**ПРАВИЛА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ**

**1 Область применения**

Настоящий предстандарт устанавливает правила управления информационной безопасностью, предназначенные для лиц, ответственных за организацию, реализацию или сопровождение безопасности организации. Предстандарт предназначен для обеспечения общего базиса при разработке организационных стандартов безопасности и реализации эффективного управления безопасностью, а также для обеспечения конфиденциальности при контактах между организациями. Рекомендации этого предстандарта должны выбираться и использоваться в соответствии с принятыми законами и правилами.

**2 Определения**

В настоящем предстандарте применяют следующие термины с соответствующими определениями:

**2.1 Информационная безопасность** - сохранение конфиденциальности, целостности и доступности информации:

* **конфиденциальность** - гарантия того, что информация доступна только полномочным на доступ лицам;
* **целостность** - сохранение точности, полноты информации и методов обработки;
* **доступность** - гарантия того, что авторизованные пользователи по запросу имеют доступ к информации и соответствующим активам.

1. **Оценка риска** - оценка угроз и их воздействия на уязвимые места информации и средств ее обработки, вероятность реализации угроз.
2. **Управление рисками** - приемлемый по стоимостным затратам процесс идентификации, управления, уменьшения или устранения риска, соответствующего информационной системе.

**3 Политика безопасности**

**3.1 Политика информационной безопасности**

Задача: сформулировать цели политики информационной безопасности и обеспечить ее поддержку руководством организации.

Администрация должна поставить четкую цель и оказывать всестороннюю поддержку информационной безопасности посредством распространения политики безопасности среди сотрудников организации.

**3.1.1** Документ о политике информационной безопасности

Документ о политике информационной безопасности должен быть одобрен руководством, опубликован и доведен до сведения всех сотрудников. В нем необходимо сформулировать обязательство по управлению и изложить подход организации к управлению информационной безопасностью. В него обязательно следует включить следующие положения:

а) определение информационной безопасности, ее основные цели и область применения, а также значение безопасности как механизма, позволяющего коллективно использовать информацию;

Ь) изложение позиции руководства по вопросам реализации целей и принципов информационной безопасности;

с) разъяснение конкретных положений политики безопасности, принципов, стандартов и требований к ее соблюдению, включая:

1. выполнение правовых и договорных требований;
2. требования к обучению персонала правилам безопасности;
3. политику предупреждения и обнаружения вирусов, а также другого вредоносного программного обеспечения;
4. политику обеспечения бесперебойной работы организации;
5. последствия нарушения политики безопасности;

с!) определение общих и конкретных обязанностей по обеспечению режима информационной безопасности;

с) разъяснение процесса уведомления о событиях, таящих угрозу безопасности.

Данная политика должна быть доведена до всех сотрудников организации в релевантной, доступной и понятной заинтересованному лицу форме.

3.1.2 Пересмотр и оценка

В организации должен быть ответственный за реализацию политики, ее поддержку и пересмотр в соответствии с определенным процессом пересмотра. Этот процесс должен гарантировать, что пересмотр политики осуществляется в ответ на изменения, затрагивающие основы первоначальной оценки риска, например важные инциденты безопасности, новые уязвимые места или изменения организационной или технической инфраструктуры, рекомендуется планировать и периодически пересматривать:

а) эффективность политики, которую можно оценить в природе количеством и силой воздействия зарегистрированных инцидентов безопасности;

Ь) стоимости средств управления и их влияние на производственную эффективность;

с) эффект от изменений технологий.

**4 Организация защиты**

**4.1 Инфраструктура информационной безопасности**

Задача: обеспечить управление информационной безопасностью в организации.

Чтобы инициировать и контролировать процесс обеспечения информационной безопасности, необходимо создать в организации соответствующую структуру управления.

В организации рекомендуется проводить регулярные совещания руководства для разработки и утверждения политики безопасности, распределения обязанностей по обеспечению защиты и координации действий по поддержанию режима безопасности. В случае необходимости следует привлечь специалистов по вопросам защиты информации для консультаций. Необходимо вступать в контакты со специалистами других организаций, чтобы быть в курсе современных направлений и промышленных стандартов, а также, чтобы установить соответствующие деловые отношения для рассмотрения случаев нарушения защиты. Следует всячески поощрять комплексный подход к проблемам информационной безопасности, например совместную работу аудиторов, пользователей и администраторов для эффективного решения проблем.

**4.1.1** Совещание руководства по проблемам информационной безопасности Ответственность за обеспечение информационной безопасности несут все члены руководства. Поэтому руководству организации рекомендуется регулярно проводить совещания по проблемам защиты информации с целью выработки четких указаний по этому вопросу, а также оказания административной поддержки инициативам по обеспечению безопасности. Эти совещания должны содействовать реализации процесса защиты в организации посредством принятия соответствующих обяза-

тельств и предоставления адекватных ресурсов. Совещание может быть частью существующего органа управления. Обычно на подобных совещаниях рассматриваются следующие вопросы:

а) анализ и утверждение политики информационной безопасности, распределение общих обязанностей;

Ь) мониторинг основных угроз, которым подвергаются информационные ресурсы;

с) анализ и слежение за инцидентами в системе безопасности;

а1) утверждение основных инициатив, направленных на усиление защиты информации.

За координацию действий по проведению политики безопасности в жизнь должен быть ответственен один из членов руководства.

4.1.2 Координация действий по защите информации

В организации, возможно, потребуется координация мер по обеспечению информационной безопасности посредством проведения совещаний, на которых должны участвовать руководители разных подразделений. Обычно на таких совещаниях:

а) согласовываются конкретные функции и обязанности по обеспечению информационной безопасности в организации;

Ь) согласовываются конкретные методики и процессы защиты информации, например оценка рисков, система классификации средств защиты;

с) согласовывается и оказывается поддержка инициативам по защите информации в организации, например программе обучения персонала правилам безопасности;

а1) обеспечивается включение защитных мер в процесс информационного планирования;

е) оценивается адекватность и координируются действия по реализации конкретных мер по обеспечению информационной безопасности для новых систем или сервисов;

т) анализируются инциденты в информационной безопасности;

д) создаются благоприятные условия для поддержки информационной безопасности во всей организации.

4.1.3 Распределение ответственности за обеспечение информационной безопасности

Необходимо четко определить обязанности по защите отдельных ресурсов и выполнению конкретных процессов обеспечения безопасности.

Политика информационной безопасности (раздел 3) должна давать общие рекомендации по распределению функций и обязанностей по защите информации в организации. Там, где необходимо, следует дополнить эти рекомендации более подробными разъяснениями, касающимися конкретных систем или сервисов. Рекомендуется назначить ответственных за конкретные физические и информационные активы и процессы обеспечения защиты, такие как планирование бесперебойной работы организации.

Во многих организациях общая ответственность за развитие и реализацию безопасности, а также за поддержку управления безопасностью возлагается на руководителя службы информационной безопасности.

Однако за распределение ресурсов и реализацию управления часто несут ответственность отдельные руководители. Общепринято назначение для каждого информационного актива владельца, ответственного за его повседневную безопасность.

Владельцы информационных активов могут делегировать свои полномочия по безопасности отдельным руководителям или поставщикам по предоставлению услуг (сервис-провайдерам). Тем не менее, владелец активов в конечном счете остается ответственным за безопасность актива и должен контролировать корректность выполнения делегированной ответственности.

Важно четко определить зоны ответственности каждого администратора, в частности следует отразить следующие положения:

а) различные активы и процессы обеспечения безопасности, связанные с каждой системой, необходимо идентифицировать и четко определить;

Ь) кандидатура администратора, отвечающего за каждый актив или процесс обеспечения защиты, должна быть одобрена, а его обязанности документально оформлены;

с) уровни полномочий необходимо четко определить и документально оформить.

4.1.4 Процесс утверждения средств обработки информации

Следует определить процедуру утверждения новых средств обработки информации руководством.

Необходимо предусмотреть следующие меры по обеспечению контроля:

а) новые средства, их цель и назначение должны быть утверждены руководством пользователей и одобрены руководителем, ответственным за сопровождение безопасной среды функционирования локальных информационных систем. Эти меры позволяют гарантировать выполнение соответствующих политик и требований безопасности;

Ь) в случае необходимости следует проверить аппаратные и программные средства, чтобы гарантировать их совместимость с другими системными компонентами.

Примечание - Утверждение такого типа может потребоваться для некоторых подключений;

с) должно быть утверждено использование и необходимый контроль за персональными средствами обработки деловой информации;

с1) использование персональных средств обработки информации в рабочей зоне может привести к возникновению новых уязвимых мест, поэтому оно должно оцениваться и утверждаться.

Указанный контроль особенно важен в сетевой среде.

4.1.5 Рекомендации специалистов по информационной безопасности

Консультант по безопасности может потребоваться многим организациям. Эти функции следует выполнять опытному специалисту по внутренней информационной защите. Однако не всем организациям выгодно нанимать такого специалиста на постоянную работу. В этом случае рекомендуется определить опытного сотрудника, знающего внутренние проблемы организации и способного принимать решения по вопросам безопасности. Организации должны также иметь связь с соответствующими внешними консультантами, чтобы получать рекомендации специалистов, имеющих больший опыт.

Следует так подобрать специалистов по защите информации и сотрудников службы поддержки, чтобы обеспечить решение любой проблемы, касающейся информационной безопасности, на основании использования своего собственного или внешнего опыта. Качество их оценок угроз системе безопасности и рекомендуемые ими меры противодействия будут определять эффективность программы обеспечения информационной безопасности в организации. Для обеспечения максимальной эффективности такой программы этим специалистам следует предоставить прямой доступ к администратору информационной системы и руководству организации.

В случаях подозрения о нарушении защиты необходимо как можно быстрее обратиться к консультанту по вопросам обеспечения информационной безопасности или равнозначный контактный пункт, чтобы получить необходимые указания или ресурсы для расследования таких инцидентов. Хотя большинство внутренних расследований, связанных с нарушением защиты, обычно выполняется под контролем руководства, можно обратиться к консультанту по информационной безопасности как за советом, так и с предложением возглавить или провести необходимые расследования.

4.1.6 Сотрудничество между организациями

Чтобы обеспечить своевременное установление контактов и получение рекомендаций в случае инцидента в системе безопасности, следует поддерживать соответствующие контакты с правоохранительными органами, поставщиками информационных сервисов и телекоммуникационными органами. Следует принять во внимание также участие в этих процессах групп по обеспечению безопасности и производственные совещания.

Обмен информацией по вопросам безопасности должен быть ограничен, чтобы гарантировать, что конфиденциальная информация организации не попадет в руки лиц, не имеющих соответствующих полномочий.

