с персоналом или посторонними лицами, работающими на защищенной территории, а также с происходящей там деятельностью других организаций. Рекомендуется рассмотреть следующие меры:

a) О наличии защищенных территорий и происходящей там деятельности должны знать только те сотрудники, которым этой действительно необходимо.

b) Работа на защищенных территориях должна происходить под наблюдением, чтобы поддержать безопасность труда и предотвратить возможности для злонамеренных действий.

c) Незанятые защищенные территории необходимо физически закрыть и периодически проверять.

d) Посторонним работникам вспомогательных служб должен предоставляться ограниченный доступ к защищенным территориям или средствам обработки конфиденциальной информации только в случае необходимости. Этот доступ должен быть санкционирован и проходить под наблюдением. Внутри периметра безопасности могут быть установлены дополнительные барьеры и периметры для контроля физического доступа к областям с различными требованиями к безопасности.

e) Фотосъемка, видео- и аудиозапись и применение других средств записи может производиться только при наличии соответствующего разрешения.

7.1.5 Изолированные площадки для погрузоразгрузочных работ

Площадки для погрузоразгрузочных работ должны находиться под контролем и по возможности должны быть отделены от средств обработки информации, чтобы избежать доступа посторонних. Требования к безопасности для таких областей необходимо определить путем оценки рисков. Рекомендуется рассмотреть следующие меры:

a) Доступ к складским помещениям снаружи здания должны иметь только определенные сотрудники, имеющие необходимое разрешение.

b) Складские помещения должны быть такими, чтобы грузчики могли разгружать доставленный груз, не получая доступа к другим частям здания.

c) Внешние двери складских помещений должны запираться при открывании внутренней

двери.

d) Перед транспортировкой поступившего груза из складских помещений в места использования его необходимо осмотреть на предмет потенциальной опасности (см. раздел 7.2.1.г).

e) В случае необходимости груз следует регистрировать (см. раздел 5.1). в момент поступления на территорию организации

7.2 Безопасность оборудования

Цель: Предотвратить утрату, повреждение или компрометацию ресурсов и вмешательство в деятельность организации.

Оборудование должно быть физически защищено от угроз, связанных с нарушением безопасности и стихийными бедствиями. Необходимо ввести защиту оборудования (в том числе и того, которое используется за пределами территории организации), чтобы снизить риск несанкционированного доступа к данным и обеспечить защиту от утраты и повреждения. Следует также рассмотреть вопросы размещения и утилизации оборудования. Для защиты от опасностей и доступа посторонних и для охраны вспомогательных средств (например, систем электропитания и кабелей) могут потребоваться дополнительные меры.

7.2.1 Установка и защита оборудования

При установке и защите оборудования необходимо снизить риск, связанный со стихийными бедствиями, и сократить вероятность доступа посторонних. Рекомендуется рассмотреть следующие меры:

a) Оборудование должно быть размещено так, чтобы максимально ограничить необязательный доступ к рабочим областям.

b) Средства обработки и хранения информации, содержащие конфиденциальные данные, должны быть расположены так, чтобы уменьшить возможность подглядывания.

c) Объекты, требующие особой защиты, следует изолировать, чтобы получить возможность снизить общий уровень необходимой защиты.

d) Необходимо принять меры для минимизации риска возникновения различных потенциальных угроз, включая следующие:

   1) кража;

   2) пожар;

   3) взрывы;

   4) задымление;

   5) утечка воды (или прекращение подачи);

   6) пыль;

   7) вибрация;

   8) воздействие химических веществ;

   9) помехи в сети электропитания;

   10) электромагнитное излучение.

e) Политика организации должна включать правила, касающиеся употребления пищи и напитков и курения рядом со средствами обработки информации.

f) Необходимо следить за условиями окружающей среды и отслеживать факторы, которые могут негативно повлиять на работу средств обработки информации.

g) Для оборудования, эксплуатируемого в производственной обстановке, могут потребоваться специальные средства защиты, например, защитные оболочки для клавиатур.

h) Необходимо рассмотреть возможные последствия бедствий, которые могут произойти на ближайших территориях – например, пожаров в соседних зданиях, утечки воды с крыши или в подвальных помещениях и взрывов на улице.

7.2.2 Источники питания

Оборудование должно иметь защиту от отключения электропитания и других проблем с электричеством. Необходимо обеспечить подходящий источник питания, соответствующий требованиям производителя оборудования.

Вот несколько вариантов, которые помогут обеспечить постоянное электропитание:

a) использование нескольких источников питания;

b) источники бесперебойного питания (ИБП);

c) резервный генератор.

Оборудование, используемое для выполнения критических операций, рекомендуется подключить к ИБП, чтобы получить возможность продолжить или правильно завершить работу при отключении сети питания. Планы действия в нештатных ситуациях должны включать сведения о мерах, которые следует принять при отказе ИБП. Необходимо регулярно проверять емкость источников бесперебойного питания и проводить тесты в соответствии с рекомендациями производителя.

Резервный генератор может потребоваться в том случае, если обработку необходимо продолжать даже при длительном отсутствии электропитания. Установленные генераторы необходимо регулярно тестировать в соответствии с рекомендациями производителя. Следует создать запас топлива, который обеспечит работу генератора в течение длительного срока.

Кроме того, рядом с запасными выходами из помещений с оборудованием должны располагаться аварийные выключатели питания, с помощью которых можно будет быстро отключить питание в чрезвычайной ситуации. На случай отказа основного электропитания следует создать систему аварийного освещения. Необходимо оборудовать все здания защитой от грозовых разрядов и установить средства защиты от грозовых разрядов на все внешние линии связи.

7.2.3 Защита кабельной системы

Кабели питания и связи, используемые для передачи данных или поддержки информационных сервисов, должны быть защищены от перехвата данных и повреждения. Рекомендуется рассмотреть следующие меры:

a) Линии питания и передачи данных, к которым подключены средства обработки информации, по возможности должны находиться под землей или быть снабжены другими подходящими средствами защиты.

b) Кабели сетей передачи данных должны быть защищены от несанкционированного перехвата данных и повреждения. К примеру, такие кабели должны прокладываться в кабельных каналах и не должны проходить через общедоступные области.

c) Кабели питания следует прокладывать отдельно от кабелей связи, чтобы

предотвратить возникновение помех.

d) Для критичных или конйиденциальных систем могут также применяться следующие меры:

   1) установка армированных кабелей и снабженных замками щитков и шкафов в местах осмотра и конечных пунктах;

   2) использование альтернативных маршрутов прокладки или средств передачи данных;

   3) использование волоконно-оптических кабелей;

   4) поиск несанкционированного подключения дополнительных устройств к кабелям.

7.2.4 Профилактическое обслуживание оборудования

Необходимо правильно выполнять все процедуры профилактического обслуживания оборудования, чтобы гарантировать его доступность и целостность в течение длительного срока. Рекомендуется рассмотреть следующие меры:

a) Профилактическое обслуживание оборудования должно проводиться в соответствии с рекомендациями производителя с установленными интервалами.

b) Ремонт и обслуживание оборудования должны проводиться только авторизованными специалистами по обслуживанию.

c) Необходимо вести записи обо всех случившихся или подозреваемых сбоях и всех мерах по их профилактике и устранению.

d) При транспортировке оборудования за пределы организации для обслуживания необходимо принимать соответствующие меры (см. также сведения об удалении, стирании и перезаписи данных в разделе 7.2.6). Необходимо соблюдать все условия, перечисленные в страховых договорах.

7.2.5 Безопасность оборудования за пределами организации

Использование любого оборудования за пределами организации для обработки информации должно быть санкционировано руководством вне зависимости от того, кому принадлежит это оборудование. Уровень защиты должен быть эквивалентен защите находящегося на территории организации оборудования, используемого в тех же целях; при этом необходимо принимать во внимание риски, связанные с работой за пределами территории организации. К средствам обработки информации относятся все виды персональных компьютеров, органайзеры, мобильные телефоны, а также бумажная документация и другие носители, которые сотрудники забирают на дом или увозят с обычного места работы. Рекомендуется рассмотреть следующие меры:

a) Оборудование и носители, вывезенные за территорию организации, не должны оставаться без присмотра в общественных местах. Портативные компьютеры следует носить в качестве ручной клади и по возможности скрывать их наличие во время поездок.

b) Необходимо постоянно соблюдать все инструкции производителя по защите оборудования, например, по защите от воздействия мощных электромагнитных полей.

c) Необходимо определить (при оценке рисков) и ввести в действие соответствующие меры предосторожности для работы на дому, например, оборудованные замками шкафы, правила очистки стола от лишней документации и средства контроля доступа

для компьютеров.

d) Для защиты оборудования, находящегося за пределами организации, необходимо создать соответствующее страховое обеспечение.

Уровень риска (например, риск повреждения, кражи и подслушивания) в разных местах может сильно различаться. Это следует учитывать при определении необходимых мер защиты. Дополнительную информацию о других аспектах защиты мобильного оборудования можно найти в разделе 9.8.1.

7.2.6 Безопасная утилизация и повторное использование оборудования

Неаккуратная утилизация и повторное использование оборудования может стать причиной утечки информации (см. также раздел 8.6.4). Устройства хранения, содержащие конфиденциальную информацию, должны быть физически уничтожены или тщательно перезаписаны. Ограничиваться только стандартными функциями удаления нельзя.

Перед утилизацией каких-либо компонентов, включающих в себя носители информации (например, несъемных жестких дисков), следует убедиться, что находившиеся на них конфиденциальные данные и лицензионные программы были удалены или перезаписаны. Если какое-то устройство хранения, содержащее конфиденциальные данные, получит повреждения, необходимо провести оценку рисков и определить, что следует сделать с этим устройством – уничтожить, восстановить или вывести из использования.

7.3 Общие меры

Цель: Предотвратить компрометацию и кражу информации и средств обработки информации.

Информацию и средства ее обработки необходимо защитить от раскрытия, модификации и кражи посторонними. Следует принять меры, которые помогут свести ущерб к минимуму. Процедуры, связанные с обработкой и хранением информации, обсуждаются в разделе 8.6.3.

7.3.1 Удаление лишних документов со столов и экранов

В организации рекомендуется ввести правило, запрещающее держать лишние документы и носители информации на столах и лишние документы на экранах средств обработки информации, чтобы уменьшить риск несанкционированного доступа, потери и повреждения информации в рабочие часы и в нерабочее время. При этом необходимо учитывать классификацию информации (см. раздел 5.2), соответствующие риски и культурные нормы организации.

Помимо прочего, документы, оставшиеся на столах, вероятнее всего пострадают при пожаре, наводнении или взрыве.

Рекомендуется рассмотреть следующие меры:

a) Не используемые в данный момент документы и компьютерные носители по возможности должны храниться в запертых шкафах и/или других надежных контейнерах, особенно в нерабочее время.

b) конфиденциальную или критичную информацию, не используемую в данный момент, следует запирать (в идеале – в огнеупорном сейфе), в особенности при уходе из помещения.

c) Персональные компьютеры, компьютерные терминалы и принтеры, оставляемые без присмотра, не должны оставаться зарегистрированными в сети. Такие устройства должны быть защищены с помощью замков, паролей и других средств.

d) Необходимо обеспечить защиту пунктов приема и передачи почты и оставляемых без присмотра факсимильных аппаратов и телексов.

e) В нерабочие часы копировальные аппараты следует закрывать на замок или защищать от несанкционированного использования другим способом.

f) Распечатки конфиденциальной информации следует сразу же забирать из принтера.

7.3.2 Вывоз имущества

Оборудование, информация и программное обеспечение не должны вывозиться за пределы организации без разрешения. В соответствующих случаях и при необходимости сотрудники должны завершать сеансы сетевой связи и возобновлять их при возвращении. Для определения несанкционированного вывоза имущества необходимо проводить выборочную проверку. Сотрудников следует предупредить о возможности выборочной проверки.

8 Обеспечение безопасности при эксплуатации

8.1 Правила работы и обязанности

Цель: Гарантировать правильность и безопасность эксплуатации средств обработки информации.

Необходимо определить правила и обязанности, связанные с использованием и управлением всех средств обработки информации. Сюда входит разработка необходимых инструкций по эксплуатации и реакции на инциденты.

В соответствующих случаях следует реализовать разделение обязанностей, чтобы уменьшить риск случайного или умышленного неправомерного использования системы (см. раздел 8.1.4.).

8.1.1 Документированные правила работы

Правила работы, определенные в политике безопасности, необходимо документировать и следить за их соблюдением. Правила работы должны считаться официальными документами, изменения в них должны вноситься с санкции руководства.

Описание правил должны содержать подробные инструкции по выполнению каждой задачи, включая:

a) обработку информации и обращение с ней;

b) требования к графику работы, включая взаимную зависимость от других систем; самое раннее время начала и самое позднее время окончания работы;

c) необходимые действия в случае ошибок и других чрезвычайных ситуаций, которые могут возникнуть во время работы, в том числе ограничения на использование системных утилит (см. раздел 9.5.5).

d) координаты сотрудников, к которым следует обращаться при возникновении непредвиденных затруднений в работе и проблем с оборудованием;

e) инструкции по особому обращению с результатами работы, например, по использованию специальных канцелярских принадлежностей и по обращению с конфиденциальными документами, включая инструкции по безопасной утилизации

результатов заданий, завершившихся неудачно;

f) инструкции по перезапуску и возобновлению работы системы в случае ее отказа.

Кроме того, необходимо разработать инструкции по сопутствующим процедурам, связанным с обработкой информации и передачей данных – например, по запуску и завершению работы компьютеров, резервному копированию, профилактическому обслуживанию оборудования, работе в компьютерных залах и обработке почты.

8.1.2 Контроль внесения изменений в эксплуатацию

Изменения в системах и средствах обработки информации необходимо контролировать. Недостаточный контроль вносимых изменений в работе систем и средств обработки информации является распространенной причиной сбоев в работе и нарушений безопасности. Необходимо официально ввести соответствующие обязанности и разработать инструкции, чтобы обеспечить достаточный контроль всех изменений в оборудовании, программном обеспечении и методах работы. Изменения в используемых программах должны строго контролироваться. При внесении изменений в программы необходимо сохранять аудиторские записи, включающие всю необходимую информацию. Изменения в среде эксплуатации могут повлиять на работу приложений. По возможности процедуры контроля изменений в условиях эксплуатации и прикладном программном обеспечении должны быть объединены (см. также раздел 10.5.1). В частности, рекомендуется рассмотреть следующие меры:

a) определение и регистрация значительных изменений;

b) оценка потенциального воздействия таких изменений;

c) формальная процедура утверждения предлагаемых изменений;

d) передача сведений об изменениях всем сотрудникам, которые должны быть поставлены в известность;

e) инструкции по распределению обязанностей, связанных с остановом и восстановлением работы после неудачных изменений.

8.1.3 Действия в случае инцидентов

Необходимо установить обязанности и правила действий (регламенты) в случае инцидентов, чтобы обеспечить быстрое, эффективное и организованное реагирование на инциденты, связанные с безопасностью (см. также раздел 6.3.1). Рекомендуется рассмотреть следующие меры:

a) Необходимо разработать регламенты для всех возможных типов инцидентов, включая:

   1) сбои в информационных системах и прекращение работы сервисов;

   2) отказ в обслуживании;

   3) ошибки, возникшие в результате поступления неполных или неточных данных;

   4) нарушения конфиденциальности.

b) В дополнение к обычным планам действия в нештатных ситуациях (предназначенным для максимально быстрого восстановления систем и сервисов), инструкции должны также освещать следующие вопросы (см. также раздел 6.3.4):

   1) анализ и определение причины инцидента;

   2) планирование и реализация средств, предотвращающих повторение инцидента (при необходимости);

3) сбор аудиторских записей и прочих улик;

4) обращение к сотрудникам, имеющим отношение к восстановлению после инцидента;

5) передача сведений о предпринятых действиях уполномоченным органам.

c) Необходимо собрать (см. раздел 12.1.7) и сохранить с соблюдением принципов безопасности аудиторские записи и прочие улики для следующих целей:

1) внутренний анализ проблемы;

2) использование в качестве доказательств при поиске потенциальных уязвимостей в условиях договора и нормативных требований, а также при административном и уголовном преследовании, например, в соответствии с законами о неправомерном использовании компьютеров и защите данных.

3) переговоры о компенсации со стороны поставщиков программного обеспечения и услуг.

d) Действия, связанные с устранением уязвимостей и восстановлением систем после сбоев, должны проходить под тщательным официальным контролем. Эти процедуры должны гарантировать, что:

1) только специально назначенные и уполномоченные сотрудники имеют доступ к работающим системам и данным (см. также информацию о доступе посторонних в разделе 4.2.2).

2) все действия, предпринимаемые в чрезвычайной ситуации, подробно документируются;

3) сведения о действиях в чрезвычайной ситуации передаются руководству и своевременно рассматриваются;

4) целостность систем и средств организации восстанавливается с минимальной задержкой.

8.1.4 Разделение полномочий

Разделение полномочий – это метод, позволяющий уменьшить риск случайного или намеренного неправомерного использования системы. Следует рассмотреть возможности разделения полномочий по управлению или выполнению определенных действий, либо областей ответственности, чтобы ограничить возможности для несанкционированного изменения или неправомерного использования информации или сервисов.

