**Содержание**

Введение . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  
1. Область применения . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .1

1. Термины и определения
2. Политика безопасности  
    3.1. Политика информационной безопасности
3. Организационные вопросы безопасности

4.1.Организационная инфраструктура информационной безопасности

4.2. Обеспечение безопасности при наличии доступа к информационным системам сторонних организаций

4.3.Привлечение сторонних организаций к обработке информации (аутсорсинг)

1. Классификация и управление активами  
    5.1. Учет активов

5.2. Классификация информации

6. Физическая защита и защита от воздействий окружающей среды.

6.1. Охраняемые зоны.

6.2. Безопасность оборудования.

6.3. Общие мероприятия по управлению информационной безопасностью.

7. Управление передачей данных и операционной деятельностью.

7.1. Операционные процедуры и обязанности.

7.2. Защита от вредоносного программного обеспечения.

7.3. Вспомогательные операции  
 7.4. Управление сетевыми ресурсами.

7.5. Безопасность носителей информации.

7.6. Обмен информацией и программным обеспечением.

9. Контроль доступа.

9.1. Требование бизнеса по обеспечению контроля в отношении логического доступа.

9.2. Контроль в отношении доступа пользователей.

9.3. Обязанности пользователей.

9.4. Контроль сетевого доступа.

9.5. Контроль доступа к операционной системе.

9.6. Контроль доступа к приложениям.

9.7. Мониторинг доступа и использования системы.

9.8. Работа с переносными устройствами и работа в дистанционном режиме.

10. Разработка и обслуживание систем

10.1. Требования к безопасности системы.

10.2. Безопасность в прикладных системах.

10.3. Меры защиты информации, связанные с использованием криптографии.

10.4. Безопасность системных файлов.

10.5. Безопасность в процессах разработки и поддержки.

11. Управление непрерывностью бизнеса.

12. Соответствие требованиям.

12.1. Соответствие требованиям законодательства.  
 12.2. Пересмотр политики безопасности и техническое соответствие требованиям безопасности

12.3. Меры безопасности при проведении аудита

**Введение**

**Понятие информационной безопасности**

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

Информационная безопасность - механизм защиты, обеспечивающий:

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

Информационная безопасность достигается путем реализации соответствующего комплекса мероприятий по управлению информационной безопасностью, которые могут быть представлены политиками, методами, процедурами, организационными структурами и функциями программного обеспечения.

**Необходимость информационной безопасности**

Планшет, его информационная система и сети все чаще сталкиваются с различными угрозами безопасности, такими как компьютерное мошенничество, шпионаж, вредительство, вандализм. Такие источники ущерба, как компьютерные вирусы, компьютерный взлом и атаки типа отказа в обслуживании, становятся более распространенными, более агрессивными и все более изощренными.

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

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

Управление информационной безопасностью нуждается, как минимум, в участии самого пользователя. Кроме того, могут потребоваться консультации специалистов сторонних лиц.

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

**Как определить требования к информационной безопасности**

Пользователь должен определить свои требования к информационной безопасности с учетом следующих факторов:

1. Оценка рисков. Посредством оценки рисков происходит выявление угроз, оценка уязвимости и вероятности возникновения угроз, а также оценка возможных последствий.
2. Специфический набор принципов, целей и требований, разработанный пользователем в отношении обработки информации.

**Оценка рисков информационной безопасности**

Требования к информационной безопасности определяются с помощью систематической оценки рисков. Методы оценки риска могут применяться как для всего планшета, так и для какой-либо его части, отдельных информационных систем, определенных компонентов систем, а именно там, где это практически выполнимо и целесообразно.

Оценка риска – это систематический анализ:

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

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

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

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

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

Уровень детализации такого анализа следует определять в зависимости от результатов предыдущих проверок и изменяющегося уровня приемлемого риска.

**Выбор мероприятий по управлению информационной безопасностью**

После того, как определены требования к информационной безопасности, следует выбрать и внедрить такие мероприятия по управлению информационной безопасностью, которые обеспечат снижение рисков до приемлемого уровня. Эти мероприятия могут быть выбраны из настоящего стандарта, других источников, а также могут быть разработаны собственные мероприятия по управлению информационной безопасностью, удовлетворяющие специфическим потребностям пользователя. Имеется множество различных подходов к управлению рисками; в настоящем стандарте приводятся примеры наиболее распространенных методов. Однако следует отметить, что некоторые из мероприятий по управлению информационной безопасностью неприменимы к отдельным информационным системам и средам и могут оказаться неприемлемыми для конкретных организаций.