4.1.7 Независимый анализ информационной безопасности

В документе о политике информационной безопасности (3.1) устанавливается ответственность по защите информации и формулируется соответствующая политика. Реальные процедуры обеспечения информационной безопасности должны быть подвергнуты независимому анализу, чтобы быть уверенными, что используемые организацией процедуры защиты соответствуют принятой политике безопасности, а также являются реализуемыми и эффективными (12.2).

Такой анализ может быть проведен при внутреннем аудите независимым руководством или третьей стороной, специализирующейся на выполнении такого анализа при условии, что она имеет надлежащую квалификацию и опыт.

**4.2 Безопасность доступа сторонних организаций**

Задача: обеспечить безопасность информационных ресурсов организации, к которым имеют доступ сторонние организации.

Доступ сторонних организаций к информационным ресурсам данной организации следует контролировать.

Там, где доступ сторонних организаций необходим по производственным причинам, следует провести анализ рисков нарушения защиты, чтобы определить его последствия для системы безопасности и требования к средствам контроля. Эти средства контроля должны быть согласованы и определены в контракте, заключенном со сторонней организацией.

Такой доступ может быть предоставлен и другим участникам. Контракты, разрешающие доступ сторонних организаций, должны включать в себя правила для доступа других участников и условия их доступа.

Настоящий предстандарт рекомендуется использовать в качестве основы при составлении подобных контрактов и при выполнении работ по обработке информации третьей стороной.

**4.2.1** Идентификация рисков, связанных с доступом сторонних организаций

*4.2.1.1 Типы доступа*

Тип доступа, предоставляемого сторонней организации, имеет особое значение. Например, риск, возникающий вследствие доступа через подключение к сети, отличается от риска, возникающего вследствие физического доступа. Основными типами доступа являются:

а) физический доступ, например в офис, компьютерный класс, картотечные блоки;

Ь) логический доступ, например к базе данных организации, информационным системам.

*4.2.1.2 Причины предоставления доступа*

Сторонним организациям может быть предоставлен доступ по ряду причин. Например, существуют сторонние организации, которые предоставляют данной организации сервисные услуги и расположены в другом месте, но могут иметь физический или логический доступ такого вида, как:

а) доступ персонала, обеспечивающий поддержку аппаратного и программного обеспечения и нуждающийся в доступе к выполняемым прикладным функциям на системном или более низком уровнях;

Ь) доступ торговых партнеров или объединенных производственных предприятий, которые могут обмениваться информацией, иметь доступ к системам доступа к информации или базе данных коллективного пользования.

*4.2.1.3 Контракты со сторонними организациями*

Сторонние организации, которые на время, оговоренное в контракте, расположены на той же территории также могут способствовать нарушению безопасности. Примерами сторонних организаций, расположенных на той же территории, являются:

а) персонал сопровождения и поддержки аппаратного и программного обеспечения;

Ь) персонал по уборке помещений, общественному питанию, охране и другим, осуществляемым сторонними организациями, сервисным услугам;

с) принятые на временную работу студенты и другие случайные исполнители;

о!) консультанты.

Важно понимать необходимость управления доступом администратора сторонней организации к средствам обработки информации, так как все требования безопасности, возникающие вследствие стороннего доступа или внутреннего контроля, должны отражаться в контракте со сторонней организацией (4.2.2). Например, в случае, когда существует особая потребность в конфиденциальности информации, могут использоваться соглашения о неразглашении информации (6.1.3).

Доступ сторонней организации к информации и средствам обработки информации может быть разрешен только после того, как будет реализован соответствующий контроль и подписан контракт, определяющий сроки подключения или доступа.

**4.2.2** Требования безопасности в контрактах, заключенных со сторонними организациями

Чтобы обеспечить соответствие политики стандартам безопасности, принятым в организации,

соглашения о доступе сторонних организаций к средствам обработки информации организации

должны основываться на контракте, в котором рекомендуется перечислить все необходимые условия

безопасности (или даны ссылки на них). Контракт должен обеспечивать отсутствие разногласий между

организациями. Организации должны удовлетворить свои потребности в компенсации затрат произведенной поставки. При составлении контрактов необходимо рассмотреть следующие вопросы:

а) общая политика информационной безопасности; Ь) защита активов, включая:

1. процедуры, касающиеся защиты активов организации, включая информацию и программное обеспечение;
2. процедуры установления того, что осуществлена компрометация какого-то актива, т. е. про изошла потеря или изменение данных;
3. контроль за обеспечением возврата или уничтожения информации и активов по окончании срока действия контракта или в оговоренный момент в течение действия контракта;
4. целостность и доступность;
5. ограничения на копирование и раскрытие информации;

с) описание каждой сервисной услуги, к которой можно получить доступ;

*б)* планируемый уровень обслуживания и недопустимые уровни обслуживания; е) положение о возможном перемещении персонала;

т) вытекающие из соглашения обязательства организаций;

д) обязанности, касающиеся правовых вопросов, например законодательство о защите данных с учетом различных национальных правовых систем в условиях, когда контракт предусматривает сотрудничество между организациями из разных стран;

п) соглашение о правах на интеллектуальную собственность, авторских правах (12.1.2) и защиту совместных работ (6.1.3);

*\)* соглашение по управлению доступом, включая:

1. разрешенные способы доступа, а также контроль и использование уникальных идентификаторов пользователей и паролей;
2. процесс предоставления привилегий и полномочий на доступ;
3. требование вести список лиц, которым разрешено использование имеющихся сервисных услуг и описание предоставляемых им прав и привилегий;

]) определение критериев качества, которые могут быть проверены, их мониторинг и связанные с ним сообщения;

к) право проводить аудит предусмотренных по контракту обязанностей или получать результаты подобного аудита, проведенного сторонней организацией;

I) право контролировать и отменять действие пользователя;

т) учреждение процесса урегулирования конфликтов с целью разрешения возникающих проблем, а в соответствующих случаях необходимо также рассмотреть соглашение о действиях в случае непредвиденных обстоятельств;

п) обязанности по установке аппаратного и программного обеспечения и их сопровождению;

0) четкая структура отчетности и согласованные форматы отчетов; р) четкий и хорошо определенный процесс управления изменениями;

*ц)* необходимые меры по управлению физической защитой и соответствующие механизмы обеспечения этого управления;

г) обучение пользователей и администрации методам, процедурам и правилам безопасности;

з) меры по обеспечению защиты от вредоносного программного обеспечения (8.3);

1) соглашения относительно уведомлений об инцидентах в системе безопасности и их расследовании;

и) участие сторонних организаций (соисполнители и другие участники).

**4.3 Заключение договора на выполнение работ сторонними организациями**

Задача: сопровождение безопасности информации в случаях, когда обязанности по обработке информации возложены на другую организацию.

В соглашении на выполнение работ сторонними организациями должны рассматриваться вопросы, связанные с риском, управлением безопасностью и процедурами информационных систем, сетей и/или сред эксплуатации (рабочего стола, компьютера), предусмотренные в контракте между сторонами.

**4.3.1** Требования безопасности в контрактах на выполнение работ сторонней организацией

В контракте, заключаемом между сторонами, должны оговариваться требования безопасности, которые выдвигает организация, заключающая со сторонней организацией договор на осуществление управления и контроля над всеми или частью ее информационных систем, сетей и/или окружением рабочего места.

В контракте рекомендуется отразить следующие положения:

а) каким правовым требованиям необходимо удовлетворять, например законодательству по защите данных;

Ь) какие соглашения должны быть приняты для обеспечения того, что все вовлеченные в договор стороны, включая соисполнителей, полностью осознают свою ответственность за обеспечение безопасности;

с) каким образом должны сопровождаться и тестироваться целостность и конфиденциальность производственных активов организации;

с!) какое физическое и логическое управление должно использоваться для ограничения и сужения доступа авторизованных пользователей к конфиденциальной производственной информации;

е) каким образом должен поддерживаться доступ к сервису в экстремальных ситуациях;

т) какой уровень физической защиты должен обеспечиваться для оборудования, используемого при выполнении работ соисполнителем;

д) право на проведение аудита.

В контракте рекомендуется также рассмотреть условия, перечисленные в 4.2.2. Контракт должен допускать возможность развития требований безопасности и процедур в плане управления, принимаемом двумя сторонами.

Хотя при составлении соисполнителем контрактов на выполнение работ могут возникнуть сложные, связанные с безопасностью вопросы, контроль, включенный в эти правила, может служить исходной базой для согласования структуры и содержания плана управления безопасностью.

**5 Классификация и управление активами**

**5.1 Ответственность за активы**

Задача: обеспечить адекватную защиту активов организации.

Все основные информационные активы должны быть подотчетны и иметь специально назначенного владельца.

Ответственность за активы позволяет обеспечить их надлежащую защиту. Для всех основных активов следует определить владельцев и возложить на них ответственность за поддержку управления соответствующим активом. Ответственность за реализацию управления может быть передана другому лицу, однако подотчетность за актив должна сохраняться за назначенным для него владельцем.

**5.1.1** Инвентаризация активов

Инвентаризация активов помогает убедиться в том, что для них обеспечена эффективная защита, а также может потребоваться для других производственных целей, например при принятии мер по охране здоровья и по технике безопасности, для страхования или финансовых (управление активами) целей. Процесс составления описи активов является важным аспектом управления риском. Организация должна идентифицировать свои активы, а также их относительную стоимость и важность. На основании этой информации организация может обеспечить уровни защиты, соответствующие стоимости и важности актива. Инвентаризацию необходимо проводить для всех основных активов, связанных с каждой информационной системой. Каждый актив рекомендуется четко идентифицировать, его владельца, категорию секретности (5.2), а также его текущее месторасположение (что важно при попытке восстановления после его потери или повреждения) установить и документально оформить. Примерами активов, связанных с информационными системами, являются:

а) информационные активы: базы данных и файлы данных, системная документация, руководства пользователей, учебные материалы, операционные процедуры и процедуры поддержки, планы обеспечения бесперебойной работы организации, процедуры перехода на аварийный режим, архивная информация;

Ь) программные активы: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и сервисные программы;

с) физические активы: компьютерное оборудование (процессоры, мониторы, портативные персональные компьютеры, модемы), коммуникационное оборудование (маршрутизаторы, частные автоматические телефонные станции с выходом в сеть общего пользования, факсы, автоответчики), магнитные носители данных (ленты и диски), другое техническое оборудование (блоки питания, кондиционеры), мебель, помещения;

с1) сервисы: вычислительные и коммуникационные сервисы, другие технические сервисы (отопление, освещение, энергоснабжение, кондиционирование воздуха).

**5.2 Классификация информации**

Задача: обеспечить надлежащий уровень защиты информационных активов.