В небольших организациях реализовать этот метод может оказаться сложно, однако сам принцип рекомендуется применять при каждой возможности. Если разделить полномочия сложно, рекомендуется подумать о введении других мер, например, о мониторинге деятельности, аудиторских записях и наблюдении со стороны руководства. Аудит безопасности обязательно должен оставаться независимым.

Необходимо обеспечить, чтобы никто не смог совершить мошенничество в области своей ответственности, не будучи замеченным. Совершение действия должно быть отделено от получения разрешения на него. Рекомендуется рассмотреть следующие меры:

a) Необходимо разделить области деятельности, которые требуют сговора для совершения мошенничества, например, размещение заказа на приобретение и проверка получения товаров.

b) Если существует опасность сговора, меры защиты должны быть реализованы так,

чтобы участие в действиях должны были принимать несколько человек. Это поможет снизить вероятность тайных действий.

8.1.5 Разделение областей разработки и эксплуатации

Чтобы добиться разделения полномочий, важно отделить друг от друга области разработки, тестирования и эксплуатации. Необходимо разработать и задокументировать правила передачи программного обеспечения из разработки в эксплуатацию.

При разработке и тестировании могут возникать серьезные проблемы, например, нежелательное изменение файлов и системного окружения и сбои в работе системы. Необходимо рассмотреть вопрос о том, какой уровень разделения между средами эксплуатации, тестирования и разработки необходим для того, чтобы избежать проблем при эксплуатации. Подобным образом следует отделить друг от друга деятельность по разработке и тестированию. В данном случае для проведения осмысленного тестирования необходимо создать известную и стабильную среду, доступ к которой разработчики не смогут получить без особой необходимости.

Если специалисты, занятые разработкой и тестированием, имеют доступ к эксплуатируемой системе и хранящейся в ней информации, они могут иметь возможность ввести в систему неразрешенный и непротестированный код или изменить рабочие данные. В некоторых системах эта возможность может быть использована для мошенничества и для размещения непротестированного или злонамеренного кода. Непротестированный и злонамеренный код может вызвать серьезные проблемы в работе. Кроме того, специалисты, занятые разработкой и тестированием, представляют угрозу для конфиденциальности рабочей информации.

Действия, связанные с разработкой и тестированием, выполняемые в одной и той же компьютерной среде, могут привести к непредусмотренным изменениям информации и программного обеспечения. Таким образом, рекомендуется разделить области разработки, тестирования и эксплуатации, чтобы снизить риск случайного изменения или несанкционированного доступа к рабочему программному обеспечению и данным организации. Рекомендуется рассмотреть следующие меры:

a) По возможности средства разработки и программы, используемые в основной работе организации, должны работать на отдельных компьютерных процессорах или в разных доменах или каталогах.

b) Действия, связанные с разработкой и тестированием, должны быть как можно больше отделены друг от друга.

c) Компиляторы, редакторы и другие системные средства не должны быть доступны из рабочих систем без необходимости.

d) Для рабочих и тестовых систем необходимо использовать различные процедуры входа в систему, чтобы уменьшить вероятность ошибки. Пользователям рекомендуется выбирать для этих систем разных пароли. В меню должны выводиться соответствующие идентификационные сообщения.

e) Специалисты по разработке должны иметь доступ к паролям рабочей системы только при наличии средств выдачи паролей для поддержки рабочих систем. Эти средства должны обеспечивать смену подобных паролей после использования.

8.1.6 Внешнее управление средствами обработки информации

Наличие внешнего подрядчика, управляющего средствами обработки информации, приводит к возникновению потенциальных уязвимостей, таких как вероятность компрометации, повреждения или потери данных на территории подрядчика. Эти риски следует определить

заранее, чтобы согласовать введение необходимых мер с подрядчиком и оговорить это в контракте (рекомендации по заключению контрактов со сторонними организациями, предполагающих доступ к принадлежащим организации средствам обработки, и контрактов на аутсорсинг можно найти в разделах 4.2.2 и 4.3).

Вот некоторые вопросы, которым следует уделить внимание:

a) определение конфиденциальных или критичных операций, которые желательно проводить внутри организации;

b) получение одобрения от владельцев бизнес-приложений;

c) влияние на план поддержки непрерывности бизнеса;

d) стандарты безопасности, которым необходимо следовать, и процедура оценки их соблюдения;

e) определение конкретных обязанностей и правил, обеспечивающих эффективное наблюдение за всеми действиями, влияющими на безопасность;

f) определение обязанностей и правил уведомления при возникновении инцидентов и реакции на эти инциденты (см. раздел 8.1.3).

8.2 Планирование разработки и приемка системы

Цель: Свести к минимуму риск сбоев системы.

Чтобы обеспечить наличие необходимой мощности и ресурсов, требуется заблаговременное планирование и подготовка.

Необходимо сделать прогноз мощности системы, которая потребуется в будущем, чтобы уменьшить риск перегрузки системы. Требования к новой системе необходимо определить, задокументировать и проверить до их утверждения и начала использования.

8.2.1 Планирование мощности

Необходимо следить за требованиями к мощности системы и прогнозировать развитие этих требований в будущем, чтобы гарантировать наличие необходимой вычислительной мощности и объема устройств хранения. При прогнозах необходимо учитывать возникающие требования к системе, развитие деятельности организации, а также текущие и прогнозируемые тенденции в области обработки информации в организации.

Особого внимания при этом требуют компьютеры-мэйнфреймы, поскольку они имеют значительно большую стоимость и имеют более длительный технологический цикл введения новых функций. Руководители, ответственные за мэйнфреймы, должны следить за использованием основных системных ресурсов, включая процессоры, основные устройства хранения, устройства хранения файлов, принтеры и другие устройства вывода, а также средства связи. Они должны определять тенденции в использовании, в особенности по отношению к бизнес-приложениям и автоматизированным системам управления.

На основе этой информации руководители должны определять и предотвращать возможность возникновения узких мест, которая может угрожать безопасности системы или пользовательских сервисов, и планировать соответствующие корректирующие меры.

8.2.2 Приемка систем

Необходимо установить критерии приемки для новых информационных систем, обновлений и новых версий. Перед приемкой система должна проходить соответствующее тестирование. Руководство должно обеспечить четкое определение, согласование, документирование и

проверку требований и критериев приемки новых систем. Рекомендуется рассмотреть следующие меры:

a) проверка требований к производительности и мощности компьютеров;

b) процедуры перезапуска и восстановления после ошибок, а также планы действия в нештатных ситуациях;

c) подготовка и проверка соответствия типовых эксплуатационных процедур на соответствие определенным стандартам;

d) создание согласованного набора средств для обеспечения безопасности;

e) эффективные процедуры управления;

f) меры по обеспечению непрерывности бизнеса (согласно требованиям, изложенным в разделе 11.1).

g) подтверждения того, что установка новой системы не окажет негативного влияния на существующие системы, в частности, в периоды максимальной нагрузки, например, в конце месяца;

h) подтверждения того, что влияние новой системы на общую безопасность в организации было проанализировано;

i) обучение методам эксплуатации или использования новой системы.

В процессе разработки новых крупномасштабных систем необходимо постоянно проводить консультации с отделом эксплуатации и пользователями, чтобы гарантировать эффективную эксплуатацию системы. Необходимо выполнить соответствующие тесты, чтобы убедиться в полном соответствии всем критерием приемки.

8.3 Защита от злонамеренного программного обеспечения

Цель: Защитить целостность программного обеспечения и информации.

Необходимо принять меры для обнаружения и обезвреживания злонамеренных программ. При работе с программными комплексами и средствами обработки информации существует риск проникновения злонамеренных программ, например, компьютерных вирусов, сетевых червей, «троянских коней» (см. также раздел 10.5.4) и логических бомб. Пользователи должны знать об опасностях, связанных с несанкционированными и злонамеренными программами. Руководители должны по мере необходимости способствовать внедрению средств для обнаружения и обезвреживания таких программ. В частности, необходимо принять меры для обнаружения и обезвреживания компьютерных вирусов на персональных компьютерах.

8.3.1 Средства борьбы со злонамеренными программами

Необходимо разработать средства обнаружения и предотвращения занесения злонамеренных программ и распространить среди пользователей информацию о них. Защита от злонамеренных программ должна базироваться на знакомстве с требованиями безопасности, контроле доступа к системам и управлении внесением изменений. Рекомендуется рассмотреть следующие меры:

a) официальная политика, требующая соблюдения условий лицензий на программное обеспечение и запрещающая использовать несанкционированные программы (см. раздел 12.1.2.2).

b) официальная политика защиты от рисков, связанных с получением файлов и программ

либо из внешних сетей или через них, либо с помощью любых других средств передачи данных. Политика должна включать описание необходимых мер по защите (см. также раздел 10.5, в частности, подразделы 10.5.4 и 10.5.5);

c) установка и регулярное обновление антивирусных программ, сканирующих компьютеры и носители либо в профилактических целях, либо на регулярной основе

d) регулярный анализ программ и данных в системах, предназначенных для выполнения критических операций. При наличии неразрешенных файлов или несанкционированных изменений следует проводить официальное расследование;

e) проверка файлов на электронных носителях, полученных из неустановленного или неавторизованного источника, а также файлов, полученных через общедоступные сети, на предмет наличия вирусов перед использованием;

f) проверка файлов, полученных по электронной почте и загруженных через сеть, на предмет наличия злонамеренных программ перед использованием. Эта проверка может выполняться в различных пунктах, например, на серверах электронной почты, на настольных компьютерах или при поступлении в сеть организации;

g) правила и обязанности, относящиеся к защите систем от вирусов, обучению методам работы, отчетности и восстановлению после вирусных атак (см. разделы 6.3 и 8.1.3).

h) планы поддержки непрерывности бизнеса, связанные с вирусными атаками, в том числе инструкции по резервному копированию и восстановлению всех необходимых данных и программ (см. часть 11).

i) процедуры проверки всей информации, связанной со злонамеренными программами, и обеспечение точности и информативности всех предупреждающих сообщений. Руководство должно гарантировать, что различия между ложными и реальными вирусами проводятся на основе информации из компетентных источников, например, из распространенных журналов, с известных Интернет-сайтов или от поставщиков антивирусных программ. Сотрудники должны быть уведомлены о проблеме ложных вирусов и о необходимых действиях при их получении.

Эти меры особенно важны для сетевых файловых серверов, поддерживающих большое количество рабочих станций.

8.4 Служебные процедуры

Цель: Поддержка целостности и доступности средств обработки информации и услуг связи.

В соответствии с принятой стратегией резервного копирования (см. раздел 11.1) необходимо разработать типовые процедуры создания резервных копий данных и технологии их быстрого восстановления, ведения журналов событий и сбоев, а также (при необходимости) наблюдения за средой, в которой работает оборудование.

8.4.1 Резервное копирование информации

Следует регулярно создавать резервные копии принадлежащей организации важной информации и программного обеспечения. Имеющиеся средства резервного копирования должны обеспечивать возможность восстановления всей важной информации и программного обеспечения в случае бедствия или повреждения носителей. Необходимо регулярно проверять правила резервного копирования для отдельных систем на предмет соответствия требованиям планов по поддержке непрерывности бизнеса (см. часть 11). Рекомендуется рассмотреть следующие меры:

a) Резервные копии минимального количества необходимой информации вместе с

подробными и точными сведениями об этих резервных копиях и инструкциями по восстановлению должны храниться на достаточном расстоянии от основной территории, чтобы они не пострадали в случае произошедшего там бедствия. Для важных областей деятельности необходимо хранить информацию как минимум за три стадии (цикла) резервного копирования.

b) Необходимо обеспечить правильные условия хранения и соответствующий уровень физической защиты резервных копий согласно стандартам, действующим на основной территории (см. раздел 7). Меры защиты, применяемые к носителям на основной территории, должны действовать и на той территории, где хранятся резервные копии.

c) Исходя из соображений практичности, необходимо регулярно тестировать резервные носители, чтобы гарантировать, что на них можно будет положиться в аварийной ситуации.

d) Необходимо регулярно проверять процедуры восстановления, чтобы убедиться в их эффективности, а также в том, что их можно выполнить за время, отведенное в правилах на восстановление информации.

Следует определить период хранения важной информации организации, а также требования к архивным копиям, предполагающим постоянное хранение (см. раздел 12.1.3).

8.4.2 Журналы операторов

Сотрудники, отвечающие за эксплуатацию систем, должны вести журнал своих действий. Сообразно необходимости, журнал должен включать следующую информацию:

a) время запуска и завершения работы системы;

b) ошибки в работе системы и принятые меры по устранению;

c) подтверждение правильного обращения с файлами данных и результатами компьютерной обработки;

d) ФИО человека, сделавшего запись в журнале.

Журналы операторов должны регулярно проходить независимую проверку на предмет соответствия процедурам эксплуатации.

8.4.3 Регистрация сбоев

При возникновении сбоя следует уведомить о нем соответствующего сотрудника и принять меры по устранению. Все переданные пользователями сообщений о сбоях, связанных с проблемами в системах обработки информации и передачи данных, должны быть зарегистрированы в журнале. Следует установить четкие правила действий при получении уведомления о сбое, в том числе:

a) просмотр журнальных записей о сбоях и проверка удовлетворительности устранения последствий сбоя;

b) анализ мер по устранению, помогающий убедиться, что средства защиты не были нарушены, а на все выполненные действия были получены соответствующие санкции.

8.5 Управление вычислительными сетями

Цель: Обеспечить защиту информации в вычислительных сетях и безопасность сопутствующей инфраструктуры.

Управление безопасностью в сетях, выходящих за пределы организации, требует особого внимания.

Для защиты конфиденциальной информации, передаваемой по общественным сетям, могут потребоваться дополнительные средства.

8.5.1 Средства обеспечения безопасности сетей

Для обеспечения и поддержки безопасности в компьютерных сетях необходим определенный перечень средств. Сетевые администраторы должны внедрить средства, обеспечивающие безопасность данных в сетях и защиту сервисов доступа от несанкционированного использования. В частности, рекомендуется рассмотреть следующие меры:

a) Обязанности по эксплуатации сети при необходимости следует отделить от обязанностей, связанных с эксплуатацией компьютеров (см. раздел 8.1.4).

b) Необходимо определить обязанности и регламенты, связанные с управлением удаленным оборудованием, в том числе тем оборудованием, которое находится на пользовательской территории.

c) В случае необходимости следует ввести особые меры для сохранения конфиденциальности и целостности данных, передаваемых по общественным сетям, и для защиты взаимодействующих систем (см. разделы 9.4 и 10.3). Кроме того, могут потребоваться специальные меры для поддержки доступности сетевых сервисов и подключенных компьютеров.

d) Мероприятия по управлению сетью должны быть скоординированы, чтобы обеспечить как оптимальный уровень предоставляемого сервиса в организации, так и согласованное внедрение средств защиты во всей инфраструктуре обработки информации.

8.6 Обращение с носителями и их безопасность

Цель: Предотвратить повреждение ресурсов и нарушение деятельности организации. Носители должны контролироваться и физически защищаться.

Необходимо разработать правила по защите документов, компьютерных носителей (лент, дисков, кассет), вводимых и выводимых данных и системной документации от повреждения, кражи и неавторизованного доступа.

8.6.1 Обращение со съемными компьютерными носителями

Необходимо разработать правила обращения со съемными компьютерными носителями, например, лентами, дисками, кассетами и печатными отчетами. Рекомендуется рассмотреть следующие меры:

a) Предыдущее содержимое любых многоразовых носителей, которые больше не требуются организации, должно быть стерто, если необходимость в нем отпала.

b) На передачу носителей за пределы организации необходимо получать разрешение. Следует сохранять записи о передачу носителей; эти записи могут потребоваться при аудиторской проверке (см. раздел 8.7.2).

c) Все носители должны храниться в безопасных местах в соответствии с инструкциями производителя.

Все правила и уровни авторизации должны быть четко документированы.

8.6.2 Утилизация носителей

Носители, ставшие ненужными, следует утилизировать с соблюдением требований безопасности. При небрежной утилизации носителей конфиденциальная информация может попасть в руки посторонних. Чтобы уменьшить риск, необходимо разработать официальные правила безопасной утилизации носителей. Рекомендуется рассмотреть следующие меры:

a) Носители, содержащие конфиденциальную информацию, должны храниться и утилизироваться надежным способом (например, путем сжигания или измельчения) или очищаться от данных перед использованием внутри организации в других целях.

b) Ниже перечислен список предметов, при утилизации которых могут потребоваться особые предосторожности:

   1) бумажные документы;
   2) аудиозаписи;
   3) копировальная бумага;
   4) отчеты о результатах работы программ;
   5) одноразовые красящие ленты для принтеров;
   6) магнитные ленты;
   7) съемные диски или кассеты;
   8) оптические носители (все виды, включая дистрибутивные носители, полученные от производителей программного обеспечения);
   9) листинги программ;
   10) тестовые данные;
   11) системная документация.

c) В некоторых случаях допускается массовое уничтожение носителей разных типов без выделения носителей с важной информацией.

d) Многие организации предлагают услуги по сбору и утилизации бумаг, носителей и оборудования. Будьте внимательны при выборе подходящего подрядчика, имеющего опыт работы и использующего необходимые средства защиты.

e) Необходимо вести учет фактов уничтожения важных носителей для обеспечения возможности контроля процессов утилизации.

При сборе носителей для утилизации необходимо подумать об «эффекте накопления», в результате которого большое количество неконфиденциальной информации может повлиять на безопасность больше, чем небольшое количество конфиденциальной.