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

**Отправная точка для внедрения информационной безопасности**

Отдельные мероприятия по управлению информационной безопасностью могут рассматриваться как руководящие принципы для управления информационной безопасностью и служить отправной точкой для ее внедрения.

Ключевыми мерами контроля являются:

* обеспечение конфиденциальности персональных данных;
* защита учетных данных организации;
* права на интеллектуальную собственность.

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

* изучение вопроса информационной безопасности;
* информирование об инцидентах, связанных с информационной безопасностью;

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

**Важнейшие факторы успеха**

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

* четкое понимание требований безопасности, оценка рисков и управление рисками;
* понимание необходимости применения мер информационной безопасности пользователем;
* всесторонняя и сбалансированная система измеряемых показателей, используемых для оценки эффективности управления информационной безопасностью и предложений по ее улучшению.

**НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Информационная технология

ПРАКТИЧЕСКИЕ ПРАВИЛА УПРАВЛЕНИЯ ИНОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Information technology. Code of practice for information  
security management

Дата введения – 2007 – 01- 01

1. **Область применения.**

Настоящий стандарт устанавливает рекомендации по управлению информационной безопасностью лицам, ответственным за поддержку безопасности в использовании. Он предназначен для обеспечения общих основ для разработки стандартов безопасности, а также в интересах обеспечения доверия в различных отношениях между пользователями. Рекомендации настоящего стандарта следует выбирать и использовать в соответствии с действующим законодательством.

1. **Термины и определения**

В настоящем стандарте применены следующие термины с соответствующими определениями:

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

Примечания   
 1 **конфиденциальность**: Обеспечение доступа к информации только авторизованным пользователям.   
 2 **целостность**: Обеспечение достоверности и полноты информации и методов ее обработки.   
 3 **доступность**: Обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

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

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

1. **Политики безопасности**
   1. **Политика информационной безопасности**

Цель: обеспечение решения вопросов информационной безопасности и вовлечение пользователей в данный процесс.

Разработка и реализация политики информационной безопасности пользователей осуществляется ими же путем выработки четкой позиции в решении вопросов информационной безопасности.

* + 1. **Содержание политики безопасности**

Политика информационной безопасности должна быть утверждена, издана и надлежащим образом доведена до сведения всех пользователей. Она должна устанавливать ответственность пользователей, а также

Издание официальное

излагать их подход к управлению информационной безопасностью. Как минимум, политика должна включать следующее:

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

б) изложение целей и принципов информационной безопасности для пользователей;

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

1) требования в отношении обучения вопросам безопасности;

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

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

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

1. **Организационные вопросы безопасности**

**4.1. Организационная инфраструктура информационной безопасности**

Цель: управление информационной безопасностью.

Структуру управления следует создавать так, чтобы она легко применялась во время использования планшета, проводились мероприятия по управлению информационной безопасностью. При необходимости следует предусмотреть наличие специалиста по вопросам информационной безопасности, к которому могут обращаться заинтересованные пользователи. Следует налаживать контакты с иными пользователями, чтобы быстро узнавать о новых методах защиты информации.

* + 1. **Управляющий совет по вопросам информационной безопасности**  
        Обеспечение информационной безопасности — это ответственность пользователя. Поэтому при формировании совета по вопросам информационной безопасности должны обеспечиваться четкие задачи для пользователей. Такой совет должен способствовать укреплению безопасности путем доступного объяснения теории и выделения необходимых ресурсов. Такой совет выполняет следующие функции:

- утверждение и пересмотр политики информационной безопасности;

- отслеживание существенных изменений в воздействиях основных угроз информационным активам;

- анализ и мониторинг инцидентов нарушения информационной безопасности.