Информация может отличаться степенью конфиденциальности и критичности. Некоторые виды информации могут потребовать дополнительной защиты или специального обращения. Систему классификации информации следует использовать для определения соответствующего уровня защиты и для уведомления пользователей о необходимости специального обращения с этой информацией.

5.2.1 Рекомендации по классификации

При классификации и всестороннем контроле над защитой информации должны быть учтены производственные потребности в распределении или ограничении доступа к информации, а также связанные с этими потребностями инциденты, например несанкционированный доступ или искажение информации. Классификация информации позволяет определить способ защиты и обращения с ней.

Информация и выходные данные систем, поддерживающих секретную информацию, снабжаются соответствующей маркировкой, отражающей ценность информации и ее конфиденциальность для организации. Классификация информации может проводиться в понятиях конфиденциальности информации, ее целостности и доступности.

Часто информация перестает быть конфиденциальной через некоторый промежуток времени, например, когда она становится общедоступной. Следует принимать это во внимание, так как чрезмерное засекречивание информации может привести к неоправданным дополнительным затратам организации. Рекомендации по маркированию должны предусматривать и учитывать тот факт, что классификация любого конкретного элемента информации может быть непостоянной и меняться в зависимости от некоторой предопределенной политики безопасности (9.1).

Необходимо рассмотреть ряд классификационных категорий и проанализировать преимущества каждой из них. Слишком сложные схемы могут быть громоздкими и неэффективными для использования либо могут продемонстрировать свою непрактичность. Следует с осторожностью подходить к интерпретации грифов секретности на документах из других организаций, поскольку одинаковый или похожий гриф может быть определен иначе.

Ответственность за классификацию конкретного вида информации, т. е. документа, файла данных или дискеты, а также за периодическую проверку этой категории возлагается на лицо, создавшее эти данные, или на их назначенного владельца.

5.2.2 Этикетирование информации и обращение с ней

Важно определить набор процедур этикетирования информации и обращения с ней, соответствующий классификационной схеме, принятой в организации. Эти процедуры должны охватывать информационные активы в физическом и электронном форматах. Для каждого класса должны быть определены процедуры обработки, охватывающие следующие виды деятельности:

а)копирование;

Ь)хранение;

с) передача по почте, факсу или электронной почте;

о!) речевая передача, включая мобильный телефон, электронную почту с телефонным каналом, аппараты с ответчиком;

е) уничтожение.

Выходные данные информационных систем, содержащие секретную информацию, должны иметь соответствующий гриф секретности (на выходе). Этот гриф должен отражать класс информации в соответствии с правилами, приведенными в 5.2.1. Примерами таких выходных данных являются печатные отчеты, информация, выводимая на экраны дисплеев, данные, хранимые на магнитных носителях (лентах, дисках, кассетах, компакт-дисках), электронные сообщения и передаваемые файлы.

Физические метки являются наиболее подходящей формой этикетирования. Однако некоторые информационные активы, такие как документы в электронной форме не могут быть снабжены физической меткой и для них нужно использовать средства электронной маркировки.

**6 Безопасность персонала**

**6.1 Безопасность в должностных инструкциях и при выделении ресурсов**

Задача: уменьшить риск ошибок персонала, краж, мошенничества или незаконного использования ресурсов.

Аспекты, связанные с безопасностью, следует учитывать еще на стадии набора персонала, включать их в должностные инструкции и договоры, а также контролировать в течение всего времени работы данного сотрудника.

Следует надлежащим образом проверять принимаемых на работу лиц (6.1.2), особенно если они будут работать с конфиденциальной информацией. Весь персонал организации и пользователи информационных ресурсов из сторонних организаций должны подписать обязательство о конфиден- циальности (неразглашении).

**6.1.1** Безопасность в должностных инструкциях

Обязанности и ответственность за безопасность, установленные принятой в организации политикой информационной безопасности (3.1), следует включать в должностные инструкции там, где это необходимо. В инструкциях необходимо отразить как общую ответственность за проведение в жизнь или поддержку политики безопасности, так и конкретные обязанности по защите определенных активов или ответственность за выполнение определенных процедур или действий по защите.

**6.1.2** Проверка персонала

Проверку лиц, принимаемых на работу, рекомендуется проводить во время подачи ими заявления о приеме на работу. Проверку следует проводить по следующим пунктам:

а) не менее двух положительных характеристик (одна - деловых качеств, другая - личных качеств);

Ь) проверка (полноты и точности) сведений, сообщенных претендентом на вакансию в своей автобиографии;

с) подтверждение академических степеней и профессиональной квалификации;

а1) независимая проверка личности (паспорт или аналогичный документ).

Если работа изначально или в связи с повышением по службе включает доступ к средствам обработки информации и, в частности, когда речь идет об обработке критической информации, например финансовой или очень конфиденциальной, необходимо проверить, можно ли доверять лицу, принимаемому на работу. Для персонала, занимающего достаточно высокие должности, эта проверка должна периодически повторяться.

Аналогичная проверка должна осуществляться для временного персонала и лиц, работающих по контракту. Когда персонал набирается через агентство, в контракте с ним должна быть четко определена обязанность агентства проводить (и оповещать об этом) процедуры, которые должны быть выполнены в случае, если проверка проведена не полностью или ее результат сомнителен или неблагоприятен.

Руководство должно осуществлять необходимое наблюдение за полномочием на доступ к конфиденциальной информации нового и неопытного персонала. Работа нового персонала должна подвергаться периодической проверке и одобрению со стороны более опытного персонала.

Руководители должны осознавать, что материальное положение персонала может влиять на его работу. Личные или финансовые проблемы персонала, изменения в режиме или стиле жизни сотру-ников, многократное отсутствие на работе, стресс или депрессия могут привести к мошенничеству, краже, ошибке или другим проблемам безопасности. Поэтому подобную информацию надо использовать, исходя из соответствующего действующего законодательства.

**6.1.3** Соглашение о конфиденциальности

Соглашения о конфиденциальности или неразглашении используются для уведомления о конфиденциальности или секретности информации. Обычно служащие организации подписывают подобное обязательство при приеме на работу, что является одним из условий найма.

Временные работники и пользователи из сторонних организаций, не предусмотренные условиями существующего договора (обязательство о неразглашении является его частью), должны подписать обязательство о неразглашении прежде, чем им будет предоставлен доступ к средствам обработки информации.

Обязательства о неразглашении необходимо пересматривать, когда изменяются условия найма или договор, особенно, если служащие должны уволиться из организации или если кончаются сроки действия договора.

**6.1.4** Договор об условиях найма

В договоре об условиях найма должна устанавливаться ответственность служащего за информационную безопасность. В случае необходимости эта ответственность продлевается на определенный период после окончания службы. Данные обязательства должны включать действия, которые предпринимаются в случае нарушения служащим требований безопасности. В договоре и условиях найма должны быть четко сформулированы юридические права и обязанности служащего, например положения об авторском праве или защите данных. Ответственность за установление степени конфиденциальности и управление возлагается на работодателя. В надлежащих случаях в договоре должно содержаться положение о распространении указанных обязательств на деятельность за пределами организации и в нерабочее время, например в случае работы на дому (7.2.5 и 9.8.1).

**6.2 Обучение пользователей**

Задача: убедиться в том, что пользователи осведомлены об угрозах нарушения режима информационной безопасности и понимают значение защиты, а также имеют необходимые навыки для выполнения процедур, необходимых для нормального функционирования системы безопасности организации.

Чтобы минимизировать риск нарушения безопасности, пользователи должны быть обучены процедурам защиты и правильному использованию средств обработки информации, обращению с информационными ресурсами.

**6.2.1** Обучение правилам информационной безопасности

Все служащие организации, а там, где это необходимо, и сторонние пользователи должны получать необходимые регулярно обновляемые сведения о политике безопасности организации и используемых для ее реализации процедурах. Эти сведения включают требования к безопасности, правовые обязательства и производственный контроль, а также обучение правильному использованию средств обработки информации, например процедур входа в систему, пакетов программ прежде, чем предоставить доступ к информации или сервису.

**6.3 Реагирование на связанные с безопасностью инциденты и неисправности**

Задача: свести ущерб от инцидентов в системе безопасности и ее сбоев к минимуму, а также отслеживать такие события и извлекать из них соответствующие уроки.

О событиях, затрагивающих безопасность, необходимо немедленно сообщать по соответствующим каналам управления.

Все сотрудники и подрядчики должны быть ознакомлены с процедурой уведомления о различных типах инцидентов (нарушение безопасности, угроза, дефект или сбой), которые могут повлиять на безопасность активов организации. Следует обязать пользователей без промедления сообщать обо всех наблюдаемых или подозрительных случаях такого рода в соответствующую службу поддержки системы защиты. В организации должна быть установлена формальная процедура наложения дисциплинарных взысканий на сотрудников, которые нарушают режим безопасности. Для того чтобы должным образом отреагировать на инцидент, необходимо как можно быстрее после его возникновения собрать свидетельские показания (12.1.7).

**6.3.1** Уведомление об инцидентах в системе безопасности

Об инцидентах в системе безопасности следует без промедления сообщать по соответствующим каналам управления.

Следует установить официальную процедуру уведомления, включающую процедуру реагирования на события с описанием мер, которые необходимо предпринять при получении сообщения об инциденте. С этой процедурой должны быть ознакомлены все сотрудники и подрядчики, на которых возлагается также обязанность немедленного сообщения о возникающих инцидентах. Должна быть

реализована соответствующая обратная связь, позволяющая после рассмотрения и устранения инцидента уведомить об этом лиц, доложивших об инциденте. Подобные инциденты могут использоваться при обучении пользователей (6.2) в качестве примеров того, что может случиться, как реагировать на подобные инциденты и как избежать их в будущем (12.1.7).

**6.3.2** Уведомление об уязвимых местах в системе безопасности

На пользователей информационных услуг должна возлагаться обязанность уведомлять об обнаружении любых недостатков в системе безопасности, или предполагаемых уязвимых мест, или угроз системам или услугам. Пользователи должны о подобных случаях незамедлительно уведомлять свое непосредственное руководство или поставщиков соответствующих услуг. Необходимо информировать пользователей о том, что ни при каких обстоятельствах они не должны пытаться.самостоятельно исправлять предполагаемые недостатки в системе защиты. Это нужно для защиты самих пользователей, поскольку их действия по исправлению недостатков могут быть истолкованы как попытки несанкционированного использования системы.

6.3.3 Уведомление о сбоях программного обеспечения

Следует установить процедуры сообщения о сбоях программного обеспечения. При этом следует предусмотреть следующие действия:

а) записать "симптомы" и все сообщения, появляющиеся на экране;

Ь) изолировать, если возможно, компьютер и прекратить работу. Немедленно сообщить о сбое в службу технической поддержки информационных систем. Если оборудование подлежит осмотру, то его необходимо отсоединить от сетей организации прежде, чем снова включить питание. Не использовать на других компьютерах дискеты, записанные на этом компьютере;

с) немедленно сообщить о происшествии администратору информационной безопасности.