8.6.3 Правила обращения с информацией

Необходимо разработать правила хранения информации и обращения с ней, чтобы защитить информацию от несанкционированного раскрытия или неправомерного использования. В правилах должны быть изложены принципы обращения с информацией в соответствии с ее классификацией (см. раздел 5.2). Эти правила должны относиться к документам,

компьютерным системам, сетям, мобильным компьютерам и мобильным средствам связи, почте, голосовой почте, устному обмену информацией в целом, мультимедийным данным, почтовым услугам и средствам, использованию факсимильных аппаратов, а также к прочим важным предметам, например, к незаполненным чекам и ордерам. Рекомендуется подумать о следующих мерах (см. также разделы 5.2 и 8.7.2):

a) правильное обращение и маркирование всех носителей (см. также раздел 8.7.2a);

b) ограничения доступа, позволяющие обнаружить неавторизованных сотрудников;

c) официальное протоколирование сведений об авторизованных получателях информации;

d) проверка полноты исходных данных, корректности завершения обработки и правильности результатов;

e) защита буферизованных данных, ожидающих вывода, в соответствии с их уровнем конфиденциальности;

f) соблюдение условий хранения носителей, рекомендованных производителем;

g) распространение информации в минимальных масштабах;

h) четкая маркировка всех копий данных для авторизованных получателей;

i) регулярный пересмотр списков распространения и списков авторизованных получателей.

8.6.4 Безопасность системной документации

Системная документация может включать в себя конфиденциальную информацию, например, описание технических процессов, процедур, структур данных и процессов авторизации (см. также раздел 9.1). Рекомендуется рассмотреть следующие меры для защиты системной документации от несанкционированного доступа:

a) Системная документация должна храниться с соблюдением правил безопасности.

b) Круг лиц, получающих доступ к системной документации, должен быть минимальным. Для доступа должно требоваться разрешение владельца программы.

c) Системная документация, хранящаяся в общественной сети или передаваемая по такой сети, должна иметь необходимую защиту.

8.7 Обмен информацией и программным обеспечением

Цель: Предотвратить потери, модификацию и неправомерное использование информации, которой обмениваются организации.

Обмен информацией и программным обеспечением между организациями должен происходить под контролем и соответствовать всем необходимым законам (см. часть 12).

Обмен должен происходить на базе соглашений. Необходимо разработать правила и стандарты защиты передаваемой информации и носителей. При этом следует учитывать вопросы деятельности и безопасности, связанные с электронным обменом данными, электронной коммерцией, электронной почтой и необходимыми мерами защиты.

8.7.1 Соглашения по обмену информацией и программным обеспечением

Для обмена информацией и программным обеспечением между организациями (в физическом и электронном виде) необходимо разработать соглашения, часть которых может быть

официальными, в том числе соглашения о депонировании программного обеспечения в случае необходимости. Требования к безопасности, налагаемые этими соглашениями, должны отражать конфиденциальность затрагиваемой информации. Соглашения об условиях обеспечения безопасности должны включать в себя следующее:

a) обязанности по контролю передачи, отправки и приема, а также по уведомлению об этих операциях;

b) правила уведомления об отправителе, передаче, отправке и приеме;

c) минимальные технические требования к упаковке и передаче;

d) требования к идентификации курьеров;

e) обязанности и ответственность в случае потери данных;

f) использование согласованной системы пометок конфиденциальной и критичной информации, обеспечивающей точное понимание меток и соответствующую им защиту информации;

g) права владения информацией и программным обеспечением и обязанности по защите данных, соблюдению авторских прав и т. п. (см. разделы 12.1.2 и 12.1.4).

h) технические стандарты, относящиеся к записи и считыванию информации и программного обеспечения;

i) специальные средства, которые могут потребоваться для защиты конфиденциальных данных, например, ключи шифрования (см. 10.3.5).

8.7.2 Безопасность носителей при передаче

Во время физической передачи (например, при пересылке носителей по почте или с курьером) может возникнуть опасность несанкционированного доступа, неправомерного использования или повреждения информации. Для защиты компьютерных носителей, передаваемых между различными территориями, необходимы следующие меры:

a) Должен использоваться надежный транспорт или курьеры. Необходимо согласовать с руководством список уполномоченных курьеров и внедрить процедуру проверки личности курьеров.

b) Упаковка должна в достаточной мере защищать содержимое от физических повреждений, которые могут произойти при пересылке, и соответствовать требованиям производителя.

c) При необходимости следует ввести специальные меры для защиты конфиденциальной информации от несанкционированного раскрытия или модификации. Вот несколько примеров:

    1) использование закрытых контейнеров;

    2) личная доставка;

    3) упаковка, которую нельзя незаметно вскрыть (такая упаковка позволит заметить попытки получить доступ);

    4) в исключительных случаях рекомендуется разделять передаваемую информацию на несколько частей и передавать эти части разными путями;

    5) использование цифровых подписей и шифрования (см. раздел 10.3).

8.7.3 Безопасность электронной коммерции

В электронной коммерции могут использоваться средства электронного обмена данными, электронная почта и онлайновые транзакции через общественные сети, например, через Интернет. Электронная коммерция уязвима для различных опасностей, связанных с сетью, что может привести к мошеннической деятельности, спорам по контрактам и раскрытию или модификации информации. Необходимо ввести меры по защите средств электронной коммерции от этих опасностей. Для обеспечения безопасности электронной коммерции рекомендуется рассмотреть следующие меры:

a) Аутентификация. Какая степень доверия необходима продавцу и покупателю к заявленным каждым из них персональным данным?

b) Авторизация. Кто имеет право устанавливать цены и выдавать или подписывать основные торговые документы? Как узнает об этом торговый партнер?

c) Процессы заключения контрактов и тендеры. Каковы требования к конфиденциальности, целостности, подтверждению отправки и получения основных документов и неотказуемости от контрактов?

d) Сведения о ценах. Насколько можно доверять целостности рекламного прейскуранта и конфиденциальности соглашений о скидках?

e) Операции с заказами. Как обеспечивается конфиденциальность и целостность заказов, сведений о платежах и доставки и подтверждения приема?

f) Контрольная проверка. Проверку какого уровня должна проходить информация о платежах, переданная заказчиком?

g) Расчет. Какая форма платежей лучше всего подходит для защиты от мошенничества?

h) Заказ. Какая защита необходима для сохранения конфиденциальности и целостности информации заказов и для предотвращения потерь или дублирования транзакций?

i) Ответственность. На кого возлагается риск, связанный с мошенническими операциями?

Многие из перечисленных выше проблем могут решаться путем применения криптографических методов, упоминаемых в разделе 10.3. При этом следует учитывать соответствие требованиям законодательства (см. раздел 12.1; сведения о законах, касающихся криптографии, приводятся в разделе 12.1.6).

Электронные коммерческие соглашения между торговыми партнерами должны поддерживаться документированным соглашением, в котором обе стороны фиксируют условия торговых операций, в том числе сведения об авторизации (см. пункт «б» выше). Кроме того, могут потребоваться и другие соглашения с владельцами информационных служб и поставщиками дополнительных сетевых услуг.

Общедоступные торговые системы должны опубликовать условия ведения своей деятельности и предоставлять эту информацию заказчикам.

Следует проанализировать устойчивость к атакам хоста, используемого для электронной коммерции, а также уровень вопросы безопасности, возникающие при осуществлении сетевых подключений, необходимых для реализации этой деятельности (см. раздел 9.4.7).

8.7.4 Безопасность электронной почты

8.7.4.1 Риски

Электронная почта используется для обмена деловой информацией и постепенно заменяет собой традиционные формы связи, например, телекс и почтовые отправления. Электронная

почта отличается от традиционных форм связи, в частности, своей скоростью, структурой сообщения, степенью неформальности и уязвимостью к несанкционированным действиям. Следует рассмотреть необходимость введения мер, уменьшающих риски, которые возникают в связи с использованием электронной почты. Риски включают в себя:

a) уязвимость сообщений для несанкционированного доступа, модификации и атак типа «отказ в обслуживании»;

b) уязвимость к ошибкам (таким как неправильный ввод адреса или неправильная пересылка), а также уровень надежности и доступности самой службы в целом;

c) влияние смены средства связи на бизнес-процессы, например, влияние увеличения скорости пересылки или того факта, что официальные сообщения пересылаются между отдельными людьми, а не между компаниями;

d) юридические вопросы, например, потенциальная необходимость удостоверения отправителя, адресата, отправки и получения;

e) влияние публикации списка сотрудников, доступного извне;

f) контроль удаленного доступа пользователей к учетным записям электронной почты.

8.7.4.2 Политика безопасности в отношении электронной почты

В организации необходимо принять четкую политику, касающуюся использования электронной почты. Данная политика должна охватывать следующие вопросы:

a) атаки, связанные с электронной почтой, например, вирусы и перехват сообщений;

b) защита файлов, передаваемых с помощью электронной почты;

c) правила, касающиеся случаев, когда использовать электронную почту не следует;

d) ответственность сотрудников за то, чтобы не компрометировать компанию (например, путем рассылки дискредитирующих или оскорбительных электронных сообщений или неразрешенного приобретения товаров);

e) применение криптографических средств для защиты конфиденциальности и целостности электронных сообщений (см. раздел 10.3);

f) сохранение сообщений, которые, будучи сохранены, могут быть восстановлены в случае возникновения судебного иска;

g) дополнительные меры для проверки сообщений, которые невозможно аутентифицировать.

8.7.5 Безопасность электронных офисных систем

Необходимо разработать политику и правила контроля операций и рисков, связанных с электронными офисными системами. Эти системы дают возможность ускоренного распространения и совместного использования информации организации с помощью сочетания следующих средств: документы, компьютеры, мобильные компьютеры и средства связи, почта, голосовая почта, устный обмен информацией в целом, мультимедийные данные, почтовые услуги и средства и факсимильные аппараты.

При анализе влияния объединения этих средств на безопасность и деятельность организации следует учитывать:

a) уязвимость информации в офисных системах, например, запись телефонных звонков и сеансов конференц-связи, конфиденциальность звонков, хранение факсов, открытие почты, распространение почты;

b) политика и соответствующие меры для управления обменом информацией, например, использование общих электронных досок объявлений (см. раздел 9.1).

c) исключение категорий конфиденциальной информации в том случае, если система не обеспечивает соответствующего уровня защиты (см. раздел 5.2).

d) ограничение доступа к дневниковой информации, связанной с частью сотрудников, например, с теми, кто участвует в конфиденциальных проектах;

e) пригодность (или непригодность) системы для поддержки определенных видов деятельности организации, например, для передачи заказов или авторизаций;

f) категории сотрудников, подрядчиков и деловых партнеров, которым разрешено использовать систему, и места, из которых к ней можно получить доступ (см. раздел 4.2);

g) предоставление доступа к определенным средствам только избранным категориям пользователей;

h) определение статуса пользователей (например, сотрудников организации или подрядчиков) с помощью каталога для удобства других пользователей;

i) сохранение и резервное копирование информации, хранящейся в системе (см. разделы 12.1.3 и 8.4.1);

j) требования к процедурам аварийного восстановления и необходимые соглашения (см. раздел 11.1).

8.7.6 Общедоступные системы

Необходимо принять меры для защиты целостности информации, опубликованной в электронном виде, чтобы предотвратить несанкционированные изменения, которые могут повредить репутации организации, опубликовавшей эту информацию.. Информация, хранящаяся в общедоступных системах, например, информация на Web-сервере, доступном через Интернет, может попадать под действия законов, правил и нормативных актов в той юрисдикции, где располагается система или совершаются торговые операции. Перед тем, как информация будет открыта для общего доступа, она должна пройти официальный процесс авторизации.

Программное обеспечение, данные и другая информация, которая требует высокой степени целостности, при предоставлении через общедоступные системы должна быть защищена с помощью соответствующих механизмов, например, с помощью цифровых подписей (см. раздел 10.3.3). Системы электронной публикации, особенно те системы, которые обеспечивают обратную связь и прямой ввод информации, должны находиться под тщательным контролем для того, чтобы:

a) информация передавалась в соответствии с действующими законами о защите данных (см. раздел 12.1.4);

b) информация, вводимая в систему публикации и обрабатываемая ей, обрабатывалась полностью и своевременно;

c) конфиденциальная информация была защищена при сборе и при хранении;

d) доступ к системе публикации не обеспечивал неограниченного доступа к сети, к которой она подключена.

8.7.7 Другие формы обмена информацией

Необходимо ввести правила и средства для защиты обмена информацией в устной форме, с

помощью факсимильной связи и с помощью видеосвязи. Безопасность информации может быть нарушена из-за недостаточной осведомленности, отсутствия четких правил по использованию подобных средств (например, из-за того, что разговор по мобильному телефону в общественном месте или сообщения на автоответчике будут подслушаны), несанкционированного доступа к телефонным системам голосовой почты или случайной отправки факсимильного сообщения неправильному адресату.

Нарушение деятельности организации и компрометация информации могут произойти из-за отказа, сбоев или перегрузки средств связи (см. раздел 7.2 и часть 11). Кроме того, информация может быть скомпрометирована в результате доступа неавторизованных пользователей (см. часть 9).

Необходимо разработать для сотрудников четкие правила, касающиеся использования голосовой, факсимильной и видеосвязи. Эти правила должны включать:

a) напоминание о том, что сотрудники должны соблюдать необходимые меры предосторожности, например, не раскрывать конфиденциальную информацию в том случае, если существует возможность подслушивания или перехвата телефонного разговора:

   1) находящимися рядом людьми (в частности, при использовании мобильных телефонов);

   2) путем прослушивания линии или другим способом, предполагающим физический доступ к телефонному аппарату или телефонной линии, или с помощью сканирующих приемников при использовании аналоговых мобильных телефонов;

   3) лицами, находящимися на другом конце линии;

b) напоминание о том, что сотрудники не должны вести конфиденциальных разговоров в общественных местах, открытых кабинетах и переговорных комнатах с тонкими стенами;

c) запрет оставлять сообщения на автоответчиках, поскольку эти сообщения могут быть прослушаны посторонними, сохранены в общедоступных системах или записаны не на том аппарате в результате ошибок в наборе номера;

d) напоминание о проблемах, связанных с использованием факсимильных аппаратов, включая:

   1) несанкционированный доступ к встроенным хранилищам сообщений для получения сообщений;

   2) случайное или намеренное программирование аппаратов для отправки сообщений по определенным номерам;

   3) отправка документов и сообщений по неправильному номеру в результате ошибок в наборе или неверного выбора сохраненных номеров.

9 Контроль доступа

9.1 Требования к контролю доступа в организации

Цель: Контроль доступа к информации.

Доступ к информации и процессам, происходящим в организации, должен контролироваться в соответствии с требованиями бизнеса и нормами безопасности.

При этом следует учитывать политику распространения и авторизации информации.

9.1.1 Политика контроля доступа

9.1.1.1 Политика и требования бизнеса

Необходимо определить и документировать бизнес-требования к контролю доступа. В политике следует четко определить правила контроля доступа и права каждого пользователя или группы пользователей. Пользователи и поставщики услуг должны получить четкое описание бизнес-требований, которым должны соответствовать средства контроля доступа. В политике должно учитываться следующее:

a) требования к безопасности различных бизнес-приложений;

b) идентификация всей информации, связанной с определенным бизнес-приложением;

c) политика распространения и авторизации информации, например, принцип распространения информации только среди тех сотрудников, которым она необходима, а также уровни безопасности и классификация информации;

d) согласование методов контроля доступа с правилами классификации информации в различных системах и сетях;

e) законы и условия контрактов, относящиеся к защите доступа к данным и сервисам (см. раздел 12);

f) стандартные профили доступа пользователей для основных категорий должностей;

g) управление правами доступа в распределенных и сетевых средах для всех имеющихся типов соединений.

9.1.1.2 Правила контроля доступа

При определении правил контроля доступа необходимо учитывать следующее:

a) различия между правилами, которые должны соблюдаться всегда, и правилами, которые являются необязательными или применяются лишь в определенных случаях;

b) установка правил на основе принципа «что не разрешено явно, то запрещено», а не на основе более слабого принципа «что не запрещено явно, то разрешено».

c) автоматическое изменение категорий информации в средствах обработки и изменение категорий информации по решению пользователя (см. раздел 5.2);

d) автоматическое изменение прав доступа пользователя информационной системой и изменение этих прав администратором;

e) правила, для исполнения которых требуется подтверждение администратора или другого лица, и правила, которые не требуют такого подтверждения.

9.2 Управление доступом пользователей

Цель: Предотвратить несанкционированный доступ к информационным системам.

Необходимо разработать официальные правила распределения прав доступа к информационным системам и сервисам.

Эти правила должны охватывать все этапы цикла пользовательского доступа, от первоначальной регистрации новых пользователей до окончательного удаления регистрационных данных тех пользователей, которым больше не требуется доступ к информационным системам и сервисам. При необходимости следует уделить особое внимание контролю над распределением привилегированных прав доступа, которые позволяют обходить реализованные меры защиты.

9.2.1 Регистрация пользователей

Необходимо разработать официальную процедуру регистрации и удаления регистрационных данных пользователей, которая будет использоваться для предоставления доступа ко всем многопользовательским информационным системам и сервисам.