* + 1. **Консультации специалистов по вопросам информационной безопасности** Консультации специалистов по вопросам безопасности требуются многим пользователям. В идеале, их должен обеспечивать опытный консультант по информационной безопасности. В иных случаях рекомендуется консультация у выделенного сотрудника какой-либо организации для обобщения знаний и опыта с целью обеспечения согласованности и поддержки в принятии решений по безопасности. Этот сотрудник должен также иметь доступ к необходимым внешним консультантам для получения профессиональных консультаций по вопросам, выходящим за рамки его собственной компетенции. Перед консультантами по информационной безопасности должна быть поставлена задача по обеспечению консультаций по всем аспектам информационной безопасности, в том числе и с привлечением внешних консультантов. От качества их оценки угроз безопасности и разработки рекомендаций относительно мероприятий по управлению информационной безопасностью существенным образом зависит ее эффективность в организации. С консультантом по информационной безопасности следует советоваться, по возможности, незамедлительно, в случае подозрения на выявление инцидента нарушения информационной безопасности или уязвимости безопасности для обеспечения получения квалифицированного совета или выделения ресурсов. Целесообразно обращение к консультанту по информационной безопасности с целью разработки рекомендаций, а также его участия в расследовании или в его руководстве.
    2. **Независимая проверка (аудит) информационной безопасности** Документ политики информационной безопасности (подраздел 3.1) устанавливает цели и обязанности в области информационной безопасности. Его выполнение должно проверяться в интересах обеспечения уверенности в том, что разработанные мероприятия должным образом отражают политику и что она является выполнимой и эффективной (подраздел 12.2). Такая проверка (аудит) может быть выполнена пользователями или специалистами, специализирующимися на таких проверках и обладающими соответствующими навыками и опытом.

**4.2. Обеспечение безопасности при наличии доступа к информационным системам сторонних пользователей**

Цель: поддерживать безопасность своих средств обработки информации при доступе третьих сторон.   
 Доступ к средствам обработки информации пользователя третьих сторон должен контролироваться. Там, где есть потребность в доступе третьей стороны, следует производить оценку риска, определять последствия для безопасности и устанавливать требования к мероприятиям по управлению информационной безопасностью. Такие мероприятия следует согласовывать и определять в соглашении с третьей стороной. Соглашения, разрешающие доступ третьей стороне, должны включать процедуру определения прав и условий доступа других участников. Настоящий стандарт может использоваться как основа для составления таких соглашений, а также при рассмотрении и привлечении сторонних пользователей для обработки информации (outsourcing).

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

**4.2.1.1 Типы доступа**

Определение типа доступа, предоставленного третьей стороне, имеет особое значение. Например, риски доступа через сетевое соединение отличаются от рисков, связанных с физическим доступом. Типами доступа, которые следует рассматривать, являются:

- физический - к компьютерным комнатам;

- логический - к базам данных, информационным системам пользователя.

**4.2.1.2 Обоснования для доступа**

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

- пользователям третьей стороны, отвечающим за обслуживание аппаратных средств и программного обеспечения, которым необходим доступ на уровне систем или более низком уровне прикладной функциональности;

- другим пользователям, которым может потребоваться обмен информацией, доступ к информационным системам или общим базам данных.

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

**4.2.2. Включение требований безопасности в договоры со сторонними лицами и организациями**

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

а) общая политика информационной безопасности;

б) защита активов, включая:

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

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

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

4) целостность и доступность активов;

5) ограничения на копирование и раскрытие информации;

в) описание каждой предоставляемой услуги;

г) определение необходимого и неприемлемого уровня обслуживания;

д) соответствующие обязательства сторон в рамках соглашения;

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

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

з) соглашения по управлению доступом, охватывающие:

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

2) процесс авторизации в отношении доступа и привилегий пользователей;

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

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

к) право мониторинга действий пользователей и блокировки доступа;

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

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

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

о) четкая структура подотчетности и согласованные форматы представления отчетов;

п) ясный и определенный процесс управления изменениями;

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

с) обучение пользователей методам и процедурам безопасности;

т) мероприятия по управлению информационной безопасностью для обеспечения защиты от вредоносного программного обеспечения (см. 8.3); 6 ГОСТ Р ИСО/МЭК 17799—2005

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

ф) привлечение третьей стороны вместе с субподрядчиками.

**4.3. Привлечение сторонних пользователей к обработке информации (аутсорсинг)**

Цель: обеспечение информационной безопасности, когда ответственность за обработку информации передана другому пользователю.