Ни при каких обстоятельствах пользователи не должны пытаться удалить подозрительное программное обеспечение. Восстановление программного обеспечения должны выполнять специалисты, имеющие соответствующие знания и опыт работы.

**6.3.4** Использование накапливаемого в процессе инцидентов опыта

Следует реализовать механизмы, позволяющие количественно оценивать и осуществлять мониторинг типов, объемов и стоимости происходящих инцидентов и сбоев. Получаемая информация должна использоваться для идентификации повторяющихся или наиболее важных инцидентов или неисправностей. Данные механизмы позволят в случае необходимости ввести повышенный или дополнительный контроль с целью ограничения частоты, ущерба или затрат на будущие сбои или учесть результаты такого контроля в процессе анализа политики безопасности (3.1.2).

**6.3.5** Процедура наложения дисциплинарных взысканий

Следует определить формальную процедуру наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые в организации политику и процедуры безопасности (6.1.4. и для сбора доказательств 12.1.7). Эта процедура должна служить сдерживающим фактором для сотрудников, которые склонны пренебрегать процедурами защиты. Кроме того, она должна обеспечивать правильное и справедливое рассмотрение дел сотрудников, подозреваемых в серьезном или постоянном нарушении безопасности.

**7 Физическая безопасность и безопасность окружающей среды**

**7.1 Защищенные области**

Задача: предотвратить несанкционированный доступ и нанесение ущерба производственным помещениям, а также несанкционированный доступ, уничтожение и искажение производственной информации.

Средства обработки критической или конфиденциальной информации должны быть размещены в защищенных областях с соответствующими защитными барьерами и контролируемым входом. Они физически должны быть защищены от несанкционированного доступа, повреждения и помех.

Обеспечиваемая защита должна соответствовать идентифицированному риску. Для уменьшения риска несанкционированного доступа или повреждения бумажной документации, носителей и средств обработки информации рекомендуется задать четкие правила использования рабочего стола.

7.1.1 Физический периметр безопасности

Для реализации физической защиты можно создать несколько физических барьеров вокруг производственных помещений и средств обработки информации. Каждый барьер создает внешнюю границу безопасности, усиливая предоставляемую общую защиту. Организации должны использовать внешние границы безопасности для защиты площадей, на территории которых находятся средства обработки информации (7.1.3). Периметр безопасности - это все, что создает барьер, например стена, контролируемый вход по пропускам или управляемый приемный пульт. Месторасположение и прочность каждого барьера выбирается в зависимости от результатов оценки риска.

В соответствующих случаях надо рассмотреть и реализовать следующие рекомендации и средства:

а) периметр безопасности должен быть четко определен;

Ь) периметр безопасности, представляющий собой строение или участок с расположенными на нем средствами обработки информации, должен быть физически исправным (т. е. без брешей в периметре или областях, наличие которых облегчает проникновение). Внешние стены объекта должны представлять собой прочные конструкции, и все внешние двери должны быть соответствующим образом защищены от несанкционированного доступа, например механизмами контроля, барьерами, сигналами тревоги, замками и т. д.;

с) должен быть установлен контролируемый пропускной пункт или другие средства контроля физического доступа к месторасположению объекта или в помещение. Доступ к месторасположению объекта и в помещения должен устанавливаться только авторизованному персоналу;

с!) физические барьеры должны, при необходимости, простираться от пола до потолка, чтобы предотвратить несанкционированный доступ в помещение и загрязнение окружающей среды от таких последствий, как последствия пожара или наводнения;

е) на все пожароопасные двери периметра безопасности должна быть поставлена сигнализация и они должны запираться при закрывании.

7.1.2 Физический контроль доступа

В защищенных областях следует установить надлежащий контроль доступа, чтобы его имел только персонал, наделенный соответствующими полномочиями. Рекомендуется применять следующие меры контроля:

а) за посетителями защищенных областей необходимо установить контроль, а дата и время их входа и выхода должны регистрироваться. Посетителям должен быть предоставлен доступ для конкретных авторизованных целей, с соответствующими инструкциями относительно требований безопасности, которые должны выполняться в данной области, и инструкциями на случай аварийной ситуации;

Ь) доступ к конфиденциальной информации и средствам обработки информации должен контролироваться и предоставляться только авторизованному персоналу. Для предоставления и проверки права на доступ надо использовать аутентификационный контроль, например карточки и личные идентификаторы. На надлежащем уровне должен вестись журнал аудита;

с) весь персонал, работающий в защищенных областях, должен иметь на одежде визуальную идентификацию; кроме того, следует дать ему право спрашивать пропуск у никем не сопровождаемых незнакомых лиц и лиц без визуальной идентификации на одежде;

а1) права на доступ в защищенные области должны регулярно пересматриваться и обновляться.

7.1.3 Защита офисов, комнат и средств

Защищенная область может представлять собой закрытый офис или несколько комнат, расположенных в пределах физического периметра безопасности, которые могут закрываться или иметь в своем составе закрываемые кабинеты или сейфы. При выборе и проектировании защищенной области необходимо принимать во внимание взрывоопасность, пожароопасность, возможность наводнения, . гражданского неповиновения или других природных или техногенных катастроф. Необходимо также учитывать соответствующие действующие санитарные правила, нормы и требования стандартов по охране труда. Кроме того, надо принимать во внимание угрозы безопасности со стороны соседних помещений, например затопление их водой.

Следует рассмотреть следующие меры:

а) основное оборудование должно быть размещено как можно дальше от общедоступных мест;

Ь) здания не должны привлекать внимание и выдавать свое назначение; не должно быть явных признаков как снаружи, так и внутри здания, указывающих на присутствие вычислительных ресурсов;

с) вспомогательное оборудование (например, фотокопировальные аппараты, факс-аппаратура) должно быть размещено так, чтобы уменьшить риск несанкционированного доступа к защищенным областям или компрометации конфиденциальной информации;

а1) в отсутствие персонала двери и окна должны быть закрыты. Следует рассмотреть возможность защиты окон снаружи, особенно на первом этаже;

е) для всех внешних дверей и доступных окон следует установить соответствующие системы обнаружения вторжения, установленные в соответствии со стандартами и регулярно тестируемые. В отсутствие персонала защищаемые области должны все время находиться на сигнализации. Это же относится и к другим местам, например помещениям с компьютерами или средствами связи;

!) средства обработки информации, которыми управляет организация, должны быть физически отделены от средств, управляемых сторонними организациями;

д) адресные книги и книги внутренних телефонов, указывающие на месторасположение средств обработки конфиденциальной информации, не должны быть общедоступными;

п) горючие и другие материалы, использование которых связано с риском, должны надежно храниться на безопасном расстоянии от защищенной области;

|) резервное оборудование и носители информации, на которых хранятся резервные копии, следует размещать на безопасном расстоянии, чтобы избежать их повреждения в случае аварии на основном рабочем месте.

7.1.4 Работа в защищенной области

Для повышения уровня безопасности защищенной области может потребоваться проведение дополнительного контроля и мер безопасности. Они включают контроль за персоналом или сторонними организациями, работающими в защищенной области, а также за действиями сторонней организации, предпринимаемыми в данной области. Необходимо предусмотреть следующие средства контроля:

а) персонал должен быть только на необходимом уровне уведомлен о существовании защищенной области или осуществляемой в ней деятельности;

Ь) по соображениям безопасности и с целью пресечения несанкционированной деятельности в защищенной области необходимо избегать проведения работ без надзора;

с) свободные защищенные области должны быть закрыты на замок и подвергаться периодической проверке;

й) персоналу сторонних организаций, обеспечивающему поддержку сервиса, ограниченный доступ в защищенные области или к средствам обработки конфиденциальной информации должен предоставляться только по необходимости;

е) допуск к фотоаппаратам, видео- или аудиомагнитофонам или к другому записывающему обору дованию без соответствующего разрешения не допускается.

7.1.5 Изолированные области разгрузки и загрузки оборудования и материалов

Области разгрузки и загрузки должны контролироваться, чтобы избежать несанкционированного доступа, и по возможности должны быть изолированы от средств обработки информации. Требования безопасности для таких областей следует определять, исходя из оценки рисков. Предлагаются следующие рекомендации:

а) доступ к складским помещениям снаружи здания должен предоставляться только проверенному персоналу, имеющему соответствующие полномочия;

Ь) складское помещение должно быть спланировано так, чтобы материалы можно было разгружать без получения доступа в другие помещения здания;

с) внешняя дверь (двери) в складское помещение должна быть заперта, когда открыта внутренняя дверь;

а1) необходимо установить, какую потенциальную опасность могут представлять собой поступающие материалы (7.2.1 с1), прежде чем их переместить из складского помещения к месту назначения;

е) в соответствующих случаях (5.1) поступающий материал должен регистрироваться на входе в объект.

**7.2 Защита оборудования**

Задача: предотвратить потерю, повреждение и компрометацию активов, а также перебои в работе организации.

Необходимо обеспечить физическую защиту оборудования от угроз нарушения безопасности и опасностей, представляемых окружающей средой.

Защита оборудования информационных систем (включая оборудование, используемое за пределами организации) необходима как для того, чтобы уменьшить риск несанкционированного доступа к данным, так и для того, чтобы не допустить его потерю или повреждение. Следует также уделить внимание проблемам размещения оборудования и его утилизации. Могут потребоваться специальные меры защиты от несанкционированного доступа и других опасностей, а также для защиты вспомогательного оборудования, например системы электропитания и кабельной разводки.

**7.2.1** Размещение и защита оборудования

Оборудование должно быть размещено и защищено так, чтобы уменьшить риск, связанный с угрозами и опасностями со стороны окружающей среды, и предотвратить несанкционированный доступ. Предлагаются следующие рекомендации:

а) оборудование следует размещать так, чтобы свести к минимуму излишний доступ в рабочую область;

Ь) средства обработки и хранения информации, предназначенные для обработки конфиденциальных данных, должны быть размещены так, чтобы уменьшить риск утечки информации в процессе их использования;

с) области, требующие специальной защиты, должны быть изолированы, чтобы понизить необходимый уровень общей защиты;

а1) необходимо осуществлять контроль с целью минимизации риска потенциальных угроз, включая:

1. кражу;
2. пожар;
3. взрыв;
4. задымление;
5. затопление (или сбои в поставке воды);
6. запыление;
7. вибрацию;
8. влияние химических веществ;
9. помехи в электропитании; 10) электромагнитную радиацию;

е) следует запретить прием пищи и курение вблизи средств обработки информации;

*Т)* необходимо осуществлять наблюдение за условиями окружающей среды, которые могут оказать неблагоприятное воздействие на работу средств обработки информации;

д) следует рассмотреть возможность использования специальных методов защиты для оборудования в промышленных средах, таких как мембранные клавиатуры;

п) следует рассмотреть возможное влияние бедствий на близлежащей территории, например пожар в соседнем здании, течь с крыши или затопление подвальных помещений, взрыв на улице.