Доступ к многопользовательским информационным сервисам должен контролироваться с помощью официального процесса регистрации пользователей, который должен включать в себя следующее:

a) использование уникальных пользовательских идентификаторов для того, чтобы каждого пользователя можно было установить и персонально привлечь к ответственности за совершенные действия. Разрешать использование групповых идентификаторов можно только в том случае, если они подходят для выполняемой задачи;

b) проверка того факта, что пользователь имеет разрешение владельца системы на использование данной информационной системы или сервиса. В дополнение к этому может потребоваться отдельное подтверждение прав доступа от руководства;

c) проверка того факта, что уровень доступа подходит для выполняемой задачи (см. раздел 9.1) и соответствует принятой в организации политике безопасности, например, не нарушает принципа разделения полномочий (см. раздел 8.1.4);

d) предоставление пользователям письменного описания их прав доступа;

e) требование к пользователям подписать заявление о том, что они знакомы с условиями доступа;

f) подтверждение того факта, что поставщики услуг не предоставляют доступа до завершения процедур авторизации;

g) поддержка официального списка всех лиц, зарегистрированных для работы с данным сервисом;

h) немедленное удаление прав доступа для пользователей, которые перешли на другую должность или покинули организацию;

i) периодическая проверка и удаление ставших ненужными пользовательских идентификаторов и учетных записей;

j) подтверждение того факта, что резервные идентификаторы не присвоены другим пользователям.

Необходимо рассмотреть возможность включения в контракты о приеме на работу и предоставлении услуг описание мер, которые последуют в случае попытки сотрудника или

агента получить несанкционированный доступ (см. также разделы 6.1.4 и 6.3.5).

9.2.2 Управление привилегиями

Распределение и использование привилегий (функций или средств многопользовательской информационной системы, позволяющих определенному пользователю обходить реализованные в системе или приложениях средства защиты) необходимо ограничить и контролировать. Неправильное использование системных привилегий зачастую является одной из основных причин нарушения работы систем, подвергшихся атаке.

В многопользовательских системах, требующих защиты от несанкционированного доступа, распределение привилегий должно контролироваться с помощью формального процесса авторизации. Рекомендуется рассмотреть следующие меры:

a) Необходимо определить привилегии, связанные с каждым компонентом системы (операционной системой, системой управления базами данных и отдельными приложениями), и категории сотрудников, которым они требуются.

b) Привилегии должны предоставляться сотрудникам только в случае необходимости их использования и для каждого события в отдельности, т. е. привилегии должны быть минимальными для их функциональной роли и только тогда, когда они необходимы.

c) Необходимо соблюдать процесс утверждения и вести запись сведений обо всех предоставленных привилегиях. Привилегии не должны предоставляться до завершения процесса утверждения.

d) Следует способствовать разработке и применению системных процедур для того, чтобы избежать необходимости предоставления привилегий пользователям.

e) Привилегии должны назначаться не для той пользовательской записи, которая используется для обычной деятельности.

9.2.3 Управление паролями пользователей

Пароли – распространенное средство проверки личности пользователя для доступа к информационной системе или сервису. Предоставление паролей должно контролироваться посредством официальной процедуры, отвечающей следующим требованиям:

a) пользователи должны подписывать заявление о том, что личные пароли будут храниться в секрете, а пароли рабочих групп будут известны только членам группы (эти условия могут быть включены в контракт о приеме на работу; см. раздел 6.1.4);

b) если пользователи должны выбирать свои пароли самостоятельно, необходимо гарантировать, что изначально им будет предоставлен надежный временный пароль, который они будут должны немедленно сменить. В том случае, если пользователь забудет свой пароль, временный пароль должен предоставляться только после однозначного подтверждения личности пользователя;

c) временные пароли должны предоставляться пользователям с соблюдением норм безопасности. Избегайте передачи через посредников и использования незащищенных (незашифрованных) сообщений электронной почты. Пользователи должны подтверждать получение паролей.

Пароли не должны храниться в компьютерной системе в незащищенном виде. При необходимости можно рассмотреть возможность использования других технологий идентификации и аутентификации пользователей, в частности, биометрических технологий (например, проверки отпечатков пальцев), проверки подписи и аппаратных средств, например, смарт-карт.

9.2.4 Проверка прав доступа пользователей

Чтобы обеспечить эффективный контроль доступа к данным и информационным сервисам, необходимо ввести официальный процесс регулярной проверки прав доступа пользователей, отвечающий следующим требованиям:

a) права доступа пользователей должны проверяться через регулярные интервалы (рекомендуется интервал в полгода), а также после внесения каких-либо изменений (см. раздел 9.2.1);

b) разрешения на обладание особыми привилегированными правами доступа (см. раздел 9.2.2) должны проверяться чаще (рекомендуется интервал в три месяца);

c) необходимо регулярно проверять предоставленные привилегии, чтобы убедиться в отсутствии привилегий, полученных без разрешения.

9.3 Обязанности пользователей

Цель: Предотвращение несанкционированного доступа пользователей.

Для эффективной поддержки безопасности требуется сотрудничество авторизованных пользователей.

Пользователи должны быть поставлены в известность о своих обязанностях по поддержке эффективных мер контроля доступа, в частности, о правилах использования паролей и защите пользовательского оборудования.

9.3.1 Использование паролей

При выборе и использовании паролей пользователи должны применять надежные методы.

Пароли служат для подтверждения личности пользователя и, следовательно, для определения прав доступа к сервисам и средствам обработки информации. Всем пользователям необходимо рекомендовать:

a) держать пароли в секрете;

b) не записывать пароли на бумаге в том случае, если гарантировать безопасность хранения этой бумаги нельзя;

c) менять пароли при любых признаках возможного нарушения безопасности системы или паролей;

d) выбирать надежные пароли, имеющие длину не менее шести символов. Пароли должны отвечать следующим требованиям:

   1) легко запоминаться;

   2) не основываться на информации, которую другие могут легко угадать или узнать (имена, номера телефонов, даты рождения и т. п.);

   3) не содержать последовательностей одинаковых символов и групп, состоящих только из цифр или только из букв.

e) менять пароли с определенным интервалом или после определенного количества сеансов доступа (пароли для привилегированных учетных записей должны меняться чаще, чем обычные пароли), и избегать повторного использования старых паролей;

f) изменять временные пароли при первом входе в систему;

g) не включать пароли в автоматизированные процедуры входа в систему (например, не

записывать их в качестве макросов и не назначать на функциональные клавиши);

h) не использовать индивидуальные пароли совместно.

Если какому-то пользователю требуется доступ к нескольким сервисам или платформам и, соответственно, несколько паролей, ему необходимо порекомендовать, что он может использовать один и тот же надежный пароль (см. пункт «г» выше) для всех сервисов, обеспечивающих необходимый уровень защиты при хранении пароля.

9.3.2 Оборудование, остающееся без присмотра

Пользователи должны обеспечивать необходимую защиту оборудования, остающегося без присмотра. Оборудование, установленное на пользовательских территориях, например, рабочие станции и файловые серверы, могут потребовать особой защиты от несанкционированного доступа в том случае, если они останутся без присмотра на длительный срок. Все пользователи и подрядчики должны быть поставлены в известность о требованиях безопасности и правилах защиты остающегося без присмотра оборудования, а также о своих обязанностях по обеспечению этой защиты. Пользователям рекомендуется:

a) прекращать активные сеансы при завершении работы, если безопасность этих сеансов не обеспечивается с помощью какого-либо механизма блокировки (например, экранной заставки с парольной защитой);

b) завершать сеанс связи с компьютером-мэйнфреймом по завершении работы (т. е. не просто выключать свой компьютер или терминал);

c) защищать компьютеры и терминалы от несанкционированного использования с помощью блокирования клавиатуры или аналогичного средства (например, парольной защиты).

9.4 Контроль доступа к вычислительной сети

Цель: Защита сетевых сервисов.

Доступ как ко внутренним, так и к внешним сетевым сервисам следует контролировать.

Это поможет гарантировать, что пользователи, имеющие доступ к сети и сетевым сервисам, не нарушают безопасность этих сервисов. Для этого используются следующие средства:

a) соответствующие интерфейсы между сетью организации и общественными сетями и сетями, принадлежащими другим организациям;

b) соответствующие механизмы аутентификации для пользователей и оборудования;

c) контроль доступа пользователей к информационным сервисам.

9.4.1 Политика использования сетевых сервисов

Незащищенные подключения к сетевым сервисам могут повлиять на безопасность всей организации. Пользователям должен предоставляться непосредственный доступ только к тем сервисам, на использование которых они получили специальное разрешение. Это в особенности важно для сетевых подключений к конфиденциальным или критичным бизнес-приложениям, а также для пользователей, работающих в областях с повышенным риском, например, в общественных местах и на внешних территориях, находящихся за пределами области действия средств защиты, реализованных в организации.

Необходимо разработать политику в отношении использования сетей и сетевых сервисов. Эта политика должна охватывать:

a) сети и сетевые сервисы, к которым разрешается доступ;

b) процедуры авторизации, позволяющие определить, какие пользователи имеют право доступа к каким сетям и сетевым сервисам;

c) административные правила и средства защиты доступа к сетевым подключениям и сетевым сервисам.

Эта политика должна быть согласована с политикой контроля доступа в организации (см. раздел 9.1).

9.4.2 Фиксированные (enforced) маршруты

Иногда возникает необходимость контролировать маршрут от пользовательского терминала к компьютерному сервису. Сети разрабатываются так, чтобы обеспечить максимальную широту совместного использования ресурсов и гибкость маршрутизации. Однако злоумышленники могут воспользоваться этими возможностями для несанкционированного доступа к бизнес-приложениям или несанкционированного использования средств обработки информации. Чтобы уменьшить вероятность этого, можно разработать средства для ограничения маршрута между пользовательским терминалом и компьютерным сервисом, с которым данный пользователь имеет право работать – например, создать фиксированный маршрут.

Цель создания фиксированного маршрута – не позволять пользователям выбирать маршруты, лежащие за пределами определенного маршрута между пользовательским терминалом и сервисами, с которыми пользователь имеет право работать.

Как правило, это требует установки определенных средств в различных пунктах маршрута. Принцип заключается в том, чтобы возможности маршрутизации в каждом пункте сети ограничивались лишь выбранными вариантами.

Вот несколько примеров:

a) использование выделенных линий или отдельных телефонных номеров;

b) автоматическое подключение портов к выбранным прикладным системам или шлюзам безопасности (Security gateway);

c) ограничение набора пунктов меню для отдельных пользователей;

d) запрет на неограниченное перемещение по сети;

e) использование только определенных прикладных программных систем и/или шлюзов безопасности для внешних пользователей сети;

f) активный контроль разрешенных соединений между источниками и адресатами с помощью шлюзов безопасности (например, межсетевых экранов);

g) ограничение доступа к сети путем создания отдельных логических зон, например, виртуальных частных сетей, для групп пользователей внутри организации (см. также раздел 9.4.6).

Требования к фиксированному маршрутизированию должны быть основаны на политике контроля доступа в организации (см. раздел 9.1).

9.4.3 Аутентификация пользователей для внешних подключений

Внешние подключения (например, подключения по телефонным линиям) предоставляют потенциальную возможность для несанкционированного доступа к информации организации. В связи с этим для доступа удаленных пользователей должна применяться аутентификация. Существуют различные методы аутентификации. Некоторые их этих методов обеспечивают

более эффективную защиту по сравнению с другими – например, методы, основанные на шифровании, могут обеспечить усиленную аутентификацию. Необходимый уровень защиты следует определить при оценке рисков. Эта информация потребуется при выборе подходящего метода аутентификации.

Для аутентификации удаленных пользователей можно использовать, например, криптографические методы, аппаратные средства или протоколы с запросом и подтверждением. Кроме того, для обеспечения достоверности источника соединения могут использоваться выделенные частные линии или средства проверки сетевых адресов пользователей.

Для защиты от несанкционированных и нежелательных подключений к средствам обработки информации в организациях могут использоваться средства обратного вызова, например, модемы с функцией обратного вызова. Этот метод контроля служит для аутентификации пользователей, пытающихся подключиться к сети организации из удаленного пункта. При применении этого метода не следует использовать сетевые сервисы, обеспечивающие перенаправление вызовов. Если функция перенаправления вызовов все же имеется, ее следует отключить, чтобы избежать связанных с ней уязвимостей. Кроме того, процесс обратного вызова обязательно должен включать проверку реального прекращения соединения со стороны организации. В противном случае удаленный пользователь может остаться на линии, сымитировав проверку путем обратного вызова. Средства обратного вызова следует тщательно проверить на наличие этой возможности.

9.4.4 Аутентификация узлов

Средства автоматического подключения к удаленному компьютеру могут быть использованы злоумышленникам для получения несанкционированного доступа к бизнес-приложениям. В связи с этим подключения к удаленным компьютерным системам должны требовать аутентификации. Это особенно важно в том случае, если для подключения используется сеть, находящаяся за пределами контроля организации. Некоторые примеры методов аутентификации и способов ее реализации приведены в разделе 9.4.3 выше.

Аутентификация узлов может служить альтернативным средством для аутентификации групп удаленных пользователей при подключении к совместно используемым защищенным компьютерным сервисам (см. раздел 9.4.3).

9.4.5 Защита удаленных диагностических портов

Доступ к диагностическим портам должен тщательно контролироваться. Во многих компьютерах и системах связи имеется система удаленной диагностики путем подключения по телефонной линии, используемая инженерами сервисной службы. При отсутствии защиты такие диагностические порты могут быть использованы для несанкционированного доступа. Поэтому они должны быть защищены с помощью соответствующего защитного механизма (например, замка). Необходимо ввести правила, гарантирующие, что эти порты будут доступны только по договоренности между сотрудником, ответственным за компьютерную систему, и специалистами сервисной службы, которым необходим доступ.

9.4.6 Разделение вычислительных сетей

По мере появления партнерских отношений, требующих объединения или совместного использования сетей и средств обработки информации, сети все чаще выходят за традиционные рамки организации. Такое расширение может увеличить риск несанкционированного доступа к подключенным к сети информационным системам, некоторые из которых могут требовать защиты от других пользователей сети из-за своей критичности или конфиденциальности. В подобных условиях рекомендуется рассмотреть

внедрение средств сетевого контроля для разделения групп информационных сервисов, пользователей и информационных систем.

Один из методов контроля безопасности в крупных сетях – разделение таких сетей на отдельные логические сетевые зоны, например, внутренние сетевые зоны организации и внешние сетевые зоны. Каждая такая зона защищается определенным периметром безопасности. Подобный периметр можно реализовать путем установки защищенного шлюза между двумя объединяемыми сетями для контроля доступа и передачи информации между этими двумя доменами. Конфигурация данного шлюза должна обеспечивать фильтрацию трафика между этими доменами (см. разделы 9.4.7 и 9.4.8) и блокировку несанкционированного доступа в соответствии с политикой контроля доступа в организации (см. раздел 9.1). Хорошим примером подобного шлюза является система, которую принято называть межсетевым экраном.

Критерии разделения сети на зоны должны быть основаны на политике контроля доступа и требованиях к доступу (см. раздел 9.1). Кроме того, при внедрении средств сетевой маршрутизации и шлюзов необходимо учитывать относительную стоимость и влияние на производительность (см. разделы 9.4.7 и 9.4.8).

9.4.7 Контроль сетевых подключений

Политика контроля доступа в совместно используемых сетях, в особенности в тех сетях, которые выходят за пределы организации, может требовать реализации средств ограничения возможностей подключения для пользователей. Подобные средства могут быть реализованы с помощью сетевых шлюзов, фильтрующих трафик в соответствии с заданной таблицей или набором правил. Вводимые ограничения должны быть основаны на политике доступа и на потребностях организации (см. раздел 9.1). Эти ограничения необходимо поддерживать и своевременно обновлять.

Вот примеры областей, для которых необходимо ввести ограничения:

a) электронная почта;

b) односторонняя передача файлов;

c) двухсторонняя передача файлов;

d) интерактивный доступ;

e) сетевой доступ с привязкой ко времени дня или дате.

9.4.8 Контроль сетевой маршрутизации

В совместно используемых сетях, в особенности в тех сетях, которые выходят за пределы организации, может возникнуть необходимость создания средств контроля маршрутизации, гарантирующих, что компьютерные подключения и потоки данных не нарушают политику контроля доступа в организации (см. раздел 9.1). Такой контроль зачастую необходим для сетей, которые используются совместно с другими пользователями, не являющимися сотрудниками организации.

Средства контроля маршрутизации должны быть основаны на специальных механизмах проверки адресов источника и пункта назначения. Кроме того, для изоляции сетей и предотвращения возникновения маршрутов между двумя сетями различных организаций очень удобно использовать механизм трансляции сетевых адресов. Эти средства могут быть реализованы как на программном, так и на аппаратном уровне. При реализации необходимо учитывать мощность выбранных механизмов.

9.4.9 Безопасность сетевых сервисов

В общественных и частных сетях существует множество сервисов. Некоторые из этих сервисов являются платными. Сетевые сервисы могут обладать уникальными или сложными характеристикам безопасности. При использовании сетевых сервисов организация должна получить четкое описание атрибутов безопасности для каждого из используемых сервисов.

9.5 Контроль доступа к операционным системам

Цель: Предотвращение несанкционированного доступа к компьютерам.