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

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

Требования безопасности в случае, когда пользователь передает для управления и контроля все или некоторые из своих информационных систем, сетей и/или планшетов, следует указать в соглашении, оговоренном между сторонами и учитывающем:

- выполнение требований законодательства, например, в отношении защиты данных;

- достижение договоренностей, обеспечивающих уверенность в том, что все стороны, включая субподрядчиков, осведомлены о своих обязанностях, касающихся безопасности;

- как будут обеспечиваться и тестироваться параметры целостности и конфиденциальности данных пользователя;

- типы физических и логических методов по управлению информационной безопасностью, используемых при предоставлении необходимого доступа к чувствительной информации владельца сторонним пользователям;

- обеспечение доступности сервисов в случае бедствия;

- уровни физической безопасности, которые должны быть обеспечены в отношении оборудования, используемого в рамках аутсорсинга;

- право на проведение аудита.

Условия, приведенные в пункте 4.2.2, следует также рассматривать как часть соглашения. Необходимо, чтобы соглашением была предусмотрена возможность дальнейшей детализации и реализации требований и процедур безопасности в согласованном между сторонами плане мероприятий в области безопасности. Несмотря на то, что соглашения по привлечению третьих сторон могут включать ряд сложных вопросов, правила и рекомендации по управлению информационной безопасностью, включенные в настоящий стандарт, должны служить отправной точкой при согласовании структуры и содержания плана по управлению безопасностью.

1. **Классификация и управление активами**
   1. **Учет активов**

Цель: обеспечение соответствующей защиты активов пользователя.

Все основные информационные активы должны быть учтены и закреплены за пользователями. Учет активов помогает обеспечивать уверенность в их надлежащей защите. Необходимо идентифицировать пользователей всех основных активов и определить их ответственность за поддержание соответствующих мероприятий по управлению информационной безопасностью.

* + 1. **Инвентаризация активов**

Описание активов дает уверенность в том, что обеспечивается их эффективная защита. Процесс составления описи активов - важный аспект управления риском. Пользователь должен быть в состоянии идентифицировать свои активы с учетом их относительной ценности и важности. Основываясь на этой информации, пользователь может обеспечивать заданные уровни защиты, соответствующие ценности и важности активов. Каждый актив должен быть четко идентифицирован и классифицирован с точки зрения безопасности (5.2). Кроме того, должно быть указано фактическое местоположение актива (это важно в случае восстановления активов при потере или повреждении). Примерами активов, связанных с информационными системами, являются:

- активы программного обеспечения: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства разработки и утилиты;

- физические активы: оборудование (переносные клавиатуры, мышки), оборудование связи (маршрутизаторы, частные автоматические телефонные станции с выходом в сеть общего пользования), внешние носители (флеш-карты), другое техническое оборудование (электропитание;

- услуги: вычислительные услуги и услуги связи.

**5.2 Классификация информации**

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

Информацию следует классифицировать, чтобы определить ее приоритетность, необходимость и степень ее защиты. Информация имеет различные степени чувствительности и критичности. Некоторые виды информации могут требовать дополнительного уровня защиты или специальных методов обработки. Систему классификации информации следует использовать для определения соответствующего множества уровней защиты и потребности в специальных методах обработки.

**5.2.1 Основные принципы классификации**

При классификации информации и связанных с ней мероприятий по управлению информационной безопасностью следует учитывать потребности пользователя в совместном использовании или ограничении доступа к информации, а также последствия, связанные с такими требованиями, например, неавторизованный доступ или повреждение информации. Классификация информации позволяет определить, как эта информация должна быть обработана и защищена. Информацию, обрабатывающую классифицированные данные, следует отнести к какой-либо категории с точки зрения ее ценности и чувствительности для организации. Можно также оценить соответствующую информацию с учетом того, насколько она критична для пользователя, например, с точки зрения обеспечения ее целостности и доступности. Эти аспекты следует принимать во внимание, поскольку присвоение повышенной категории может вести к ненужным дополнительным расходам. Категория любого вида информации необязательно должна быть постоянной в течение всего времени— она может изменяться в соответствии с некоторой политикой безопасности (9.1). Чрезмерно сложные схемы категорирования информации могут стать обременительными и неэкономичными для использования или оказываются неосуществимыми. Следует проявлять осмотрительность при интерпретации категорий (грифов) классификации, которые могут иметь другие определения или содержание для тех же самых или подобных категорий. Ответственность за определение категории информации (например, документа, записи данных файла) и периодичность пересмотра этой категории должны оставаться за пользователем.