**7.2.2** Источники электропитания

Оборудование необходимо защищать от сбоев в системе электропитания и других неполадок в электрической сети. Источник питания должен соответствовать спецификациям производителя оборудования.

Условия обеспечения бесперебойной поставки электроэнергии включают:

а) резервные источники питания, позволяющие исключать сбой в поставке электроэнергии в одном узле;

Ь) источник бесперебойного питания;

с) дублирующий генератор.

Для оборудования, поддерживающего критически важные производственные операции, рекомендуется установить источник бесперебойного питания для обеспечения надлежащего завершения или бесперебойности в работе. План действий в чрезвычайных ситуациях должен включать меры, которые необходимо принять при отказе источника бесперебойного питания. Оборудование, работающее с источниками бесперебойного питания, необходимо регулярно тестировать относительно адекватности его мощности и в соответствии с рекомендациями изготовителя.

7.2.3 Защита кабельной разводки

Кабели электропитания и сетевые кабели передачи данных необходимо защищать от вскрытия с целью перехвата информации и повреждения. Предлагается реализовать следующие защитные меры:

а) кабели электропитания и линии связи, идущие к средствам обработки информации, должны быть по возможности проведены под землей или защищены надлежащим образом с помощью других средств;

Ь) сетевые кабели должны быть защищены от несанкционированного вскрытия с целью перехвата информации и повреждения, например путем использования экранов или прокладки этих линий таким образом, чтобы они не проходили через общедоступные места;

с) для предотвращения помех кабели электропитания должны быть отделены от кабелей передачи информации;

с1) для уязвимых или критически важных систем следует рассмотреть необходимость принятия дополнительных мер, таких как:

1. установка экранированных проводников или использование запираемых помещений, боксов в точке приема и конечной точке;
2. использование альтернативных маршрутов или сред передачи данных;
3. использование оптоволоконных кабелей;
4. удаление несанкционированных приборов, присоединенных к кабелям.

7.2.4 Техническое обслуживание оборудования

Необходимо осуществлять надлежащее техническое обслуживание оборудования, чтобы' обеспечить его постоянную работоспособность и доступность. Предлагаются следующие рекомендации:

а) техническое обслуживание оборудования должно осуществляться через промежутки времени, рекомендуемые поставщиком, и в соответствии с инструкциями;

Ь) ремонт и обслуживание оборудования должен выполнять только персонал, имеющий соответствующие полномочия;

с) необходимо регистрировать все подозреваемые и фактические неисправности, все действия по профилактике и ремонту;

д) при отправке оборудования для обслуживания за пределы помещения необходимо предпринять соответствующие меры (7.2.6) относительно удаления, разрушения и перезаписи данных. Необходимо выполнить все условия страхования.

7.2.5 Защита оборудования, используемого за пределами организации

Использование оборудования для обработки информации за пределами организации должно быть санкционировано (независимо от того, кто им владеет) руководством. Обеспечиваемый уровень защиты такого оборудования должен быть таким же, как и для оборудования, расположенного на территории организации и используемого для таких же целей, принимая в расчет риск работы за пределами организации. Оборудование по обработке информации включает все виды персональных компьютеров, калькуляторов, мобильные телефоны, бумагу и другое оборудование, используемое для работы на дому и транспортированное из обычного месторасположения. Предлагаются следующие рекомендации:

а) оборудование и носители информации, взятые из организации, не должны оставляться в общедоступных местах без присмотра. Во время поездок портативные компьютеры должны перевозиться как ручной багаж и с возможной маскировкой;

Ь) следует всегда соблюдать инструкции изготовителя, касающиеся защиты оборудования, например защищать его от воздействия сильных электромагнитных полей;

с) уровень контроля за работой на дому должен определяться исходя из оценки риска. В соответствии с этим применяется такой контроль, как закрытие на замок кабинетов с картотекой файлов, соблюдение политики чистого рабочего стола, контроль доступа к компьютеру;

с1) для защиты оборудования за пределами организации необходимо обеспечить соответствующие меры по страхованию.

Риски нарушения безопасности (например, повреждения, кражи, прослушивания) могут значительно изменяться при перемещении, что следует обязательно учитывать при определении наиболее подходящих защитных средств. Дополнительная информация о других аспектах защиты мобильного оборудования - по 9.8.1.

**7.2.6** Надежная передача или повторное использование оборудования

Информация может быть скомпрометирована вследствие небрежной передачи или повторного использования оборудования (8.6.4). Запоминающие устройства, содержащие конфиденциальную информацию, должны быть физически уничтожены или надежно перезаписаны вместо того, чтобы использовать стандартные функции удаления информации.

Все компоненты оборудования, содержащего носители информации, например жесткие диски, необходимо проверять, чтобы гарантировать, что конфиденциальные данные и лицензированное программное обеспечение было до передачи оборудования удалено или перезаписано. Поврежденные запоминающие устройства, содержащие конфиденциальные данные, могут потребовать оценки рисков для того, чтобы определить, следует ли их уничтожать, ремонтировать или избавиться от них.

**7.3 Общий контроль**

Задача: предотвратить компрометацию или кражу информации и средств обработки информации.

Информация и средства обработки информации должны быть защищены от раскрытия, изменения или кражи неполномочными лицами, а для минимизации потери или разрушения должен осуществляться соответствующий контроль.

Процедуры обработки и хранения рассматриваются в 8.6.3.

**7.3.1** Политика чистого рабочего стола и чистого экрана

Организациям настоятельно рекомендуется ввести правила использования чистого рабочего стола, касающиеся документов и дискет, чтобы уменьшить риск несанкционированного доступа, потери и повреждения информации в рабочее и нерабочее время. Данная политика должна принимать во внимание уровень конфиденциальности информации (5.2), соответствующий риск и этические нормы, принятые в организации.

Информация, оставленная на рабочих столах, может быть также повреждена или уничтожена в результате аварии, например пожара, наводнения или взрыва.

Предлагаются следующие рекомендации:

а) бумажная документация и дискеты, когда они не используются, должны храниться в специальных шкафах или другой надежной мебели, особенно в нерабочее время;

Ь) конфиденциальная или критически важная производственная информация, когда она не используется, должна храниться под замком (лучше всего в несгораемом сейфе или шкафу), особенно в условиях отсутствия в помещении людей;

с) персональные компьютеры, компьютерные терминалы и принтеры не должны находиться без надзора после того, как пользователь зарегистрировался (подключился к системе, вошел в систему), и должны быть защищены с помощью блокировки с ключом, паролей или других средств контроля;

с!) следует рассмотреть необходимость защиты входящей и исходящей почты, а также факсимильных и телексных устройств, оставленных без присмотра;

е) в нерабочее время фотокопии должны храниться под замком (или защищены от несанкционированного использования каким-то другим способом);

т) после печати конфиденциальной или грифованной информации ее необходимо сразу удалить из принтера.

**7.3.2** Вынос имущества за пределы организации

Оборудование, информация или программное обеспечение не могут быть вынесены за пределы организации без соответствующей санкции. При необходимости и в соответствующих случаях оборудование исключается из журнала регистрации и обратно регистрируется при возвращении. Для выявления несанкционированного перемещения собственности следует проводить местные проверки. Люди должны уведомляться о предстоящем проведении местной проверки.

**8 Управление коммуникациями и процессами**

**8.1 Рабочие процедуры и ответственность**

Задача: обеспечить корректную и надежную работу средств обработки информации.

Необходимо определить ответственность и процедуры по управлению и обеспечению функционирования всех средств обработки информации. Это включает разработку соответствующих рабочих инструкций и процедур реагирования на инциденты.

Для уменьшения риска небрежного или несанкционированного использования систем следует в соответствующих случаях применять принцип разделения обязанностей (8.1.4).

8.1.1 Документированные операционные процедуры

Операционные процедуры, определенные политикой безопасности, рекомендуется документировать и поддерживать. Операционные процедуры рекомендуется рассматривать как формальные документы, изменения в которые можно вносить только после их утверждения руководством, наделенным соответствующими полномочиями.

Процедуры должны включать в себя подробные инструкции по выполнению каждого задания, включая:

а) корректное оперирование информацией;

Ь) требования к планированию выполнения заданий, включая взаимосвязи с другими системами, а также самое раннее и самое позднее время начала и окончания выполнения заданий;

с) инструкции по обработке ошибок и других исключительных ситуаций, которые могут возникнуть во время выполнения заданий, в том числе ограничения на использование системных обслуживающих программ (9.5.5);

с1) обращение за помощью к персоналу поддержки в случае возникновения неожиданных операционных или технических трудностей;

е) специальные инструкции по оперированию с выходными данными, такими как использование специальной бумаги для печатающих устройств или управление конфиденциальными выходными данными, включая процедуры, обеспечивающие безопасность удаленного вывода информации при сбоях;

т) процедуры перезапуска и восстановления работоспособности систем, используемые в случае отказа систем.

Документированные процедуры должны быть также подготовлены для работы по обслуживанию систем, связанных с обработкой информации и средствами связи, такими как запуск и завершение работы компьютеров, резервное копирование данных, техническое обслуживание оборудования, управление компьютерными залами, обработка электронной почты и обеспечение их защиты.

8.1.2 Контроль текущих изменений в информационной системе

Внесение изменений в средства и системы обработки информации необходимо контролировать. Неадекватный контроль внесения изменений в системы и средства обработки информации является распространенной причиной их отказов и нарушения режима безопасности. Поэтому следует определить формальные процедуры управления и ответственность за обеспечение жесткого контроля всех изменений в оборудовании, программном обеспечении или процедурах. Предметом строгого контроля вносимых изменений должны быть используемые программы. При внесении изменений в программу должен сохраняться протокол аудита, содержащий всю связанную с этими изменениями информацию. Изменения в операционной среде могут влиять на приложения. По возможности контроль изменений в системных и прикладных процедурах должен быть полным (10.5.1). В частности, необходимо рассмотреть:

а) выявление и регистрацию существенных изменений;

Ь) оценку возможных последствий от таких изменений;

с) формальную процедуру утверждения предлагаемых изменений;

а1) доведение деталей предлагаемых изменений до сведения всех заинтересованных лиц;

е) процедуры и обязанности по ликвидации неудачных изменений и восстановлению систем после их внесения.