Для ограничения доступа к ресурсам компьютеров следует использовать средства защиты на уровне операционной системы. Система должна поддерживать следующие средства:

a) идентификация и проверка каждого авторизованного пользователя (при необходимости сюда может входить проверка терминала или местонахождения пользователя);

b) запись сведений об успешных и неудачных попытках доступа к системе;

c) поддержка необходимых средств аутентификации. При использовании паролей система должна гарантировать их надежность (см. раздел 9.3.1.г);

d) при необходимости – ограничение времени подключения пользователей.

Если деятельность организации требует дополнительной защиты, можно использовать и другие средства контроля доступа, например, метод запроса и подтверждения.

9.5.1 Автоматическая идентификация терминалов

Для аутентификации подключений к определенным пунктам и к портативному оборудованию рекомендуется использовать механизм автоматической идентификации терминалов. Механизм автоматической идентификации терминалов можно использовать в том случае, если система должна позволять устанавливать подключения только из определенного пункта или с определенного компьютерного терминала. Идентификатор, встроенный в терминал или присоединенный к нему, может указывать, имеет ли данный терминал право выполнять определенные операции. Чтобы обеспечить безопасность такого идентификатора, может потребоваться физическая защита терминала. Кроме того, для аутентификации пользователей может применяться ряд других методов (см. раздел 9.4.3).

9.5.2 Процедуры входа в систему с помощью терминала

Для доступа к информационным сервисам должна использоваться защищенная процедура входа в систему. Процедура входа в компьютерную систему должна быть разработана так, чтобы свести к минимуму возможность несанкционированного доступа. Поэтому такая процедура должна включать в себя минимум информации о системе, чтобы злоумышленники не смогли воспользоваться полученной информацией в своих целях. Ниже перечислены качества, которыми должна обладать правильная процедура входа в систему:

a) идентификаторы системы или приложений должны выводиться на экран только после того, как процесс входа в систему будет успешно завершен;

b) на экран должно выводиться общее предупреждение о том, что доступ к данному компьютеру могут получать только авторизованные пользователи;

c) во время входа в систему на экран не должны выводиться справочные сообщения, которые могут помочь злоумышленникам;

d) сведения о правильности введенной информации должны выводиться только после того, как информация будет введена полностью. При возникновении ошибки система не должна указывать, какая часть данных является правильной или неправильной;

e) количество неудачных попыток входа должно быть ограничено (рекомендуется три попытки). Кроме того, рекомендуется ввести следующие меры:

   1) запись сведений о неудачных попытках;

   2) введение задержки перед тем, как попытку входа систему можно будет повторить, или запрещение дополнительных попыток до получения соответствующего разрешения;

   3) отключение каналов передачи данных;

f) необходимо ограничить максимальное и минимальное время, которое отводится на процедуру входа в систему. При превышении этого времени процедура входа в систему должна быть прекращена;

g) при успешном входе в систему по завершении процедуры должна выводиться следующая информация:

   1) дата и время предыдущего успешного входа в систему;

   2) сведения о неудачных попытках входа в систему с момента последнего успешного входа в систему.

9.5.3 Идентификация и аутентификация пользователей

Все пользователи (включая специалистов по технической поддержке – операторов, сетевых администраторов, системных программистов, администраторов баз данных и т. п.) должны иметь уникальный идентификатор для единоличного использования. Благодаря этому для любой операции можно будет определить выполнившего ее пользователя. Пользовательские идентификаторы никоим образом не должны указывать на уровень привилегий пользователей (см. раздел 9.2.2), например, администраторов и супервизоров.

В исключительных случаях при наличии очевидных преимуществ для деятельности организации можно использовать общие идентификаторы для группы пользователей или для конкретной задачи. Для подобных случаев необходимо письменное разрешение руководства. При этом могут потребоваться дополнительные меры для определения персонализации ответственности.

Существуют различные процедуры аутентификации, которые можно использовать для подтверждения заявленных персональных данных пользователя. Одним из наиболее распространенных средств идентификации и аутентификации являются пароли (см. также разделы 9.3.1 и далее), основанные на секретной информации, известной только пользователю-владельцу пароля. Тех же целей можно достичь с помощью криптографических средств и протоколов аутентификации.

Кроме того, для идентификации и аутентификации можно использовать такие средства, как карты памяти или смарт-карты, или биометрические технологии аутентификации, действующие на основе уникальных характеристик или атрибутов отдельного человека. Для усиленной аутентификации можно использовать сочетание связанных между собой технологий и механизмов.

9.5.4 Система управления паролями

Пароли – это одно из основных средств подтверждения прав пользователя на доступ к компьютерному сервису. Системы управления паролями должны включать в себя

эффективные интерактивные функции, обеспечивающие надежность паролей (рекомендации по использованию паролей можно найти в разделе 9.3.1).

В некоторых случаях пользовательские пароли должны назначаться какой-либо независимой структурой. Однако в большинстве случаев пароли выбираются и поддерживаются самими пользователями.

Ниже перечислены требования, которым должна удовлетворять хорошая система управления паролями:

a) обязывать к использованию индивидуальных паролей для сохранения ответственности;

b) при необходимости позволять пользователям выбирать и изменять свои собственные пароли и включать в себя процедуру подтверждения ввода, оберегающую от ошибок при вводе;

c) обязывать к использованию надежных паролей, как описано в разделе 9.3.1;

d) обязывать к изменению паролей, как описано в разделе 9.3.1, если пользователи выбирают пароли самостоятельно;

e) если пользователи выбирают пароли самостоятельно, обязывать их менять временные пароли при первом входе в систему (см. раздел 9.2.3);

f) хранить сведения о ранее использовавшихся паролях пользователей (например, за предыдущие 12 месяцев) и предотвращать повторное использование;

g) не отображать пароли на экране при вводе;

h) хранить файлы паролей отдельно от информации прикладных систем;

i) хранить пароли в зашифрованном виде с использованием одностороннего алгоритма шифрования;

j) изменять стандартные пароли после установки программного обеспечения.

9.5.5 Использование системных утилит

В большинстве компьютерных систем имеется определенное число служебных программ (утилит), которые могут иметь возможность обходить средства защиты, реализованные в системе и приложениях. Необходимо ограничить и тщательно контролировать использование этих утилит. Рекомендуется рассмотреть следующие меры:

a) использование процедур аутентификации для системных утилит;

b) изоляция системных утилит от прикладных программ;

c) предоставление возможности использования системных утилит лишь минимальному кругу доверенных авторизованных пользователей, которым они действительно необходимы;

d) авторизация для использования системных утилит при возникновении разовой необходимости;

e) ограничение доступности системных утилит (например, утилиты могут быть доступны только при внесении санкционированных изменений в систему);

f) ведение журнала работы всех системных утилит;

g) определение и документирование уровней авторизации для системных утилит;

h) удаление всех ненужных утилит и системных программ.

9.5.6 Сигнал тревоги для защиты пользователей

Рекомендуется подумать о создании сигнала тревоги для пользователей, которые могут действовать под принуждением. Решение о том, следует ли применять на практике такие сигналы, должно быть основано на результатах оценки рисков. Необходимо определить обязанности и правила реакции на сигнал тревоги, указывающий на действия под принуждением.

9.5.7 Отключение терминалов по тайм-ауту

Неактивные терминалы на территориях с высокой степенью риска (например, терминалы в общедоступных или внешних помещениях, на которые не распространяются реализованные в организации меры по обеспечению безопасности, а также терминалы, подключенные к системам высокой важности) должны отключаться после определенного периода неактивности, чтобы предотвратить несанкционированный доступ к ним. При отключении терминалов по тайм-ауту после определенного периода бездействия экран терминала должен очищаться, а сетевые соединения и сеансы работы с программами должны прекращаться. Длительность тайм-аута должна соответствовать уровню риска на той территории, где находится терминал, и кругу пользователей терминала.

На некоторых персональных компьютерах можно использовать ограниченную форму отключения по тайм-ауту, при которой очищается экран и включается защита от несанкционированного доступа, однако сетевые соединения и сеансы работы с программами не прекращаются.

9.5.8 Ограничение времени соединения

Ограничение на время соединения должно обеспечить дополнительную безопасность для областей деятельности, связанных с высокой степенью риска. Ограничение периода, в течение которого разрешены терминальные подключения к компьютерным сервисам, уменьшает возможность несанкционированного доступа во время подключения. Рекомендуется рассмотреть введение подобной меры для важных компьютерных приложений, особенно в том случае, если используемые для работы с ними терминалы установлены в областях с высоким риском, например, в общедоступных или внешних помещениях, на которые не распространяются реализованные в организации меры по обеспечению безопасности. Вот несколько примеров подобных ограничений:

a) использование заранее заданных промежутков времени, например, для пакетной передачи файлов, или регулярных кратковременных интерактивных сеансов;

b) предоставление соединений только в обычные рабочие часы (в том случае, если сверхурочная работа не выполняется).

9.6 Контроль доступа к приложениям

Цель: Предотвратить несанкционированный доступ к информации, хранящейся в информационных системах. Необходимо ввести меры, ограничивающие доступ к прикладным системам. Логический доступ к программному обеспечению и информации должен предоставляться только авторизованным пользователям. Прикладные системы должны:

a) контролировать доступ пользователей к информации и функциям прикладных программ в соответствии с принятой в организации политикой контроля доступа;

b) обеспечивать защиту от несанкционированного доступа для любых утилит и системных программ, которые способны обходить средства защиты, реализованные в операционной системе и приложениях;

c) не нарушать безопасность других систем, совместно с которыми используются информационные ресурсы;

d) иметь возможность обеспечить доступ к информации только для владельца, для других выделенных авторизованных пользователей или для определенных групп пользователей.

9.6.1 Ограничение доступа к информации

Пользователи прикладных систем, в том числе специалисты по поддержке, должны получать доступ к информации и функциям прикладных программ в соответствии с принятой в организации политикой доступа к информации (см. раздел 9.1) и индивидуальными потребностями каждой области деятельности. Рекомендуется рассмотреть возможность введения следующих мер для ограничения доступа:

a) создание меню для управления доступом к функциям прикладных программ;

b) предоставление пользователям только той информации о функциях прикладных программ, которую им разрешено знать (для этого может потребоваться соответствующее редактирование пользовательской документации);

c) контроль прав доступа пользователей (например, прав чтения, записи, удаления и исполнения);

d) проверка того факта, что результаты работы прикладных программ, работающих с конфиденциальной информацией, содержат только те данные, которые необходимы для целей использования результатов, и что результаты пересылаются только на авторизованные терминалы и в разрешенные пункты. Следует регулярно проверять, удаляется ли излишняя информация из результатов работы.

9.6.2 Изоляция конфиденциальных систем

Конфиденциальные системы могут потребовать создания выделенной (изолированной) вычислительной среды. Некоторые прикладные системы настолько чувствительны к потенциальным потерям, что требуют особого обращения. В зависимости от степени конфиденциальности система может работать на отдельном компьютере, использовать ресурсы совместно только с доверенными прикладными системами или вообще не иметь ограничений. Необходимо принимать во внимание следующее:

a) Уровень конфиденциальности прикладной системы должен быть четко определен и задокументирован владельцем системы (см. раздел 4.1.3).

b) Если конфиденциальное приложение должно работать в совместно используемой среде, необходимо определить прикладные системы, совместно с которыми будут использоваться ресурсы, и согласовать их список с владельцем конфиденциального приложения.

9.7 Мониторинг доступа и использования системы

Цель: Обнаружение несанкционированных действий.

За работой систем необходимо наблюдать, определяя отклонения от политики управления доступом и регистрируя события, которые можно отследить, чтобы иметь улики в случае инцидентов, связанных с безопасностью.

Мониторинг систем позволяет проверить эффективность реализованных мер и соответствие модели политики безопасности (см. раздел 9.1).

9.7.1 Ведение журнала событий

Необходимо вести контрольные журналы, в которые будут заноситься исключительные ситуации и другие события, связанные с безопасностью. Эти журналы должны храниться в течение установленного периода, чтобы иметь возможность использовать их в будущих расследованиях и при мониторинге контроля доступа. Помимо прочего, контрольные журналы должны включать следующую информацию:

a) идентификаторы пользователей;

b) дату и время входа в систему и завершения сеансов;

c) идентификатор или местоположение терминала (по возможности);

d) записи об успешных и неудачных попытках получения доступа к системе;

e) записи об успешных и неудачных попытках получения доступа к данным и другим ресурсам.

Некоторые контрольные журналы могут требовать архивирования в соответствии с политикой хранения записей или в связи с требованиями к сбору улик (см. также часть 12).

9.7.2 Мониторинг использования системы

9.7.2.1 Процедуры и области риска

Необходимо разработать процедуры для мониторинга использования средств обработки информации. Эти процедуры помогут гарантировать, что пользователи выполняют только те действия, которые явным образом им разрешены. Уровень мониторинга, необходимый для отдельных средств, следует определить при оценке рисков. Рекомендуется рассмотреть мониторинг следующих областей:

a) авторизованный доступ, включая следующую информацию:

   1) идентификатор пользователя;

   2) дата и время основных событий;

   3) типы событий;

   4) файлы, к которым был получен доступ;

   5) использованные программы и утилиты;

b) все привилегированные операции, например:

   1) использование учетной записи супервизора;

   2) запуск и остановка системы;

   3) подключение и отключение устройств ввода-вывода;

c) попытки несанкционированного доступа, в том числе:

   1) неудачные попытки;

   2) нарушения политики доступа и уведомления о нарушениях для сетевых шлюзов и межсетевых экранов;

   3) сигналы тревоги от специализированных систем обнаружения вторжений;

d) системные сигналы о событиях и сбоях, например:

   1) сообщения и сигналы тревоги на консоли;

   2) чрезвычайные события, записанные в системный журнал;

3) сигналы тревоги от средств сетевого управления.

9.7.2.2 Факторы риска

Результаты мониторинга необходимо регулярно просматривать. Частота просмотра должна зависеть от существующей степени риска. Вот некоторые факторы риска, которые следует учитывать:

a) критичность прикладных процессов;

b) ценность, конфиденциальность или критичность обрабатываемой информации;

c) предыдущие случаи проникновения в систему и неправомерного использования;

d) степень взаимосвязи систем (в частности, в общедоступных сетях).

9.7.2.3 Ведение и просмотр журнала событий

При просмотре журнала необходимо понимать угрозы, с которыми сталкивается система, и способы, которыми эти угрозы могут проявиться. Примеры событий, которые могут потребовать дополнительного расследования в случае инцидентов, приводятся в разделе 9.7.1.

Системные журналы часто содержат большие объемы информации, значительная часть которых не относится к мониторингу безопасности. Чтобы упростить обнаружение значительных событий, относящихся к мониторингу безопасности, рекомендуется рассмотреть средства автоматического копирования сообщений определенных типов в отдельный журнал и/или о применении подходящих системных утилит или аудиторских средств для анализа файлов.

При распределении обязанностей по просмотру журнала следует постараться, чтобы лица, просматривающие журнал, не входили в круг тех лиц, информация о действиях которых просматривается.

Следует обратить особое внимание на защиту средств ведения журнала, поскольку в случае их подделки может возникнуть ложное чувство безопасности. Необходимо реализовать средства защиты от несанкционированных изменений и от проблем в работе, в том числе от следующих проблем:

a) деактивация системы ведения журнала;

b) изменение перечня записываемых типов сообщений;

c) редактирование или удаление файлов журнала;

d) недостаток свободного места для записи журнала, в результате чего события могут быть либо перезаписаны, либо не записаны вообще.

9.7.3 Синхронизация часов

Правильная установка часов компьютеров необходима для того, чтобы гарантировать точность контрольных журналов, которые могут потребоваться для расследований или в качестве улик при уголовном или административном преследовании. Неточность контрольных журналов может затруднить расследование и снизить достоверность этих улик.

Если в компьютере или коммуникационном устройстве имеются часы истинного времени, эти часы необходимо установить в соответствии в принятым стандартом (например, всемирным координированным временем – UCT) или в соответствии с местным временем. Поскольку некоторые часы со временем отстают или уходят вперед, необходимо ввести процедуру проверки и коррекции значительных отклонений.

9.8 Мобильные компьютеры и средства удаленной работы

Цель: Гарантировать безопасность информации при использовании мобильных компьютеров и средств удаленной работы.

Вводимые меры безопасности должны соответствовать рискам, связанным с этими методами работы. При использовании мобильных компьютеров необходимо учесть риск, связанный с работой в незащищенной среде, и принять соответствующие защитные меры. При использовании средств удаленной работы в организации необходимо создать защиту места удаленной работы и обеспечить наличие соответствующих мер для данного вида работы.

9.8.1 Мобильные компьютеры

При использовании мобильных вычислительных средств (например, ноутбуков, карманных компьютеров и мобильных телефонов) необходимо соблюдать особые меры предосторожности, чтобы не допустить компрометирования информации, принадлежащей организации. Необходимо принять официальную политику, учитывающую риск, связанный с использованием мобильных компьютеров, и в частности с работой в незащищенной среде. К примеру, такая политика должна включать требования к физической защите, контролю доступа, криптографическим методам, резервному копированию и защите от вирусов. Кроме того, эта политика также должна включать в себя правила подключения мобильных устройств к сетям и рекомендации по использованию этих устройств в общественных местах.

При использовании мобильных вычислительных средств в общественных местах, переговорных комнатах и других незащищенных помещениях за пределами территории организации необходимо соблюдать осторожность. Подобные устройства должны быть защищены от несанкционированного доступа и раскрытия хранящейся и обрабатываемой ими информации, например, с помощью криптографических средств (см. раздел 10.3).