**5.2.2 Обработка информации**

Важно, чтобы был определен соответствующий набор процедур для обработки информации в соответствии с системой классификации. Эти процедуры должны относиться к информационным активам, представленным как в физической, таки в электронной форме.

**6 Физическая защита и защита от действия окружающей среды**

**6.1 Охраняемые зоны**

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

Средства обработки критичной или важной информации пользователя необходимо размещать в зонах безопасности, обозначенных определенным периметром безопасности, обладающим соответствующими защитными барьерами и средствами контроля проникновения. Эти зоны должны быть физически защищены от неавторизованного доступа, повреждения и воздействия. Уровень защищенности должен быть соразмерен с идентифицированными рисками. С целью минимизации риска неавторизованного доступа или повреждения бумажных документов, носителей данных и средств обработки информации, рекомендуется внедрить политику «чистого стола» и «чистого экрана».

**6.1.1 Периметр охраняемой зоны**

Физическая защита может быть достигнута созданием нескольких физических барьеров (преград). Барьеры устанавливают отдельные периметры безопасности, каждый из которых обеспечивает усиление защиты в целом. Периметр безопасности — это граница, создающая барьер. Расположение и уровень защиты (стойкости) каждого барьера зависят от результатов оценки рисков. Рекомендуется четко определять периметр безопасности для обеспечения информационной безопасности.

**6.1.2 Контроль доступа в охраняемые зоны**

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

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

- доступ к важной информации и средствам ее обработки должен контролироваться и предоставляться только авторизованным лицам;

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

**6.1.3 Выполнение работ в охраняемых зонах**

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

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

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

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

**6.2 Безопасность оборудования**

Цель: предотвращение потерь, повреждений или компрометаций активов

Оборудование необходимо защищать от угроз его безопасности и воздействий окружающей среды. Необходимо обеспечивать безопасность оборудования, чтобы уменьшить риск неавторизованного доступа к данным и защитить их от потери или повреждения. При этом необходимо принимать во внимание особенности, связанные с расположением оборудования и возможным его перемещением. Могут потребоваться специальные мероприятия защиты от опасных воздействий среды или неавторизованного доступа через инфраструктуры обеспечения, в частности, системы электропитания и кабельной разводки.

**6.2.1 Расположение и защита оборудования**

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

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

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

в) меры по управлению информационной безопасностью должны свести к минимуму риск потенциальных угроз;

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

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

**6.2.2 Подача электропитания**

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

- наличие нескольких источников электропитания, чтобы избежать последствий при нарушении его подачи от единственного источника;

- устройства бесперебойного электропитания (UPS);

- резервный генератор.

Чтобы обеспечить безопасное выключение и/или непрерывное функционирование устройств рекомендуется подключать оборудование через UPS. В планах обеспечения непрерывности следует предусматривать действия, которые должны быть предприняты при отказе UPS. Оборудование UPS следует регулярно проверять на наличие адекватной мощности, а также тестировать в соответствии с рекомендациями производителя. Резервный генератор следует применять, если необходимо обеспечить функционирование оборудования в случае длительного отказа подачи электроэнергии от общего источника. Резервные генераторы следует регулярно проверять в соответствии с инструкциями производителя. Для обеспечения работы генератора в течение длительного срока необходимо обеспечить соответствующую поставку топлива. Следует обеспечить работу аварийного освещения на случай отказа электропитания, потребляемого от сети.

**6.2.3 Безопасная утилизация (списание) или повторное использование оборудования**

Информация может быть скомпрометирована вследствие небрежной утилизации (списания) или повторного использования оборудования (7.6.4). Носители данных, содержащие важную информацию, необходимо физически разрушать или перезаписывать безопасным образом, а не использовать стандартные функции удаления. Все компоненты оборудования, содержащего носители данных (встроенные жесткие диски), следует проверять на предмет удаления всех важных данных и лицензионного программного обеспечения. В отношении носителей данных, содержащих важную информацию, может потребоваться оценка рисков с целью определения целесообразности их разрушения, восстановления или выбраковки.