8.1.3 Процедуры управления в случае инцидентов

Для обеспечения своевременного, эффективного и организованного реагирования на инциденты, таящие угрозу безопасности, необходимо определить соответствующие процедуры управления и ответственность за их выполнение (6.3.1). Предлагаются следующие рекомендации:

а) процедуры должны включать в себя все возможные типы инцидентов в системе безопасности, в том числе:

1. отказы систем и потеря обслуживания;
2. отказ в обслуживании;
3. ошибки, возникающие от неполноты или неточности производственных данных;
4. случаи нарушения конфиденциальности.

Ь) кроме обычного плана действий в экстремальных ситуациях, процедуры должны включать в себя:

1. анализ и выявление причины инцидента;
2. планирование и реализацию мер по предотвращению повторения инцидента;
3. ведение контрольного журнала регистрации событий и сбор аналогичной информации;
4. взаимодействие с пользователями и другими лицами, пострадавшими от инцидента или участвующими в процессе восстановления систем;
5. сообщение руководству о выполненных действиях;

с) ведение и защита контрольного журнала регистрации событий (12.1.7), а также сбор и защита аналогичной информации, необходимой для:

1. анализа внутренних проблем;
2. использования в качестве свидетельства возможного нарушения условий контракта, нару шения технических нормативов или в случае судебных разбирательств, попадающих под законода тельство о несанкционированном использовании компьютера или защите данных;

3) ведения переговоров с поставщиками программных средств и услуг о выплате компенсации; а1) необходимо осуществлять тщательный и формальный контроль над мерами по восстановлению

систем после нарушения режима безопасности и их отказов. Процедуры должны обеспечивать следующее:

1. предоставление разрешения на доступ к рабочим системам и данным только точно иденти фицированному и имеющему соответствующие полномочия персоналу (по вопросу доступа сторонних организаций 4.2.2);
2. подробное документирование всех мер, предпринимаемых в чрезвычайных ситуациях;
3. доведение мер, предпринимаемых в чрезвычайных ситуациях, до сведения руководства и их организованный анализ;
4. подтверждение целостности производственных систем и средств управления безопасно стью с минимальной задержкой.

8.1.4 Разделение обязанностей

Разделение обязанностей - это метод уменьшения риска небрежного или несанкционированного использования систем. Следует рассмотреть разделение управления по выполнению определенных обязанностей и областей ответственности, чтобы уменьшить возможность несанкционированного изменения или использования информации или сервиса.

Для небольших организаций реализация данного метода может быть затруднительна, однако указанный принцип должен применяться настолько, насколько это возможно и практически реализуемо. В случае, когда разделение осуществить трудно, следует рассмотреть другие виды контроля, такие как текущий контроль выполняемых действий, журналов аудита и организационный управленческий супервизор. Важно, чтобы аудит безопасности оставался независимым.

Необходимо следить, чтобы в областях единоличной ответственности ни одно лицо не могло совершить обмана, который останется нераскрытым. Инициализация события должна быть отделена от его санкционирования. Следует использовать следующие виды контроля:

а) важно разделить действия, которые допускает сговор с целью мошенничества, например утверждение порядка проведения закупки и проверка того, какие товары получены;

Ь) если существует опасность сговора, то можно ввести контроль, для чего нужно привлечь не менее двух человек и таким образом снизить возможность незаконной сделки.

8.1.5 Разделение процессов разработки и использования рабочих программ

Для достижения разделения обязанностей важно разделение процессов разработки программных средств, их тестирования и использования системных программных средств. Следует определить и представить в виде документов правила передачи программного обеспечения после разработки к эксплуатации.

Работы, связанные с разработкой и тестированием систем, могут привести к серьезным проблемам, например к нежелательному изменению файлов, среды функционирования системы или системному сбою. Для предотвращения возникновения проблем при эксплуатации следует обеспечить необходимый уровень разделения между средами эксплуатации, тестирования и разработки. Аналогичное разделение необходимо произвести также между функциями разработки и тестирования. В этом случае существует потребность в поддерживании хорошо изученной и устойчивой среды, в которой можно производить результативное тестирование и предотвращать нежелательное вмешательство разработчика.

Если персонал, занимающийся разработкой и тестированием, имеет доступ к операционной системе и связанной с ней информацией, он может внедрить несанкционированный скрытый код или изменить данные операционной системы. В некоторых системах эта возможность может использоваться для совершения мошенничества или внедрения непроверенного или вредоносного кода.Непроверенный или вредоносный код может вызвать серьезные проблемы в работе системы. Разработчики и специалисты по тестированию могут также создать угрозу конфиденциальности рабочей информации.

Действия по разработке и тестированию могут вызвать непреднамеренное изменение программного обеспечения и информации, использующих одну вычислительную среду. С целью уменьшения риска непреднамеренного изменения или несанкционированного доступа к действующему программному обеспечению и производственным данным желательно произвести разделение процессов разработки, тестирования и эксплуатации действующих средств. Необходимо предусмотреть следующее:

а) разрабатываемое программное обеспечение и системное программное обеспечение должны по возможности выполняться на разных процессорах или в разных директориях/сегментах сети;

Ь) разработку и тестирование необходимо проводить раздельно;

с) если нет необходимости, то компиляторы, редакторы и другие системные сервисные программы не должны храниться вместе с рабочими системами;

о!) чтобы избежать ошибки, следует использовать разные процедуры входа в операционные и тестируемые системы. Необходимо приучать пользователей к использованию разных паролей для входа в эти системы, а система меню должна выводить на экран соответствующие идентификационные сообщения;

е) там, где для поддержки рабочей системы уместен контроль над созданием паролей, персонал разработчиков должен иметь доступ только к рабочим паролям. Контроль должен гарантировать замену таких паролей после использования.

8.1.6 Внешнее управление средствами обработки информации

Привлечение подрядчика со стороны к управлению средствами обработки информации может привести к дополнительному риску нарушения режима безопасности, такому как возможность компрометации, повреждения или потери данных подрядчиком. Необходимо заблаговременно выявить такой риск и включить в контракт надлежащие защитные меры по его уменьшению, согласованные с подрядчиком (относительно рекомендаций по заключению контрактов со сторонней организацией с предоставлением доступа к программным и аппаратным средствам организации и контрактов на выполнение работ сторонними организациями по 4.2.2. и 4.3).

Следует рассмотреть следующие вопросы:

а) идентификацию особо уязвимых или критически важных приложений, вынос которых за пределы организации нежелателен;

Ь) получение санкции на использование производственных приложений от их владельцев;

с) последствия для планов обеспечения бесперебойной работы организации;

а1) стандарты безопасности, подлежащие определению, и процесс проверки их соблюдения;

е) назначение специальных обязанностей и процедур для эффективного слежения за всей деятельностью, связанной с безопасностью;

т) обязанности и процедуры по уведомлению об инцидентах в системе безопасности и реагированию на них (8.1.3).

**8.2 Планирование систем и их приемка**

Задача: свести риск отказов систем к минимуму.

Для обеспечения доступности ресурсов и надлежащей загрузки систем требуется заблаговременное планирование и подготовка.

Чтобы уменьшить риск перегрузки систем необходимо оценить будущие потребности в их загрузке на основе прогноза.

Эксплуатационные требования к новым системам следует определить, документально оформить и проверить до приемки и использования систем.

**8.2.1** Планирование производительности

Для обеспечения надлежащей производительности компьютеров и емкости запоминающих устройств следует оценить будущие потребности в их загрузке на основе прогноза. Этот прогноз должен учитывать требования к новым производствам и системам, а также текущие и прогнозируемые тенденции организации в обработке информации.

Большие ЭВМ требуют особого внимания вследствие гораздо большей стоимости повышения их производительности и необходимого для этого времени. Администраторы больших ЭВМ должны постоянно следить за использованием ключевых системных ресурсов, включая процессоры, основную

оперативную память, файловые запоминающие устройства, принтеры и другие устройства вывода, а также коммуникационные системы. Они должны определить тенденции использования ресурсов, особенно это касается использования производственных приложений или средств управления информационной системы.

Администраторы должны использовать эту информацию для выявления и устранения возможных уязвимых мест, которые могут представлять угрозу системе безопасности или пользовательским сервисам, и планировать надлежащие меры по исправлению ситуации.

8.2.2 Приемка систем

Для приемки новых информационных систем, модернизированных систем и новых версий систем должны быть установлены критерии, а соответствующее тестирование систем должно быть проведено до их приемки. Администраторы должны гарантировать, что требования и критерии приемки четко определены, согласованы, документированы и протестированы. Следует проконтролировать:

а) требования к производительности и загрузке компьютеров;

Ь) подготовку процедур восстановления и перезапуска систем после сбоев, а также планов действий в экстремальных ситуациях;

с) подготовку и тестирование повседневных операционных процедур в соответствии с заданными стандартами;

а1) согласованность множества соответствующих средств контроля за безопасностью;

е) эффективность процедур ручного управления;

т) производственные соглашения;

д) указания на то, что установка новой системы не будет иметь пагубных последствий для функционирующих систем, особенно в моменты пиковой нагрузки на процессоры (например, в конце месяца);

п) эффект, который новая система оказывает на общую безопасность организации;

|) готовность персонала к использованию новых систем.

Для обеспечения эффективной работы предлагаемой системной конфигурации следует консультироваться по вопросам поддерживания ее работоспособности на всех стадиях процесса разработки новых систем. Для подтверждения полного соответствия всем критериям приемки систем необходимо провести соответствующие испытания.

**8.3 Защита от вредоносного программного обеспечения**

Задача: обеспечить целостность данных и программ

Для предотвращения и выявления случаев внедрения вредоносного программного обеспечения требуется принятие надлежащих мер предосторожности.

Программное обеспечение и средства обработки информации уязвимы относительно внедрения вредоносных кодов, таких как "компьютерные вирусы", "сетевые черви", "троянские кони" и "логические бомбы". Пользователи должны быть всегда готовы к опасности проникновения несанкционированного или вредоносного программного обеспечения, а администраторы в соответствующих случаях должны принимать специальные меры по предотвращению или обнаружению их внедрения. В частности, крайне важно принять меры предосторожности для предотвращения и обнаружения компьютерных вирусов на персональных компьютерах.