При использовании подобных устройств в общественных местах надо следить за тем, чтобы посторонние не смогли подсмотреть важную информацию. Необходимо установить средства защиты от злонамеренных программ и своевременно обновлять их (см. раздел 8.3). Следует обзавестись оборудованием для быстрого и простого резервного копирования информации. Резервные копии должны иметь адекватную защиту, в частности, от кражи и потери информации.

Необходимо обеспечить должный уровень защиты при использовании мобильных устройств, подключенных к сетям. Удаленный доступ к информации организации через общественную сеть с помощью мобильных вычислительных устройств должен осуществляться только после успешной идентификации и аутентификации и при наличии соответствующих механизмов контроля доступа (см. раздел 9.4).

Кроме того, мобильные вычислительные средства должны быть физически защищены от кражи, в особенности в том случае, если их оставляют в автомобилях и других транспортных средствах, номерах гостиниц, конференц-залах и переговорных комнатах. Устройства, содержащие критичную и/или конфиденциальную информацию, не должны оставаться без присмотра. По возможности их следует хранить в запертом помещении или защищать с помощью специальных замков. Дополнительную информацию о физической защите мобильного оборудования можно найти в разделе 7.2.5.

Необходимо провести обучение сотрудников, использующих мобильные вычислительные средства, чтобы привлечь их внимание к дополнительным рискам, связанным с этими методами работы, и необходимым мерам.

9.8.2 Средства удаленной работы

В средствах удаленной работы используются технологии связи, позволяющие отдельным

сотрудникам работать удаленно, находясь в фиксированном месте за пределами организации. Территория, где происходит удаленная работа, должна иметь необходимую защиту – в частности, от кражи оборудования и информации, несанкционированного раскрытия информации, несанкционированного удаленного доступа к внутренним системам организации и неправомерного использования технических средств. Применение средств удаленной работы должно санкционироваться и контролироваться руководством. Данный метод работы должен обеспечиваться соответствующими мерами.

Организации рекомендуется разработать политику, правила и стандарты для управления удаленной работой. Использование средств удаленной работы должно разрешаться только в том случае, если эти средства обладают необходимыми функциями для обеспечения безопасности и соответствуют принятой в организации политике безопасности. Рекомендуется рассмотреть следующее:

a) нынешняя физическая безопасность места, где будет происходить удаленная работа, в том числе физическая безопасность здания и ближайшего окружения;

b) предполагаемые средства удаленной работы;

c) требования к безопасности связи с учетом необходимости удаленного доступа к внутренним системам организации, конфиденциальности информации, которая будет использоваться в работе и передаваться по каналу связи, а также конфиденциальности внутренней системы;

d) угроза несанкционированного доступа других людей, находящихся в том же помещении (например, родственников и друзей), к информации или ресурсам.

Ниже перечислены условия и меры, о которых необходимо позаботиться:

a) наличие необходимого оборудования и мебели для хранения средств удаленной работы;

b) определение разрешенных работ, рабочих часов, классификации информации, которая может использоваться, и внутренних систем и сервисов, право доступа к которым имеет удаленный работник;

c) наличие необходимого коммуникационного оборудования и методов защиты удаленного доступа;

d) физическая безопасность;

e) нормы и правила, касающиеся доступа родственников и посетителей к оборудованию и информации;

f) поддержка и обслуживание оборудования и программного обеспечения;

g) процедуры резервного копирования и обеспечения непрерывности бизнеса;

h) аудит и мониторинг безопасности;

i) отзыв полномочий, аннулирование прав доступа и возврат оборудования по окончании удаленной работы.

10 Разработка и обслуживание систем

10.1 Требования к безопасности систем

Цель: Обеспечить наличие встроенных средств защиты в информационных системах.

Сюда входит инфраструктура, бизнес-приложения и приложения, разработанные пользователями. Разработка и внедрение бизнес-процесса для поддержки приложения или сервиса могут оказывать значительное влияние на безопасность. Перед тем, как приступать к разработке информационной системы, необходимо определить и согласовать требования к безопасности.

Все требования к безопасности, включая возможную необходимость средств аварийного восстановления, должны быть учтены в проекте на этапе определения требований и оценены, согласованы и задокументированы в составе общего процесса создания информационной системы.

10.1.1 Анализ и определение требований к безопасности

При описании требований организации к созданию новых систем или к усовершенствованию существующих необходимо учитывать потребность в средствах обеспечения безопасности. При создании подобных спецификаций следует рассмотреть возможность включения в систему автоматических средств управления и необходимость в дополнительных ручных средствах управления. Подобный подход следует применять и при оценке программных пакетов, которые предполагается использовать в деятельности организации. В случае необходимости руководство может принять решение воспользоваться продуктами, прошедшими независимую оценку и сертификацию.

Требования к безопасности и средства защиты должны соответствовать ценности используемых информационных ресурсов и потенциальному ущербу для организации в случае сбоя или нарушения безопасности. Основой для анализа требований к безопасности и выбору мер для поддержки безопасности является оценка рисков и управление рисками.

Средства, включенные в состав системы на этапе разработки, обычно оказываются значительно дешевле в реализации и поддержке, чем средства, включенные во время реализации или после нее.

10.2 Безопасность в прикладных системах

Цель: Предотвратить потери, модификацию и неправомерное использование пользовательских данных в прикладных системах.

В прикладные системы (в том числе и в приложения, разработанные пользователями) должны быть встроены необходимые средства защиты и функции ведения аудиторских записей или журналов операций. Эти средства должны обеспечивать проверку вводимых данных, внутренней обработки и результатов работы.

Для систем, которые обрабатывающих конфиденциальную, ценную и/или критичную информацию или оказывают определенное воздействие на такую информацию, могут потребоваться дополнительные средства защиты. Перечень необходимых средств следует определить на основе требований к безопасности и результатов оценки рисков.

10.2.1 Проверка вводимых данных

Данные, вводимые в прикладные системы, необходимо проверять, чтобы гарантировать их правильность и соответствие поставленной задаче. Проверку должны проходить исходные данные бизнес-транзакций, постоянные данные (имена и адреса, кредитные лимиты, контрольные номера заказчиков) и таблицы параметров (отпускные цены, курсы валют, суммы налогов). Рекомендуется рассмотреть следующие меры:

a) двукратный ввод или другой способ проверки ввода для обнаружения следующих ошибок:

   1) значения, выходящие за допустимый диапазон;

   2) недопустимые символы в полях данных;

   3) отсутствующие или неполные данные;

   4) превышение верхних и нижних пределов объема данных;

   5) несанкционированные или несогласованные управляющие данные;

b) периодический просмотр содержимого ключевых полей и файлов данных для проверки их достоверности и целостности;

c) просмотр документов, введенных с печатных копий, на предмет несанкционированного изменения введенных данных (все изменения во вводимых документах должны санкционироваться);

d) правила реакции на ошибки при проверке;

e) процедуры проверки правдоподобности введенных данных;

f) определение обязанностей всех сотрудников, участвующих в процессе ввода данных.

10.2.2 Контроль обработки информации

10.2.2.1 Области риска

Данные, которые были введены правильно, могут быть повреждены в результате ошибок при обработке или злого умысла. Для обнаружения таких повреждений в систему должны быть встроены функции проверки. Структура приложений должна обеспечивать наличие ограничений, которые уменьшили бы риск ошибок обработки, приводящих к утрате целостности. Вот вопросы, которые следует рассмотреть:

a) использование и размещение в программах функций добавления и удаления данных для внесения изменений в данные;

b) процедуры, предотвращающие запуск программ в неправильном порядке или запуск после сбоя в предыдущей процедуре обработки (см. также раздел 8.1.1);

c) использование нужных программ для восстановления после сбоев, чтобы обеспечить правильную обработку данных.

10.2.2.2 Проверка и контроль

Перечень средств, которые необходимо реализовать, зависит от природы приложения и влияния, которое повреждение данных может оказать на деятельность организации. Ниже приведено несколько примеров проверок, которые необходимо реализовать:

a) средства проверки на уровне сеанса или пакета, позволяющие проверить баланс файлов данных после выполненной транзакции;

b) средства балансировки, обеспечивающие сравнения начального результата с предыдущим конечным результатом, а именно:

1) средства проверки при каждом проходе;

2) проверка итогов обновления файлов;

3) средства проверки результатов работы различных программ;

c) проверка правильности данных, сгенерированных системой (см. раздел 10.2.1);

d) проверка целостности программ и данных, передаваемых между центральным и удаленными компьютерами (см. раздел 10.3.3);

e) контрольные суммы записей и файлов;

f) проверка правильности времени запуска прикладных программ;

g) проверки, позволяющие убедиться в том, что программы запускаются в правильном порядке и прекращают работу в случае сбоев, а дальнейшая обработка не выполняется до тех пор, пока проблема не будет решена.

10.2.3 Аутентификация сообщений

Аутентификация сообщений – это метод, позволяющий обнаружить несанкционированные изменения или повреждение содержимого передаваемых электронных сообщений. Этот метод может быть реализован либо на аппаратном, либо на программном уровне – с помощью физического устройства аутентификации или программного алгоритма.

Аутентификацию сообщений рекомендуется применять в тех областях, безопасность которых требует защиты целостности содержимого сообщения – например, электронное перечисление средств, передача характеристик, контрактов и предложений значительной важности, а также прочие подобные операции обмена электронными данными. Необходимо выполнить оценку рисков, чтобы установить, необходима ли аутентификация сообщений, и определить наиболее подходящий метод реализации.

Аутентификация сообщений не обеспечивает защиту содержимого сообщения от несанкционированного раскрытия. Для реализации аутентификации сообщений можно использовать криптографические методы (см. разделы 10.3.2 и 10.3.3).

10.2.4 Проверка результатов работы

Результаты работы, выдаваемые прикладной системой, необходимо проверять для того, чтобы убедиться, что сохраненная информация была обработана правильно и соответствует всем условиям. Как правило, при разработке систем предполагается, что при принятии соответствующих мер результаты проверки достоверности и тестирования выданных данных всегда будут положительными. Это не всегда так. Проверка результатов работы может включать:

a) проверку правдоподобия, позволяющую убедиться в осмысленности выданных данных;

b) подсчет контрольных сумм, позволяющий убедиться, что данные были обработаны полностью;

c) предоставление достаточного количества данных для того, чтобы читатели или последующие системы обработки смогли определить правильность, полноту, точность и классификацию информации;

d) правила реакции на ошибки при проверке результатов;

e) определение обязанностей всех сотрудников, участвующих в процессе вывода данных.

10.3 Криптографические средства

Цель: Защитить конфиденциальность, подлинность и целостность информации. Криптографические системы и методы следует использовать для защиты информации, которая может подвергаться риску, если другие средства не обеспечивают достаточной защиты.

10.3.1 Политика использования криптографических средств

Принятие решения о том, подходят ли криптографические методы для выбранной цели, должно входить в более широкий процесс оценки рисков и выбора средств. Оценку рисков необходимо выполнить для того, чтобы определить уровень защиты, которого требует информация. Затем по результатам оценки можно определить, подходят ли в данном случае криптографические средства, какие средства необходимо реализовать и для каких целей и бизнес-процессов они будут использоваться.

В организации необходимо разработать политику применения криптографических средств для защиты своей информации. Такая политика необходима для того, чтобы извлечь максимум выгоды и уменьшить риск от использования криптографических методов, а также избежать неправомерного и неправильного использования. При разработке политики необходимо учитывать следующее:

a) отношение руководства к применению криптографических средств в организации, в том числе общие принципы защиты информации, принадлежащей организации;

b) подход методам управления ключевой информацией, в том числе методы восстановления зашифрованной информации в случае утери, компрометирования или повреждения ключей;

c) должности и обязанности, например, назначение сотрудников, ответственных за:

d) реализацию политики;

e) управление ключами;

f) метод определения необходимого уровня криптографической защиты;

g) стандарты, которые должны быть приняты для эффективной реализации во всей организации (соответствие выбранных решений и бизнес-процессов).

10.3.2 Шифрование

Шифрование – это криптографический метод, который можно использовать для защиты конфиденциальности информации. Рекомендуется подумать о применении этого метода для защиты конфиденциальной или критичной информации.

На основе результатов оценки рисков следует определить необходимый уровень защиты с учетом типа и качества выбранного алгоритма шифрования и длины используемых криптографических ключей.

При реализации криптографической политики в организации следует учитывать законы и государственные ограничения в отношении использования криптографических методов, которые могут существовать в разных странах, а также вопросы передачи зашифрованной информации за пределы страны. Кроме того, необходимо рассмотреть вопросы, относящиеся к экспорту и импорту криптографических технологий (см. также раздел 12.1.6).

Чтобы определить необходимый уровень защиты, следует проконсультироваться со специалистом, который поможет выбрать подходящие средства, обеспечивающие нужную защиту и способные поддерживать надежную систему управления ключами (см. также раздел

10.3.5). Кроме того, могут потребоваться консультации юриста в отношении законов и нормативных требований, под действие которых могут попадать выбранные организацией методы шифрования.

10.3.3 Цифровые подписи

Цифровые подписи – это средство защиты подлинности и целостности электронных документов. Их можно использовать, например, в электронной коммерции, чтобы проверять, кто подписал электронный документ, и не изменилось ли содержимое подписанного документа.

Цифровые подписи могут применяться к любым типам документов, обрабатываемым в электронном виде. Их можно использовать, например, для заверения электронных платежей, передачи средств, контрактов и соглашений. Систему цифровых подписей можно реализовать с помощью криптографического метода, основанного на использовании пары ключей, взаимосвязанных уникальным образом. При этом один ключ используется для создания подписи (секретный ключ), а другой – для ее проверки (открытый ключ).

Необходимо тщательно следить за конфиденциальностью секретного ключа. Этот ключ должен храниться в тайне, поскольку любой, кто получит доступ к этому ключу, сможет подписывать документы (счета, контракты и т. п.), подделывая подпись владельца ключа. Кроме того, необходимо защитить целостность открытого ключа. Подобная защита обеспечивается с помощью сертификатов открытого ключа (см. раздел 10.3.5).

Необходимо подумать о типе и качестве алгоритма создания подписей и длине используемых ключей. Криптографические ключи, используемые для цифровых подписей, должны отличаться от ключей, используемых для шифрования (см. раздел 10.3.2).

При использовании цифровых подписей необходимо учитывать законы, описывающие условия, согласно которым цифровая подпись имеет юридическую силу. Например, в области электронной коммерции необходимо знать юридическую силу цифровых подписей. Если условий действующего законодательства недостаточно, для поддержки использования цифровых подписей могут потребоваться договора или другие соглашения. Необходимо получить консультацию юриста по поводу законов и нормативных актов, которые могут относиться к выбранным организацией способам применения цифровых подписей.

10.3.4 Обеспечение неотказуемости

Средства, обеспечивающие неотказуемость, могут потребоваться при разрешении споров о том, имело ли место какое-либо событие или действие – например, при возникновении спора, относящегося к использованию электронной подписи или платежу. Эти средства могут помочь в получении улик, убедительно доказывающих, что какое-либо событие или действие имело место, например, отказ от отправки инструкции с цифровой подписью по электронной почте. Данные средства основаны на применении шифрования и цифровых подписей (см. также разделы 10.3.2 и 10.3.3).

10.3.5 Управление ключами

10.3.5.1 Защита криптографических ключей

Средства управления криптографическими ключами необходимы для эффективного применения криптографических методов. Компрометирование или потеря криптографических ключей может привести к нарушению конфиденциальности, подлинности и/или целостности информации. В организации необходимо создать систему управления, способную поддерживать применение криптографических методов двух типов, а именно:

a) методы с секретным ключом, в которых две или более сторон обладают одним и тем

же ключом, который используется и для шифрования, и для расшифровки информации. Этот ключ держится в секрете, поскольку любой, кто имеет доступ к нему, может расшифровать всю информацию, зашифрованную с его помощью, или ввести в систему несанкционированную информацию;

b) методы с открытым ключом, при использовании которых у каждого пользователя имеется пара ключей – открытый ключ (который можно передавать любому) и закрытый ключ (который должен храниться в тайне). Методы с открытым ключом можно использовать для шифрования (см. раздел 10.3.2) и для создания цифровых подписей (см. раздел 10.3.3).

Все ключи должны иметь защиту от модификации и уничтожения. Секретные и закрытые ключи должны быть защищены от несанкционированного раскрытия. Для этой цели можно также использовать криптографические методы. Оборудование, используемое для создания, хранения и архивирования ключей, должно быть защищено физически.

10.3.5.2 Стандарты, процедуры и методы

Система управления ключами должна быть основана на согласованном наборе стандартов, процедур и безопасных методов для выполнения следующих задач:

a) создание ключей для различных криптографических систем и различных областей применения;

b) создание и получение сертификатов открытых ключей;

c) передача ключей нужным пользователям вместе с инструкциями о том, как активизировать ключ после получения;

d) хранение ключей и инструкции по получению ключей для авторизованных пользователей;

e) смена или обновление ключей, а также правила, оговаривающие сроки и методы смены ключей;

f) действия в отношении скомпрометированных ключей;

g) аннулирование ключей, в том числе методы отзыва или деактивации ключей, например, в том случае, если ключ был скомпрометирован или если его владелец покидает организацию (в данном случае ключ также необходимо архивировать);

h) восстановление потерянных или поврежденных ключей для поддержки непрерывности бизнеса, например, для восстановления зашифрованной информации;

i) архивирование ключей, например, для архивов и резервных копий информации;

j) уничтожение ключей;

k) ведение журналов и аудит действий, связанных с управлением ключами.