**6.3 Общие мероприятия по управлению информационной безопасностью**

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

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

**6.3.1 Политика «чистого стола» и «чистого экрана»**

Пользователям следует применять политику «чистого стола» в отношении бумажных документов и сменных носителей данных, а также политику «чистого экрана» в отношении средств обработки информации с тем, чтобы уменьшить риски неавторизованного доступа, потери и повреждения информации. При применении этих политик следует учитывать категории информации с точки зрения безопасности (5.2) и соответствующие риски. Носители информации, оставленные на столах, также могут быть повреждены или разрушены при бедствии, например, при пожаре, наводнении или взрыве. Следует применять следующие мероприятия по управлению информационной безопасностью:

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

- носители с важной или критичной информацией, когда они не требуются, следует убирать и запирать, особенно когда помещение пустует;

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

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

1. **Управление передачей данных и операционной деятельностью**

**7.1 Операционные процедуры и обязанности**

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

Должны быть установлены обязанности и процедуры по управлению и функционированию всех средств обработки информации. Они должны включать разработку соответствующих операционных инструкций и процедуры реагирования на инциденты. С целью минимизации риска при неправильном использовании систем вследствие небрежности или злого умысла следует, по возможности, реализовывать принцип разделения полномочий (7.1.4).

* + 1. **Документальное оформление операционных процедур**

Операционные процедуры, определяемые политикой безопасности, должны рассматриваться как официальные документы. Процедуры содержат детальную инструкцию выполнения конкретного задания (работы) и включают:

- обработку и управление информацией;

- определение требований в отношении графика выполнения заданий, включающих взаимосвязи между системами;

- обработку ошибок или других исключительных ситуаций, которые могут возникнуть в течение выполнения заданий, включая ограничения на использование системных утилит (8.5.5);

- необходимые контакты на случай неожиданных операционных или технических проблем;

- перезапуск системы и процедуры восстановления в случае системных сбоев.

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

**7.1.2 Контроль изменений**

Изменения конфигурации в средствах и системах обработки информации должны контролироваться надлежащим образом. Неадекватный контроль изменений средств и систем обработки информации — распространенная причина системных сбоев и инцидентов нарушения информационной безопасности. С целью обеспечения надлежащего контроля всех изменений в оборудовании, программном обеспечении или процедурах должны быть определены и внедрены формализованные роли, ответственности и процедуры. При изменении программного обеспечения вся необходимая информация должна фиксироваться и сохраняться в системном журнале аудита.

**7.1.3 Процедуры в отношении инцидентов нарушения информационной безопасности**

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

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

1) сбои информационных систем и утрата сервисов;

2) отказ в обслуживании;

3) ошибки вследствие неполных или неточных данных;

4) нарушения конфиденциальности;

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

1) анализа и идентификации причины инцидента;

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

3) использования журналов аудита и аналогичных свидетельств;

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

**7.1.4 Управление средствами обработки информации сторонними пользователями**

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

**7.2 Защита от вредоносного программного обеспечения**

Цель: обеспечение защиты целостности программного обеспечения и массивов информации.

Необходимо принимать меры предотвращения и обнаружения внедрения вредоносного программного обеспечения. Программное обеспечение и средства обработки информации уязвимы к внедрению вредоносного программного обеспечения, такого как компьютерные вирусы, сетевые «черви», «троянские кони» (9.5.4) и логические бомбы. Пользователи должны быть осведомлены об опасности использования неавторизованного или вредоносного программного обеспечения, а соответствующие руководители должны обеспечить внедрение специальных средств контроля с целью обнаружения и/или предотвращения проникновения подобных программ. В частности, важно принятие мер предосторожности с целью обнаружения и предотвращения заражения компьютерными вирусами персональных компьютеров.