**8.3.1** Контроль, противодействующий внедрению вредоносного программного обеспечения

Необходимо реализовать меры по обнаружению и предотвращению вредоносного программного обеспечения и процедуры информирования пользователей об их вреде. В основе защиты от вредоносного программного обеспечения должны лежать хорошие знания и понимание правил безопасности, надлежащие средства управления доступом к системам и административный контроль изменений. Следует проконтролировать:

а) выполнение формальной политики, требующей соблюдения условий лицензий на использование программного обеспечения и запрещающей использование несанкционированных программ (12.1.2.2);

Ь) выполнение формальной политики, направленной на защиту от опасностей, связанных с получением файлов и программного обеспечения через внешнюю сеть или с помощью другого носителя, с указанием необходимых мер защиты (10.5, 10.5.4 и 10.5.5);

с) процесс инсталляции и регулярного обновления средств обнаружения и устранения программных вирусов, которые следует применять при проверке компьютеров и носителей информации на наличие известных вирусов либо как меру предосторожности;

*6)* программы и данные в системах, поддерживающих критически важные производственные процессы. Наличие случайных файлов и несанкционированных исправлений должно быть расследовано с помощью формальных процедур;

е) все файлы на электронных носителях неизвестного или несанкционированного происхождения или файлы, полученные по ненадежным сетям, на наличие вирусов до их использования;

т) все подключения и загрузки электронной почты на наличие вредоносного кода до их использования. Эта проверка может быть проведена, например, на серверах электронной почты, настольных компьютерах или при входе в сеть организации;

д) управленческие процедуры и обязанности, связанные с защитой системы от вирусов, обучение работе с этими средствами, уведомление и отражение вирусных атак (6.3 и 8.1.3);

п) планы обеспечения бесперебойной работы организации на случай вирусного заражения, в том числе планы резервного копирования всех необходимых данных, программ и их восстановления (раздел 11);

*\)* процедуры проверки всей информации, имеющей отношение к вредоносному программному обеспечению и обеспечение точности и информативности предупреждающих сообщений. Администраторы должны гарантировать использование квалифицированных источников, например серьезных журналов, надежных сайтов Интернета или надежных поставщиков антивирусного программного обеспечения. Персонал должен быть осведомлен о проблеме и о том, что делать в случае ее возникновения.

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

**8.4 Обслуживание систем**

Задача: обеспечить целостность и доступность сервиса, связанного с обработкой информации и связью.

Необходимо определить повседневные процедуры для выполнения согласованной стратегии дублирования, снятия резервных копий данных и их повторного и своевременного восстановления, регистрации событий и сбоев, а также, в соответствующих случаях, обеспечить слежение за средой, в которой функционирует оборудование.

**8.4.1** Резервное копирование данных

Резервные копии с критически важной производственной информации и программ должны сниматься регулярно. Для обеспечения возможности восстановления всех критически важных производственных данных и программ после выхода из строя компьютера или отказа носителя информации необходимо иметь надлежащие средства резервного копирования. Процедуры резервного копирования для отдельных систем должны удовлетворять требованиям планов обеспечения бесперебойной работы организации ( раздел 11). Следует проводить следующие мероприятия:

а) минимальный уровень дублирования информации вместе с точными и полными записями о резервных копиях и документированными процедурами восстановления следует хранить в удаленном месте, на достаточном расстоянии для того, чтобы избежать последствий от аварии на основном рабочем месте. Необходимо создать по крайней мере три экземпляра резервных копий данных для важных производственных приложений;

Ь) резервным копиям следует предоставлять соответствующий уровень физической защиты и защиты окружающей их среды, согласующийся с уровнем защиты на главном узле системы. Средства контроля, применяемые к носителям информации на главном узле, следует использовать и для резервных копий;

с) резервные данные необходимо регулярно тестировать, чтобы быть уверенным, что на них можно будет положиться в случае аварии;

с!) процедуры восстановления должны регулярно проверяться и тестироваться для обеспечения их эффективности и возможности завершения восстановления за время, отведенное для этого в рабочих процедурах.

Владельцы данных должны задать период сохранности критически важных производственных данных, а также требования к постоянному хранению архивных копий (12.1.3).

**8.4.2** Журналы регистрации событий

Операторы компьютеров должны вести журнал регистрации своих действий. Этот журнал должен по необходимости включать:

а) время запуска и завершения работы систем;

Ь) системные ошибки и предпринимаемые корректирующие действия;

с) подтверждение корректного оперирования файлами данных и выходной информацией от компьютеров;

*б)* имя лица, совершившего вход в систему.

Журналы регистрации событий должны быть предметом регулярных независимых сверок с рабочими процедурами.

**8.4.3** Регистрация сбоев

Необходимо извещать о сбоях в работе систем и предпринимать соответствующие корректирующие меры. Зафиксированные пользователями сбои, касающиеся проблем с компьютерными и коммуникационными системами, следует заносить в журнал регистрации. Должны существовать четкие правила обработки зарегистрированных сбоев, включая следующие:

а) анализ журнала регистрации сбоев для обеспечения их удовлетворительного разрешения;

Ь) анализ корректирующих мер, цель которого состоит в проверке того, не скомпрометированы ли средства управления безопасностью и является ли предпринятое действие полностью санкционированным.

**8.5 Сетевое администрирование**

Задача: обеспечить защиту информации, циркулирующей в сетях и поддерживающей инфраструктуры.

Управление безопасностью компьютерных сетей, отдельные сегменты которых могут находиться за пределами организации, требует особого внимания.

Возможно, что потребуется принятие специальных мер для защиты конфиденциальных данных, передаваемых по общедоступным сетям.

8.5.1 Средства управления безопасностью сетей

Компьютерные сети требуют целого ряда средств управления безопасностью. Администраторы сетей должны определить надлежащие средства контроля для обеспечения защиты данных, циркулирующих в сетях и в подключенных к ним системах, от несанкционированного доступа. Необходимо предусмотреть следующие меры:

а) ответственность по обеспечению работы сетей и компьютеров должна быть по необходимости разделена (8.1.4);

Ь) необходимо определить обязанности и процедуры по управлению удаленным оборудованием, в том числе оборудованием на рабочих местах пользователей;

с) при необходимости для обеспечения конфиденциальности и целостности данных, передаваемых по общедоступным сетям, и для защиты подключенных к ним систем требуется определение специальных средств контроля (9.4 и 10.3). Специальный контроль может также потребоваться для поддержания доступности сетевого сервиса и соединенных компьютеров;

а1) необходимо координировать работы по администрированию компьютеров и сетей как для оптимизации сервиса для производственных нужд, так и для обеспечения согласованной реализации защитных мер для всей инфраструктуры обработки информации.

**8.6 Оперирование с носителями информации и их защита**

Задача: предотвратить повреждение активов и перебои в работе организации.

Необходимо контролировать компьютерные носители данных и обеспечить их физическую защиту.

Следует определить надлежащие операционные процедуры для защиты документов, компьютерных носителей информации (магнитные ленты, диски, кассеты), входных/выходных данных и системной документации от повреждения, хищения и несанкционированного доступа.

8.6.1 Управление съемными компьютерными носителями информации

Для управления такими съемными носителями информации, как магнитные ленты, диски, кассеты и распечатки, необходимо иметь соответствующие процедуры. Следует использовать следующие меры:

а) стирание предыдущего содержимого с повторно используемых носителей информации, которые подлежат удалению из организации, если они больше не нужны;

Ь) получение письменной санкции на удаление всех носителей информации из организации и регистрация всех случаев их удаления в контрольном журнале (8.7.2);

с) хранение всех носителей информации в надежной, защищенной среде в соответствии с инструкциями производителей.

Все процедуры и уровни полномочий должны быть четко документально оформлены.

8.6.2 Удаление носителей данных

Для удаления компьютерных носителей информации, которые больше не нужны, требуются надежные и проверенные процедуры. Конфиденциальная информация может просочиться за пределы организации и попасть в руки лиц, не имеющих соответствующих прав, вследствие небрежного удаления компьютерных носителей данных. Для сведения такого риска к минимуму следует определить четкие процедуры надежного удаления носителей информации. Предлагаются следующие рекомендации:

а) носители данных, содержащие конфиденциальную информацию, следует хранить в безопасном месте и уничтожать надежным способом, например, путем сжигания или измельчения, или удалять данные так, чтобы можно было использовать эти носители внутри организации для других приложений;

Ь) для идентификации носителей данных, которые могут потребовать надежного удаления, предлагается использовать следующий контрольный список: 1)бумажная документация;

1. голос или другие записи;
2. копировальная бумага;
3. выходные отчеты;
4. одноразовые ленты для принтеров;
5. магнитные ленты;
6. съемные диски или кассеты;
7. оптические носители информации (все виды, включая носители с размещением программного обеспечения промышленным способом);
8. распечатки программ;
9. тестовые данные;
10. системная документация;

с) в некоторых средах возможно будет проще собрать все носители данных и надежно их удалить, чем пытаться выделить из них носители, на которых записана конфиденциальная информация;

с!) многие организации предлагают услуги по сбору и удалению бумажной документации, оборудования и носителей данных. Следует позаботиться о выборе надежного подрядчика с соответствующим опытом работы, использующего надлежащие средства контроля безопасности;

е) каждый случай удаления носителей конфиденциальной информации необходимо (по возможности) регистрировать в контрольном журнале для будущих справок.

При накоплении информации, подлежащей удалению, следует учитывать эффект аккумуляции, который может привести к тому, что большое количество несекретной информации становится более конфиденциальным, чем малое количество секретной информации.

8.6.3 Процедуры оперирования данными

Чтобы защитить конфиденциальные данные от несанкционированного раскрытия или использования, необходимо определить процедуры оперирования и хранения такой информации. Для документов, компьютерных систем, сетей, телексов, магнитных лент, дисков, мобильных вычислений, мобильной связи, отчетов, незаполненных чеков, счетов и других рекомендуется подготовить процедуры для оперирования информацией в соответствии с ее уровнем конфиденциальности (5.2). Следует проводить следующие мероприятия (8.7.2):

а) обработку и маркировку всех носителей (8.7.2а);

Ь) ограничение доступа неполномочному персоналу;

с) формальную регистрацию получателей данных, имеющих соответствующие полномочия;

с!) обеспечение полноты входных данных, должного завершения их обработки и проверки выходных данных;

Ь) уязвимость данных, пересылаемых по электронной почте, по отношению к ошибкам, например неправильная адресация или направление сообщений не по назначению, а также надежность и доступность сервиса в целом;

с) влияние изменения характеристик коммуникационной среды на производственные процессы, например влияние повышенной скорости передачи данных или посылки формальных сообщений от одного лица к другому предпочтительнее, чем от организации к организации;

*6)* правовые соображения, такие как необходимость проверки источника передачи, доставки и приема сообщений;

е) условия опубликования доступных извне списков персонала;

г) необходимость принятия защитных мер для контроля удаленного доступа пользователей к электронной почте.