Чтобы уменьшить вероятность компрометирования, для ключей необходимо определить даты начала и конца действия, чтобы их можно было использовать лишь в течение ограниченного срока. Этот срок должен зависеть от условий, при которых используется криптографическое средство, и от возможного риска.

Может потребоваться разработка правил реакции на юридические запросы о доступе к криптографическим ключам (например, может возникнуть необходимость предоставить зашифрованную информацию в незашифрованном виде в качестве улики на суде).

Помимо вопросов безопасности закрытых и секретных ключей, необходимо подумать также и о защите открытых ключей. Существует опасность, что злоумышленник сможет подделать цифровую подпись, заменив открытый ключ пользователя на свой собственный. Решить эту

проблему можно с помощью сертификатов открытого ключа. Эти сертификаты должны создаваться таким способом, чтобы информация, относящаяся к владельцу пары «открытый-закрытый ключ», была уникальным образом связана с открытым ключом. Поэтому очень важно, чтобы на управляющий процесс, используемый для генерации этих сертификатов, можно было положиться. Этот процесс обычно выполняется удостоверяющим центром, который должен быть известной организацией, обладающей необходимыми средствами и процедурами для того, чтобы обеспечить нужную степень доверия.

Соглашения с внешними поставщиками криптографических услуг (например, с удостоверяющими центрами) об уровне предоставляемого сервиса должны охватывать вопросы ответственности, надежности сервиса и времени реакции при предоставлении сервиса (см. раздел 4.2.2).

10.4 Безопасность системных файлов

Цель: Гарантировать безопасность выполнения проектов в области информационных технологий и сопутствующих операций. Доступ к системным файлам должен контролироваться.

Поддержка целостности системы должна входить в обязанности пользователей или группы разработки, которым принадлежит прикладная система или программа.

10.4.1 Контроль используемого программного обеспечения

Необходимо обеспечить контроль над внедрением программного обеспечения в рабочих системах. Чтобы свести к минимуму риск повреждения программного обеспечения, рекомендуется рассмотреть следующие меры:

a) Обновление библиотек программного обеспечения должно выполняться только назначенным библиотекарем после соответствующего разрешения руководства (см. раздел 10.4.3).

b) По возможности программное обеспечение должны включать в себя только исполняемый код.

c) Исполняемый код должен включаться в состав программного обеспечения только после получения подтверждения успешного тестирования и приемки пользователями и обновления необходимых библиотек исходного кода программ.

d) Необходимо вести контрольный журнал всех обновлений библиотек программного обеспечения.

e) Предыдущие версии программ необходимо сохранять на случай непредвиденных обстоятельств.

Уровень поддержки используемого программного обеспечения, предоставленного другими поставщиками, должен соответствовать требованиям поставщиков. Любое решение о переходе на новую версию должно приниматься с учетом безопасности этой версии (например, с учетом появления новых функций защиты или количества и серьезности проблем с безопасностью, которыми отличается эта версия). Программные исправления необходимо устанавливать в том случае, если они помогут устранить уязвимости или уменьшить их серьезность.

Физический или логический доступ должен предоставляться представителям поставщика только для поддержки и с разрешения руководства. Действия представителей поставщика должны происходить под надзором.

10.4.2 Защита данных, используемых для тестирования

Тестовые данные должны находиться под контролем и защитой. Для системных и приемочных испытаний обычно требуются значительные объемы тестовых данных, максимально близко соответствующих рабочим данным. Необходимо избегать использования рабочих баз данных, содержащих личную информацию. Если подобная информация все же будет использоваться, перед использованием ее необходимо обезличить. Для защиты рабочих данных, используемых при тестировании, должны применяться перечисленные ниже меры.

a) Процедуры контроля доступа, применяемые для рабочих прикладных систем, должны применяться также и для тестовых прикладных систем.

b) На каждое копирование рабочей информации в тестовую прикладную систему необходимо получать отдельное разрешение.

c) Рабочая информация должна стираться из тестовой прикладной системы сразу же после завершения тестирования.

d) Сведения о копировании и использовании рабочей информации должны заноситься в контрольный журнал.

10.4.3 Контроль доступа к библиотекам исходного кода программ

Чтобы уменьшить вероятность нарушения работы программ, необходимо строго ограничить доступ к библиотекам исходного кода программ, как описано ниже (см. также раздел 8.3).

a) По возможности библиотеки исходного кода программ не должны входить в состав рабочих систем.

b) Для каждого приложения необходимо назначить библиотекаря, ответственного за программы.

c) Специалисты по поддержке информационных технологий не должны иметь неограниченного доступа к библиотекам исходного кода программ.

d) Программы, находящиеся на стадии разработки или сопровождения, не должны храниться в библиотеках исходного кода рабочих систем.

e) Обновление библиотек исходного кода программ и предоставление исходного кода программистам должно осуществляться только назначенным библиотекарем после получения разрешения руководителя отдела информационных технологий, ответственного за соответствующую программу.

f) Листинги программ должны храниться с соблюдением мер защиты (см. раздел 8.6.4).

g) Все случаи доступа к библиотекам исходного кода программ должны заноситься в контрольный журнал.

h) Старые версии исходного кода должны архивироваться с четким указанием точной даты и времени для того периода, когда они использовались в работе. К ним должны прилагаться все необходимые вспомогательные программы, средства контроля, описания структур данных и инструкции.

i) Поддержка и копирование библиотек исходного кода программ должны происходить в строгом соответствии с правилами контроля изменений (см. раздел 10.5.1).

10.5 Безопасность при разработке и поддержке

Цель: Обеспечить безопасность прикладных программ и информации.

Среды, в которых происходит проектирование и поддержка, должны находиться под строгим контролем.

Руководители, ответственные за прикладные системы, должны также нести ответственность за среды проектирования или поддержки. Они должны обеспечить контроль всех предлагаемых изменений в системе, чтобы гарантировать, что эти изменения не нарушат безопасность системы или среды эксплуатации.

10.5.1 Правила управления внесением изменений

Чтобы свести вероятность повреждения информационных систем к минимуму, следует ввести строгий контроль над внесением изменений. Необходимо установить официальные правила управления внесением изменений. Эти правила должны гарантировать, что процедуры, связанные с безопасностью и контролем, не будут нарушены, что программисты, занимающиеся поддержкой, получают доступ только к тем частям системы, которые необходимы для их работы, и что для выполнения любого изменения требуется получить официальное разрешение и подтверждение. Внесение изменений в прикладные программы может повлиять на рабочую среду. По возможности процедуры управления внесением изменений в системном и прикладном программном обеспечении должны быть объединены (см. также раздел 8.1.2). Эти правила должны включать следующее:

a) запись сведений о согласованных уровнях авторизации;

b) возможность внесения изменений только авторизованными пользователями;

c) проверка процедур контроля и поддержки целостности, гарантирующая, что изменения не приведут к их нарушению;

d) определение всех компьютерных программ, информации, записей баз данных и аппаратных компонентов, которые потребуют изменения;

e) получение официального одобрения подробно описанных предложений до начала работ;

f) возможность начала реализации только после того, как авторизованный пользователь подтвердит предложенные изменения;

g) процедуры реализации, оказывающие минимальное влияние на деятельность организации;

h) гарантия обновления системной документации по завершении каждого обновления и архивирование или утилизация старой документации;

i) поддержка управления версиями для всех обновлений программного обеспечения;

j) ведение аудиторских записей для всех запросов об изменении;

k) гарантия внесения необходимых изменений в рабочую документацию (см. раздел 8.1.1) и правила работы;

l) гарантия внесения изменений в правильное время и без нарушения организационных процессов, к которым они относятся.

Во многих организациях имеется среда, в которой пользователи могут протестировать новые программы. Эта среда должна быть отделена от среды разработки и основной деятельности. Это помогает обеспечить контроль над новым программным обеспечением и ввести

дополнительную защиту рабочей информации, используемой для тестирования.

10.5.2 Техническая проверка изменений в операционной системе

Время от времени в операционную систему приходится вносить изменения, например, устанавливать новые версии программ или обновления. После таких изменений необходимо проверять и тестировать систему, чтобы убедиться в отсутствии нарушения безопасности или эффективности работы. Данный процесс должен включать в себя следующие меры:

a) после внесения изменений в операционную систему должна производиться проверка процедур контроля и поддержки целостности в приложениях, позволяющая убедиться в отсутствии нарушений;

b) необходимо убедиться, что годичный план поддержки и бюджет включает в себя проверку и тестирование после внесения изменений в операционную систему;

c) необходимо обеспечить своевременное уведомление об изменениях в операционной системе, чтобы соответствующие проверки могли быть выполнены до начала реализации;

d) необходимо внести соответствующие изменения в план поддержки непрерывности бизнеса (см. раздел 11).

10.5.3 Ограничения на изменения в программных пакетах

Постарайтесь избежать внесения изменений в программные пакеты. До тех пор, пока это возможно и применимо на практике, предоставленные поставщиками программные пакеты должны использоваться без изменений. Если обойтись без модификации программного пакета все же не удается, необходимо рассмотреть следующие вопросы:

a) риск нарушения встроенных средств поддержки безопасности и целостности;

b) необходимость в получении разрешения поставщика;

c) возможность получения версии с необходимыми изменениями от поставщика в качестве стандартного обновления программы;

d) последствия того, что в результате изменений будущая поддержка программного пакета может оказаться обязанностью самой организации.

Если обойтись без изменений не удастся, необходимо сохранить исходную версию программного обеспечения и внести изменения в четко определенную копию. Все изменения должны быть полностью протестированы и документированы, чтобы их можно было внести заново при обновлении программ в будущем.

10.5.4 «Черные ходы» и троянский код

Наличие «черных ходов» может привести к косвенному и незаметному раскрытию информации. Такой канал может быть активизирован в результате изменения параметра, доступного как защищенным, так и не защищенным элементам компьютерной системы, или в результате встраивания информации в поток данных. Троянский код выполняет в системе неразрешенные действия, которые могут быть незаметными и ненужными получателю или пользователю программы. Черные ходы и троянские программы не возникают случайно. Если существует вероятность наличия черных ходов и троянского кода, необходимо рассмотреть следующие меры:

a) приобретение программ только у поставщиков с хорошей репутацией;

b) приобретение программ в виде исходного кода (чтобы иметь возможность проверить

этот код);

c) использование программ, прошедших предварительную оценку;

d) просмотр всего исходного кода перед введением в эксплуатацию;

e) контроль доступа к коду и его модификации после установки;

f) предоставление доступа к наиболее важным системам только тем сотрудникам, на которых можно положиться.

10.5.5 Разработка программ внешним разработчиком

Если программное обеспечение разрабатывается по заказу внешним разработчиком, необходимо подумать о следующем:

a) лицензионные соглашения, права владения кодом и права на интеллектуальную собственность (см. раздел 12.1.2);

b) сертификация качества и правильности выполненной работы;

c) соглашения о разрешении претензий со стороны третьих лиц;

d) права доступа для оценки качества и правильности выполненной работы;

e) зафиксированные в контракте требования к качеству кода;

f) тестирование перед установкой на предмет наличия троянского кода.

11 Обеспечение непрерывности бизнеса

11.1 Аспекты обеспечения непрерывности бизнеса

Цель: Противостоять нарушению деятельности организации и защитить важные процессы от воздействия крупных сбоев и бедствий.

Процесс поддержки непрерывности бизнеса необходимо реализовать для того, чтобы уменьшить негативное влияние бедствий и нарушений безопасности (которые могут быть, например, результатами стихийных бедствий, случайностей, отказа оборудования и преднамеренный действий) с помощью сочетания профилактических и восстановительных мер.

Последствия бедствий, нарушений безопасности и прекращения работы сервисов необходимо анализировать.

Следует разработать и реализовать планы действия в нештатных ситуациях, гарантирующие, что деятельность организации можно будет восстановить за необходимый отрезок времени.

Подобные планы должны поддерживаться в актуальном состоянии и стать неотъемлемой частью всех прочих процессов управления. Поддержка непрерывности бизнеса должна включать в себя меры для определения и уменьшения рисков, уменьшение негативных последствий инцидентов и своевременного возобновления важных операций.

11.1.1 Процесс обеспечения непрерывности бизнеса

Необходимо разработать контролируемый процесс для обеспечения и поддержки непрерывности бизнеса во всей организации. Данный процесс должен объединять в себе основные элементы поддержки непрерывности бизнеса, перечисленные ниже:

a) определение степени риска, с которым сталкивается организация, с учетом вероятности и негативных последствий инцидентов, плюс определение и установка приоритетов наиболее важных бизнес-процессов;

b) определение последствий нарушения работы для деятельности организации (важно найти решения, пригодные для устранения последствий мелких инцидентов, а также решения для серьезных инцидентов, которые могут угрожать жизнеспособности всей организации) и установка назначения средств обработки информации;

c) рассмотрение возможности приобретения страховых полисов, которые могут стать частью процесса поддержки непрерывности бизнеса;

d) разработка и документирование стратегии поддержки непрерывности бизнеса, соответствующей установленным целям и приоритетам в деятельности организации;

e) разработка и документирование планов поддержки непрерывности бизнеса в соответствии с принятой стратегией;

f) регулярное тестирование и обновление реализованных планов и процессов;

g) внедрение мер по поддержке непрерывности бизнеса в процессы и структуры организации. Обязанности по координации процесса поддержки непрерывности бизнеса должны быть распределены в организации на соответствующем уровне, например, в совете по управлению информационной безопасностью (см. раздел 4.1.1).

11.1.2 Непрерывность бизнеса и анализ ущерба

Поддержка непрерывности бизнеса должна начинаться с определения событий, которые могут нарушить деятельность организации (поломка оборудования, наводнения, пожары и т. п.). Затем необходимо провести оценку рисков, чтобы определить ущерб от подобных нарушений (как степень повреждений, так и время, которое потребуется на восстановление). Оба этих процесса должны происходить при непосредственном участии владельцев ресурсов и процессов, используемых в деятельности организации. Оценка должна включать в себя все области деятельности организации и не ограничиваться средствами обработки информации.

На основе результатов оценки рисков необходимо разработать стратегический план, позволяющий определить общий подход к поддержке непрерывности бизнеса. После создания такой план должен быть одобрен руководством.

11.1.3 Разработка и внедрение планов обеспечения непрерывности

Необходимо разработать планы по поддержке и восстановлению деятельности организации за определенный отрезок времени после сбоев и нарушений важных процессов. При разработке планов поддержки непрерывности бизнеса нужно учитывать следующее:

a) определение и согласование всех обязанностей и планов действия в нештатных ситуациях;

b) реализация планов действия в нештатных ситуациях, позволяющих устранить повреждения и возобновить работу за необходимый отрезок времени. Особое внимание необходимо уделить оценке зависимости от внешних процессов и действующих контрактов;

c) документирование согласованных процедур и правил;

d) ознакомление сотрудников с согласованными планами действия в нештатных ситуациях и процессами реагирования на кризисы;

e) тестирование планов и внесение необходимых изменений.

При планировании необходимо сконцентрироваться на основных целях организации, например, на возобновлении предоставления определенных услуг клиентам за приемлемый отрезок времени. Необходимо учитывать сервисы и ресурсы, которые потребуются для этого, в том числе кадровое обеспечение, ресурсы, не связанные с обработкой информации, а также варианты аварийного восстановления для средств обработки информации.

11.1.4 Структура планирования обеспечения непрерывности бизнеса

Необходимо создать единую структуру планов поддержки непрерывности бизнеса, чтобы гарантировать согласованность всех планов и определить приоритеты в области тестирования и технического обслуживания. В каждом плане поддержки непрерывности бизнеса должны быть четко указаны условия начала его исполнения и сотрудники, ответственные за выполнение каждого фрагмента плана. При появлении новых требований необходимо внести поправки в принятые планы действия в нештатных ситуациях, например, в планы эвакуации или соглашения об использовании альтернативных средств.

При разработке структуры планов поддержки непрерывности бизнеса необходимо учитывать следующее:

a) условия активизации планов, включающие необходимые действия (оценка ситуации, участвующий персонал и т. п.), которые должны быть выполнены перед тем, как привести план в действие;

b) планы действия в нештатных ситуациях, описывающие действия, которые необходимо выполнить после инцидента, угрожающего деятельности организации и/или человеческим жизням. Сюда должны входить инструкции для отдела по связям с общественностью и рекомендации по обращению в органы государственной власти (правоохранительные органы, пожарную охрану, органы местного самоуправления и т. п.);

c) правила аварийного восстановления, описывающие действия по переносу основных областей деятельности или вспомогательных служб на альтернативные временные участки и по возобновлению деятельности организации в установленные сроки;

d) правила возобновления деятельности, описывающие действия по возврату к нормальной деятельности организации;

e) график профилактического обслуживания, определяющий время и условия тестирования плана и процесс поддержки плана;

f) действия по ознакомлению и обучению, в результате которых сотрудники должны получить представление о процессе поддержки непрерывности бизнеса и обеспечить сохранение эффективности этого процесса;

g) ответственность отдельных сотрудников (обязанности каждого сотрудника по выполнению отдельных фрагментов плана). По мере необходимости могут указываться альтернативные варианты.