**7.2.1 Мероприятия по управлению информационной безопасностью для борьбы с вредоносным программным обеспечением**

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

- документированную политику, требующую соблюдения лицензионных соглашений и устанавливающую запрет на использование неавторизованного программного обеспечения (11.1.2.2);

- документированную политику защиты от рисков, связанных с получением файлов и программного обеспечения из внешних сетей, через внешние сети или из любой другой среды. В этой политике должно содержаться указание о необходимости принятия защитных мер (9.5, 9.5.4, 9.5.5);

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

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

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

- проверку любых вложений электронной почты и скачиваемой информации на наличие вредоносного программного обеспечения до их использования. Эта проверка может быть выполнена в разных точках, например, на электронной почте, персональных планшетах или при входе в сеть организации;

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

- процедуры по контролю всей информации, касающейся вредоносного программного обеспечения, обеспечение точности и информативности предупредительных сообщений.

Для определения различия между ложными и реальными вирусами должны использоваться профессиональные источники, например, респектабельные журналы, заслуживающие доверия интернет-сайты или поставщики антивирусного программного обеспечения.

**7.3. Вспомогательные операции**

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

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

**7.3.1 Резервирование информации**

Резервное копирование важной информации и программного обеспечения должно выполняться на регулярной основе. Следует обеспечивать адекватные средства резервирования для обеспечения уверенности в том, что вся важная деловая информация и программное обеспечение смогут быть восстановлены после бедствия или сбоя оборудования. Целесообразно применять следующие мероприятия по управлению информационной безопасностью:

- минимально необходимый объем резервной информации, вместе с точными и полными регистрационными записями по содержанию резервных копий;

- резервная информация должна быть обеспечена гарантированным уровнем физической защиты и защиты от воздействий окружающей среды в соответствии с уровнем безопасности.

**7.4. Управление сетевыми ресурсами**

Цель: обеспечение безопасности и защиты информации в сетях.

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

**7.4.1 Средства контроля сетевых ресурсов**

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

- следует распределять ответственность за поддержание сетевых ресурсов;

- следует устанавливать процедуры и обязанности по управлению удаленным оборудованием;

- если необходимо, специальные средства контроля следует внедрять для обеспечения конфиденциальности и целостности данных, проходящих по общедоступным сетям, а также для защиты подключенных систем.

**7.5. Безопасность носителей информации**

Цель: предотвращение повреждений активов.

Использование носителей информации должно контролироваться, а также должна обеспечиваться их физическая безопасность. Должны быть определены соответствующие процедуры защиты документов, компьютерных носителей информации (флеш-карт), данных ввода/вывода и системной документации от повреждений, воровства и неправомочного доступа.

**7.5.1 Использование сменных носителей компьютерной информации**

Должны существовать процедуры по использованию сменных носителей компьютерной информации. В этих случаях необходимо рассматривать следующие мероприятия по управлению информационной безопасностью:

- если носители информации многократного использования больше не требуются и передаются иным пользователям, то их содержимое должно быть уничтожено;

- в отношении всех уничтожаемых носителей информации должно быть принято соответствующее решение;

- все носители информации следует хранить в надежном, безопасном месте в соответствии с требованиями изготовителей.

**7.5.2 Утилизация носителей информации**

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

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

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

1) бумажные документы;

2) речевые или другие записи;

3) оптические носители данных (все разновидности, в том числе носители, содержащие программное обеспечение, поставляемое производителями);

4) тексты программ;

5) тестовые данные;

**7.5.3 Процедуры обработки информации**

С целью обеспечения защиты информации от неавторизованного раскрытия или неправильного использования необходимо определить процедуры обработки и хранения информации. Эти процедуры должны быть разработаны с учетом категорирования информации, а также в отношении документов, вычислительных систем, сетей, переносных планшетов. Необходимо использовать следующие мероприятия по управлению информационной безопасностью:

- ограничения доступа с целью идентификации неавторизованных пользователей;

- обеспечение уверенности в том, что данные ввода являются полными, процесс обработки завершается должным образом и имеется подтверждение вывода данных;

- обеспечение защиты информации, находящейся в буфере данных и ожидающей вывода в соответствии с важностью этой информации;

- хранение носителей информации в соответствии с требованиями изготовителей;

- сведение рассылки данных к минимуму.

**7.6 Обмен информацией и программным обеспечением**.

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

Обмен информацией и программным обеспечением между организациями должен быть под контролем и соответствовать действующему законодательству. Необходимо определить процедуры и мероприятия по защите информации и носителей при передаче. Необходимо учитывать последствия для деятельности и безопасности организации, связанные с электронным обменом данных, электронной торговлей и электронной почтой, а также требования к мероприятиям по управлению информационной безопасностью.

**7.6.1 Безопасность носителей информации при пересылке**

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

а) следует использовать надежных перевозчиков или курьеров;

б) упаковка должна быть достаточной для защиты содержимого от любого физического повреждения, которое может иметь место при транспортировке;

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

**7.6.2 Безопасность электронной торговли**

В электронной торговле могут использоваться различные способы обмена данными, например, в электронном виде (EDI), через электронную почту и транзакции в режиме онлайн через общедоступные сети, в частности, Интернет. Электронная торговля подвержена ряду сетевых угроз, которые могут привести к краже, оспариванию контрактов, а также раскрытию или модификации информации. Чтобы защитить электронную торговлю от таких угроз, необходимо применять соответствующие мероприятия по управлению информационной безопасностью.

**7.6.3 Безопасность электронной почты**

**7.6.3.1 Риски безопасности**

Социальные сети используются для обмена информацией между пользователями, заменяя традиционные формы связи, такие как почта. Социальные сети отличаются от традиционных форм коммуникаций скоростью, структурой сообщений, определенной упрощенностью, а также уязвимостью к неавторизованным действиям. При этом необходимо учитывать потребность в средствах контроля для уменьшения рисков безопасности, связанных с социальными сетями. При оценке рисков безопасности необходимо учитывать, например, уязвимость сообщений по отношению к возможности неавторизованного доступа или модификации.

**7.6.3.2 Политика в отношении социальных сетей**

Пользователям следует внедрить четкие правила использования социальных сетей, предусматривающие следующие аспекты:

- вероятность атаки на социальные сети (вирусы, перехват);

- защиту вложений в сообщения социальных сетей;

- данные, при передаче которых не следует пользоваться социальными сетями;

- исключение возможности компрометации пользователей со стороны собеседников, например, путем рассылки дискредитирующих и оскорбительных сообщений;

- использование криптографических методов для защиты конфиденциальности и целостности электронных сообщений;

- хранение сообщений, которые, в этом случае, могли бы быть использованы в случае судебных разбирательств;

- дополнительные меры контроля обмена сообщениями, которые не могут быть аутентифицированы.

**7.6.4 Системы публичного доступа**

Следует уделять внимание защите целостности информации, опубликованной электронным способом, чтобы предотвратить неавторизованную модификацию, которая могла бы навредить репутации пользователя, поместившего эту информацию. Информацию системы публичного доступа, например информацию на Web-сайте, доступную через Интернет, возможно, потребуется привести в соответствие с законодательством и регулирующими нормами страны. Необходим соответствующий формализованный процесс авторизации прежде, чем информация будет сделана общедоступной. Программное обеспечение, данные и другую информацию, требующую высокого уровня целостности, доступ к которой осуществляется через системы публичного доступа, необходимо защищать адекватными способами, например, посредством цифровой подписи. Системы, предоставляющие возможность электронной публикации информации, обратной связи и непосредственного ввода информации, должны находиться под надлежащим контролем.

**7.6.5 Другие формы обмена информацией**

Необходимо предусмотреть наличие процедур и мероприятий по управлению информационной безопасностью с целью защиты процесса обмена информацией посредством речевых, факсимильных и видеосредств коммуникаций. Информация может быть скомпрометирована из-за недостаточной осведомленности по использованию средств передачи информации. В частности, информация может быть подслушана при переговорах по мобильному телефону в общественном месте, а также с автоответчиков; информация может также быть скомпрометированной вследствие неавторизованного доступа к системе голосовой почты или случайной отсылки факсимильных сообщений неправильному адресату. Информация может быть скомпрометирована, если к ней имели место доступ неавторизованные пользователи. Следует сформулировать четкие требования по соблюдению процедур, которым должны следовать пользователи при использовании речевой, факсимильной и видеосвязи. В частности, необходимо предусмотреть следующее:

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

б) напоминание пользователям о том, что не следует вести конфиденциальные беседы в общественных местах;

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

г) напоминание пользователям о возможных рисках, присущих использованию факсимильных аппаратов.