Для каждого плана должен быть назначен определенный владелец. Правила действия в нештатных ситуациях, планы ручного аварийного восстановления и планы возобновления деятельности должны находиться в ведении владельцев соответствующих ресурсов или процессов, к которым они имеют отношение. Планы о переходе на альтернативные варианты, относящиеся к техническим службам, например, к средствам обработки информации и передачи данных, обычно находятся в ведении поставщиков услуг.

11.1.5 Тестирование, поддержка и повторная оценка планов обеспечения непрерывности бизнеса

11.1.5.1 Тестирование планов

При тестировании может выясниться, что планы поддержки непрерывности бизнеса оказались неудачными. Зачастую это происходит из-за неверных предположений, недосмотра или кадровых и технических изменений. Таким образом, необходимо регулярно тестировать планы, чтобы гарантировать их эффективность и соответствие текущим условиям. Кроме того, подобные тесты помогут убедиться, что все члены группы реагирования и прочие задействованные сотрудники знакомы с планами.

В графике тестирования планов поддержки непрерывности бизнеса должна содержаться информация о том, когда и как будет тестироваться каждый элемент плана. Рекомендуется регулярно тестировать отдельные компоненты планов. Чтобы гарантировать работоспособность плана в реальной ситуации, следует применять самые различные методы. Вот некоторые варианты:

a) теоретическое тестирование различных сценариев (обсуждение методов восстановления на примерах инцидентов);

b) имитация (в частности, для обучения сотрудников правилам работы в случаях инцидентов и кризисов);

c) тестирование восстановления технических средств (проверка эффективности восстановления информационных систем);

d) тестирование восстановления на альтернативном участке (выполнение деятельности организации за пределами основной территории параллельно с восстановлением)

e) тестирование средств и сервисов, предоставляемых поставщиками (проверка соответствия предоставляемых сервисов и средств условиям контракта);

f) учебные тревоги (проверка того, смогут ли организация, персонал, оборудование, средства и процессы справиться с инцидентами).

Эти методы можно использовать в любой организации. Они должны применяться в соответствии с условиями конкретного плана восстановления.

11.1.5.2 Поддержка и повторная оценка планов

Поддержка планов непрерывности бизнеса должна заключаться в регулярной проверке и обновлении для гарантии их постоянной эффективности (см. разделы 11.1.5.1–11.1.5.3). В программу управления изменениями в организации необходимо включить процедуры, гарантирующие правильное отношение к вопросам поддержки непрерывности бизнеса.

Необходимо распределить обязанности по регулярной проверке каждого плана поддержки непрерывности бизнеса. Если в деловых соглашениях будут обнаружены перемены, которые еще не отражены в планах поддержки непрерывности, планы необходимо соответствующим образом изменить. Этот официальный процесс контроля изменений должен гарантировать распространение и обновление измененных планов путем регулярной проверки общего плана.

Обновление планов может потребоваться при приобретении нового оборудования, при модернизации программных систем и при изменениях в следующих областях:

a) штат сотрудников;

b) адреса или номера телефонов;

c) стратегия организации;

d) расположение средств и ресурсов;

e) законодательство;

f) подрядчики, поставщики и основные клиенты;

g) процессы (включая добавление или отказ от каких-либо процессов)

h) риск (эксплуатационный и финансовый).

12 Соответствие требованиям

12.1 Соответствие требованиям законодательства

Цель: Избежать нарушений, связанных с гражданским и уголовным правом, требованиями законов и нормативных актов, обязательствами по контрактам и требованиями к безопасности.

Разработка, эксплуатация и управление информационными системами может попадать под действие требований к безопасности, определенных в законах, нормативных актах и контрактах. Необходимо обратиться к юрисконсультам организации или имеющим необходимую квалификацию юристам, чтобы получить консультации по вопросам, связанным с законодательством. Требования законодательства могут отличаться в различных странах и при передаче информации, созданной в одной стране, в другую страну (т. е. при передаче данных через границы).

12.1.1 Определение применяемого законодательства

Для каждой информационной системы необходимо четко определить и задокументировать все имеющие к ней отношение требования законов, нормативных актов и контрактов. Подобным образом необходимо определить и задокументировать конкретные меры и обязанности отдельных сотрудников по соблюдению этих требований.

12.1.2 Права интеллектуальной собственности

12.1.2.1 Авторское право

Необходимо реализовать процедуры, обеспечивающие соответствие законодательным ограничениям на использование материалов, на которые могут распространяться права интеллектуальной собственности (авторское право, право разработки, торговые марки и т. п.). Нарушение авторского права может привести к правовым действиям, в том числе и к уголовному преследованию.

Требования законов, нормативных актов и контрактов могут налагать ограничения на копирование материалов, являющихся интеллектуальной собственностью. В частности, эти требования могут разрешать использование только тех материалов, которые были разработаны в самой организации, лицензированы или предоставлены организации разработчиками.

12.1.2.2. Авторские права на программное обеспечение

Программные продукты, являющиеся предметом интеллектуальной собственности, обычно распространяются на основе лицензионного соглашения, которое ограничивает использование этих продуктов отдельными компьютерами и может разрешать копирование только для создания резервных копий. Рекомендуется рассмотреть следующие меры:

a) публикация политики соблюдения авторских прав на программное обеспечение, определяющей законное использование программных и информационных продуктов;

b) разработка стандартных правил приобретения программных продуктов;

c) требования к соблюдению авторских прав и правил приобретения программного обеспечения и применение дисциплинарных взысканий к сотрудникам, нарушающим их;

d) поддержка необходимых перечней ресурсов;

e) сохранения доказательств прав владения лицензиями, основными дисками, документацией и т. п.

f) реализация мер, предотвращающих превышение максимально допустимого числа пользователей;

g) выполнение проверок, гарантирующих установку только разрешенных и лицензированных программных продуктов;

h) разработка политики по соблюдению условий лицензий;

i) разработка политики по утилизации программного обеспечения и его передаче другим сторонам;

j) использование необходимых средств контроля;

k) обеспечение соответствия условиям применения программ и данных, полученных из общественных сетей (см. также раздел 8.7.6).

12.1.3 Защита документов организации

Важные документы, принадлежащие организации, должны иметь защиту от утраты, повреждения и фальсификации. Некоторые документы должны храниться с соблюдением норм безопасности для того, чтобы обеспечить соответствие требованиям законов и нормативных актов, а также поддержать важные области деятельности организации. Примером могут послужить документы, которые могут потребоваться для доказательства того факта, что организация выполняет все требования законов и нормативных актов, для защиты от административного или уголовного преследования, или для подтверждения финансового статуса организации по просьбе акционеров, партнеров и аудиторов. Период хранения и содержание хранимой информации могут устанавливаться законами или нормативными актами.

Документы необходимо классифицировать по типу (например, бухгалтерские записи, записи баз данных, журналы транзакций, контрольные журналы и правила эксплуатации). Для каждой записи необходимо указать период хранения и тип носителя (например, бумага, микрофильм, магнитный или оптический диск). Все криптографические ключи, относящиеся к зашифрованным архивам или цифровым подписям (см. разделы 10.3.2 и 10.3.3) должны храниться в секрете и при необходимости предоставляться авторизованным лицам.

Необходимо учитывать возможность ухудшения качества носителей, используемых для хранения документов. Процедуры хранения и обращения должны разрабатываться в соответствии с рекомендациями производителя.

При выборе электронных средств хранения необходимо разработать процедуры, гарантирующие возможность доступа к данным (читаемость носителей и совместимость форматов) в течение всего периода хранения, чтобы избежать потерь информации в связи с изменением технологии в будущем.

Системы хранения данных необходимо выбирать так, чтобы необходимые данные можно было получить с соблюдением требований, предъявляемых судебными органами (например, должна быть возможность получить все необходимые записи за определенный период времени и в подходящем формате).

Система хранения и обработки должна обеспечивать четкую идентификацию записей и их

периода хранения в соответствии с требованиями законов и нормативных актов. Эта система должна иметь возможность уничтожения записей по истечении периода хранения, если эти записи больше не требуются организации.

Чтобы обеспечить соответствие перечисленным требованиям, необходимо принять в организации следующие меры:

a) разработка правил хранения, обработки и утилизации записей и информации;

b) разработка графика хранения, определяющего типы необходимых записей и период времени, в течение которого они должны храниться;

c) поддержка перечня источников важной информации;

d) введение необходимых мер для защиты важных записей и информации от утраты, нарушения и фальсификации.

12.1.4 Защита данных и сохранение тайны персональных данных

В ряде стран приняты законы, ограничивающие обработку и передачу персональных данных (как правило, информации о живых людях, которых можно идентифицировать с помощью этой информации). Подобные законы могут определять полномочия, связанные со сбором, обработкой и распространением персональных данных, и ограничивать возможности передачи такой информации в другие страны.

Для того, чтобы обеспечить соответствие законам о защите данных, необходимо разработать соответствующую структуру управления и контроля. Наилучших результатов зачастую удается добиться путем назначения специалиста по защите данных, который должен консультировать руководителей, пользователей и поставщиков услуг по вопросам их личных обязанностей и правил, которые необходимо соблюдать. Владелец данных должен сам информировать специалиста по защите данных о любых предложениях, относящихся к хранению личной информации в структурированных файлах, и обеспечивать соблюдение принципов защиты данных, сформулированных в соответствующих законах.

12.1.5 Предотвращение неправомерного использования средств обработки информации

Средства обработки информации в организации предназначены для поддержки деятельности организации. Использование этих средств должно санкционироваться руководством. Любое использование этих средств непредусмотренным способом или в целях, не связанных с деятельностью организации, без соответствующего разрешения руководства должно считаться неправомерным. Если подобные действия будут обнаружены при мониторинге или другим способом, об этом следует уведомить соответствующего представителя руководства, ответственного за необходимые дисциплинарные взыскания.

Законодательные требования к подобному мониторингу в различных странах могут отличаться. В некоторых случаях может возникнуть необходимость предупредить сотрудников о мониторинге или получить их согласие. Перед тем, как приступать к реализации средств мониторинга, необходимо получить консультацию юриста.

В некоторых странах приняты или разрабатываются законы, которые должны предотвратить неправомерное использование компьютеров. Использование компьютера в неразрешенных целях может считаться уголовным преступлением. В связи с этим необходимо уведомить всех пользователей о точных границах разрешенной им деятельности. К примеру, для этого можно выдавать пользователям письменные разрешения, копии которых должны быть подписаны пользователями и должны храниться в организации с соблюдением норм безопасности. Сотрудников организации и сторонних пользователей следует уведомить о запрете на любые

действия, на которые не получено явного разрешения.

При входе в систему на экране компьютера должно появляться предупреждающее сообщение о том, что система, к которой подключается пользователь, является закрытой, и несанкционированный доступ к ней запрещен. Чтобы продолжить процесс входа в систему, пользователь должен будет подтвердить согласие с этим сообщением.

12.1.6 Ограничения на использование криптографических средств

В некоторых странах приняты законы, нормативные акты или другие документы, ограничивающие применение криптографических средств или доступ к ним. Ограничения могут включать:

a) импорт и/или экспорт криптографического компьютерного оборудования и программного обеспечения;

b) импорт и/или экспорт компьютерного оборудования и программного обеспечения, рассчитанного на включение в него криптографических функций;

c) требования по предоставлению доступа государственным организациям к информации, зашифрованной с помощью аппаратных или программных средств.

Необходимо получить консультацию у юриста, чтобы обеспечить соответствие действующему законодательству. Кроме того, консультацию у юриста необходимо получить также и перед перемещением зашифрованной информации или криптографических средств в другие страны.

12.1.7 Сбор улик

12.1.7.1 Правила использования улик

Для того, чтобы поддержать обвинение в отношении какого-либо человека или организации, необходимы соответствующие улики. Если обвинение связано с внутренним дисциплинарным взысканием, необходимые улики определяются внутренними процедурами.

Если обвинение относится к области права (гражданского или уголовного), предъявленные улики должны соответствовать правилам предъявления улик, сформулированным в соответствующем законе, или правилам, принятым в суде, в котором будет слушаться дело. В большинстве случаев эти правила определяют:

a) достоверность улики: возможность использования улики в суде;

b) совокупность улик: качество и полноту улик;

c) свидетельства правильности и согласованности работы систем (например, сведения о контроле процессов) в течение периода хранения и обработки улик в системе.

12.1.7.2 Достоверность улики

Чтобы обеспечить достоверность улики, организация должна гарантировать, что ее информационные системы соответствуют всем опубликованным стандартам и правилам работы, относящимся к получению достоверных улик.

12.1.7.3 Качество и полнота улик

Чтобы обеспечить качество и полноту улик, необходимы убедительные доказательства получения улик. Как правила, для получения убедительных доказательств должны соблюдаться следующие условия:

a) Для документов на бумаге: оригинал хранился защищенным образом; существуют записи о том, кто обнаружил его, где и когда он был обнаружен и кто был свидетелем обнаружения. Расследования должны показать, что оригиналы не были подделаны.

b) Для информации на компьютерных носителях: необходимо создавать копии всех съемных носителей и информации на жестких дисках и в памяти, чтобы обеспечить ее доступность. Все действия в процессе копирования должны подробно регистрироваться в журнале и происходить в присутствии свидетелей. Одну копию носителя и журнала необходимо хранить защищенным образом.

При первом обнаружении инцидента может быть неочевидно, что он может привести к судебному преследованию. Таким образом, существует опасность, что необходимые улики будут случайно уничтожены до того, как серьезность инцидента будет осознана. При возможности судебных действий рекомендуется как можно раньше обратиться к юристам или в правоохранительным органам и получить консультации о том, какие улики потребуются.

12.2 Проверка политики безопасности и соответствие техническим требованиям

Цель: Обеспечить соответствие систем принятым в организации политикам безопасности и стандартам.

Безопасность информационных систем необходимо регулярно контролировать.

Такая проверка должна осуществляться в соответствии с действующими политиками безопасности. Технические платформы и информационные системы необходимо проверять на соответствие стандартам реализации безопасности.

12.2.1 Соответствие политике безопасности

Руководство должно обеспечить правильное выполнение всех связанных с безопасностью процедур, которые находятся в их ведении. Кроме того, все области деятельности организации должны проходить регулярную проверку на предмет соответствия политикам безопасности и стандартам. Проверка должна охватывать:

a) информационные системы;

b) поставщиков систем;

c) владельцев информации и информационных ресурсов;

d) пользователей;

e) руководство.

Владельцы информационных систем (см. раздел 5.1) должны способствовать регулярной проверке соответствия своих систем политикам безопасности, стандартам и прочим требованиям к безопасности. Методы мониторинга систем во время эксплуатации описаны в разделе 9.7.

12.2.2 Проверка соответствия техническим требованиям

Информационные системы необходимо регулярно проверять на предмет соответствия стандартам реализации безопасности. Проверка на соответствие техническим требованиям включает в себя анализ рабочих систем, позволяющий убедиться в правильности внедрения аппаратных и программных средств. Для данного типа проверки необходима помощь технических специалистов. Эта проверка должна выполняться вручную опытным системным инженером (при необходимости с использованием соответствующих программных средств) или с помощью автоматического программного пакета, создающего отчет, который в дальнейшем будет анализироваться техническим специалистом.

В дополнение к этому проверка соответствия включает в себя проверку возможности

проникновения, которая может выполняться независимыми экспертами, приглашенными специально для этой цели. Этот метод может помочь обнаружить уязвимости в системе и проверить эффективность средств защиты от несанкционированного доступа с учетом найденных уязвимостей. Необходимо соблюдать осторожность, поскольку успешное выполнение проверки на возможность проникновения может привести к нарушению безопасности системы и непреднамеренной эксплуатации других уязвимостей.

Проверка на соответствие техническим требованиям должна выполняться только компетентными авторизованными сотрудниками или под их наблюдением.

12.3 Рекомендации по аудиту систем

Цель: Увеличить эффективность и уменьшить помехи в работе, связанные с процессом ревизии системы.

Необходимо разработать меры для защиты рабочих систем и средств аудита во время его выполнения.

В дополнение к этому необходимы средства для защиты целостности и предотвращения неправомерного использования средств аудита.

12.3.1 Средства аудита систем

Требования к проверке и действия по проверке рабочих систем необходимо тщательно запланировать и согласовать, чтобы свести к минимуму риск нарушения деятельности организации. Рекомендуется рассмотреть следующие меры:

a) Требования по аудиту должны быть согласованы с руководством.

b) Необходимо согласовать область аудита и обеспечить ее контроль.

c) При ревизии доступ к данным и программам должен ограничиваться только чтением.

d) Доступ, предполагающий не только чтение, должен быть разрешен только для изолированных копий системных файлов, которые должны быть удалены после завершения аудита.

e) Необходимо четко определить информационные ресурсы, предназначенные для проведения аудита, и обеспечить их доступность.

f) Необходимо определить и согласовать требования к специальной или дополнительной обработке.

g) Необходимо отслеживать и регистрировать все сеансы доступа с целью создания контрольных записей.

h) Необходимо документировать все процедуры, требования и обязанности.

12.3.2 Защита средств аудита систем

Доступ к средствам аудита систем, в частности, к программам и файлам данных, должен быть ограничен, чтобы предотвратить их неправомерное использование или повреждение. Такие средства должны быть отделены от рабочих систем и систем разработки. Они не должны храниться в библиотеках данных и на пользовательских территориях без обеспечения дополнительной защиты.