*8.7.4.2 Политика для электронной почты*

Организация должна проводить четкую политику использования электронной почты, включающую:

а) атаки на электронную почту, например вирусы, перехват сообщений;

Ь) защиту приложений электронной почты;

с) рекомендации об ограничениях на использование электронной почты;

с1) обязанности служащих не компрометировать организацию, например посылкой по электронной почте клеветнических сообщений, использованием электронной почты для преследования, для несанкционированной покупки (10.3);

е) использование криптографических средств для защиты конфиденциальности и целостности электронных сообщений;

т) хранение сообщений, которые могут быть обнародованы в случае судебных процессов;

д) дополнительный контроль при посылке сообщений, которые не могут быть аутентифицированы.

8.7.5 Защита систем электронного офиса

Для контроля риска, связанного с использованием систем электронного офиса, которому подвергаются производственные процессы и система безопасности, требуются четкие правила и рекомендации. Это предоставляет возможности для более быстрого распространения и коллективного использования производственной информации посредством документов, компьютеров, мобильных вычислений, мобильной связи, электронной почты, речевой корреспонденции, речевой связи вообще, комплексного представления информации, почтовых служб/средств и факсов.

Последствия для производственной деятельности и режима безопасности от использования таких средств включают:

а) уязвимость информации в офисных системах, например запись телефонных звонков или запросов на конференции, конфиденциальность запросов, хранение факсов, открытие электронной почты, распределение электронной почты;

Ь) политику и соответствующий контроль для администрирования коллективно используемой информации, например использование корпоративных электронных досок объявлений (9.1);

с) исключение некоторых категорий конфиденциальной производственной информации, если системе не обеспечен соответствующий уровень защиты (5.2);

с1) ограничение доступа к персональной информации, относящейся к избранным лицам, например к персоналу, работающему над конфиденциальными проектами;

е) пригодность (или непригодность) системы для поддержания производственных приложений, таких как упорядочение связи (передачи данных) или предоставление полномочий;

г) категории персонала и подрядчиков или торговых партнеров, которым разрешено использовать систему и места, из которых можно получить доступ к ней (4.2);

д) ограничение на использование определенных средств для конкретных категорий пользователей; п) идентификацию статуса пользователей, например сотрудников организации или подрядчиков,

в каталогах к сведению других пользователей;

■ I) правила, касающиеся периода сохранности и резервного копирования информации, хранимой в системе (12.1.3 и 8.4.1);

.I) требования и процедуры перехода на аварийный режим (11.1).

8.7.6 Системы общего доступа

Необходимо заботиться о защите целостности опубликованной в электронном виде информации, чтобы предотвратить ее несанкционированное изменение, которое может повредить репутации организации, опубликовавшей информацию. Информация в системе общего доступа, например информация на \МеЬ-сервере, доступная через Интернет, может нуждаться в согласовании с законами, правилами и инструкциями в соответствующей для системы области. До того как информация станет общедоступной, она должна пройти формальный процесс санкционирования (наделения ее соответствующими полномочиями).

Программное обеспечение, данные и другая информация, требующая высокого уровня целостности, ставшая доступной в общедоступной системе, должна быть защищена соответствующими механизмами, например цифровой подписью. Электронные издательские системы и особенно те, которые допускают обратную связь и прямой ввод информации, должны тщательно контролироваться для того, чтобы:

а) информация формировалась в соответствии с законодательством по защите данных (12.1.4);

Ь) информация, вводимая и обрабатываемая в издательских системах, обрабатывалась полностью, без искажений и своевременно;

с) конфиденциальная информация защищалась в течение процесса обработки и хранения;

с1) пользователи издательских систем не должны иметь доступа к сети, к которой издательская система подсоединена.

8.7.7 Другие виды информационного обмена

Для защиты информации, обмен которой осуществляется с помощью голоса, факсимиле и средств видеосвязи, необходимы соответствующие процедуры и контроль. При использовании таких средств информация может быть скомпрометирована вследствие недостаточной осведомленности, недостатков в политике или применяемых процедурах (например, подслушивание разговора по мобильному телефону в общественном месте, подслушивание отвечающих машин, несанкционированный доступ к системе с автоматической связью и голосовой электронной почтой или факсимиле, при случайной посылке не тому лицу, использующему факсимильное оборудование).

Производственная деятельность может быть подорвана, а информация скомпрометирована, если вследствие сбоя средств связи происходит перезагрузка или прерывание работы. Информация может быть также скомпрометирована, если к ней могут получить доступ неавторизованные пользователи.

Следует четко сформулировать политику, которой должен следовать персонал, используя голос, факсимиле и видеосвязь. Политика включает:

а) напоминание персоналу, что он должен соблюдать соответствующую предосторожность, например не разглашать конфиденциальную информацию для того, чтобы избежать ее подслушивания или перехвата при телефонном разговоре:

1. людьми, которые находятся в непосредственной близости от него (особенно при использо вании мобильных телефонов);
2. с помощью физического доступа к телефонной трубке, телефонной линии или посредством сканирующего приемника при использовании мобильного аналогового телефона;
3. людьми, находящимися рядом с получателем информации;

Ь) напоминание персоналу, что он не должен вести конфиденциальные разговоры в общественных местах, открытых офисах и назначать встречи в помещениях с тонкими стенами;

с) не оставлять сообщений на отвечающих машинах, так как этим могут воспользоваться неавторизованные лица, хранить сообщения на коллективных системах или некорректно;

с1) напоминание персоналу о проблемах использования факсимильных машин, а именно:

1. несанкционированный доступ с целью встроить банки сообщений для поиска сообщений;
2. преднамеренное или случайное программирование машин для посылки сообщений по спе циальному номеру;

3) посылка документов и сообщений по неправильному номеру или без набора номера, используя неправильно хранимое число.

**9 Управление доступом к системам**

**9.1 Производственные требования к управлению доступом**

Задача: обеспечить контроль доступа к производственной информации.

Доступ к компьютерным системам и данным необходимо контролировать исходя из производственных требований.

Такой контроль должен учитывать правила распространения информации и разграничения доступа, принятые в организации.

**9.1.1** Документированная политика управления доступом к информации

*9.1.1.1 Политика и производственные требования*

Производственные требования к управлению доступом к системам необходимо определить и документально оформить. Правила управления доступом и права доступа для каждого пользователя или группы пользователей должны быть четко сформулированы в положениях политики управления доступом к информации. Пользователи и поставщики услуг должны знать четко сформулированные производственные требования, удовлетворяющие политике управления доступом.

Эта политика должна учитывать следующее:

а) требования безопасности отдельных производственных прикладных программ;

Ь) идентификацию всей информации, связанной с производственными прикладными программами;

с) политику распространения и авторизации информации, например необходимость знать правила и уровни безопасности и классификацию информации;

а1) согласованность между политикой управления доступом и политикой классификации информации различных систем и сетей;

е) соответствующее законодательство и договорные обязательства, касающиеся защиты доступа к данным или сервисам (раздел 12);

т) типовые матрицы доступа пользователей к типовым категориям работы;

д) управление правами доступа в распределенной и сетевой среде, которая признает все типы доступных подключений (соединений).

*9.1.1.2 Правила управления доступом*

При определении правил управления доступом необходимо рассмотреть следующее:

а) различия между правилами, которые всегда должны быть выполнены, и правилами, которые являются необязательными или условными;

Ь) формулировать правила лучше на предпосылке "запрещено все, что явно не разрешено", чем на предпосылке "разрешено все, что явно не запрещено";

с) изменения в информационных метках, которые инициализированы автоматически средствами обработки информации и инициализированы по усмотрению пользователя;

а1) изменения в правах доступа пользователю, которые инициализированы автоматически информационной системой и инициализированы администратором;

е) правила, которые требуют одобрения администратора или кого-либо другого перед вступлением в силу, и те правила, которые не требуют чьего-либо одобрения.

**9.2 Управление доступом пользователей**

Задача: предотвратить несанкционированный доступ к информационным системам.

Для управления процессом предоставления прав доступа к информационным системам и сервисам требуются формальные процедуры.

Эти процедуры должны включать в себя все стадии жизненного цикла управления доступом пользователей - от начальной регистрации новых пользователей до удаления учетных записей поль зователей, которые больше не нуждаются в доступе к информационным системам и сервисам. Особое внимание следует уделить необходимости управления процессом предоставления привилегированных прав доступа, которые позволяют пользователям обойти средства системного контроля.

**9.2.1** Регистрация пользователей

Для предоставления доступа ко всем многопользовательским информационным системам и сервисам рекомендуется применять формальную процедуру регистрации и удаления учетных записей пользователей.

Доступ к многопользовательским информационным сервисам необходимо контролировать посредством формального процесса регистрации пользователей, который должен включать в себя следующие действия:

а) использовать уникальные идентификаторы пользователей для того, чтобы пользователи могли войти в систему и нести ответственность за свои действия. Группу идентификаторов можно использовать только там, где эти идентификаторы являются подходящими для выполняемой работы;

Ь) проверять, предоставлено ли пользователю разрешение от владельца системы на использование информационной системы или сервиса. Также может быть соответствующее отдельное разрешение для управления правами доступа;

с) проверять, достаточен ли предоставленный пользователю уровень доступа к системе для выполнения возложенных на него функций (9.1) и не противоречит ли этот уровень политике безопасности организации, например не компрометирует ли он принцип разделения обязанностей (8.1.4);

с1) предоставлять пользователям их права доступа в письменном виде;

е) потребовать от пользователей подписания обязательства, чтобы показать, что они понимают условия доступа;

т) потребовать от поставщиков услуг, чтобы они не предоставляли доступ к системам до тех пор, пока не будут закончены процедуры определения полномочий;

д) вести формальный учет всех зарегистрированных лиц, использующих систему;

п) немедленно изымать права доступа у тех пользователей, которые сменили работу или покинули организацию;

|) периодически проверять и удалять пользовательские идентификаторы и учетные записи, которые больше не требуются;

.I) проверять, не выданы ли пользовательские идентификаторы, которые больше не нужны другим пользователям.

При заключении контрактов со штатными или обслуживающими исполнителями необходимо учитывать перечисленные выше предложения и определить в контрактах санкции при попытке несанкционированного доступа исполнителями (6.1.4 и 6.3.5).

9.2.2 Управление привилегиями

Использование специальных привилегий (любая особенность или уступка многопользовательской информационной системы, дающая возможность пользователю обойти средства контроля системы или приложения) следует ограничить и контролировать. Предоставление и использование излишних системных привилегий зачастую оказывается одним из основных факторов, способствующих нарушению режима безопасности системы, т. е. ее уязвимости.

Для многопользовательских систем, требующих защиты от несанкционированного доступа, предоставление привилегий рекомендуется контролировать посредством формального процесса определения полномочий следующим образом:

а) идентифицировать привилегии, связанные с каждым программным продуктом, поддерживаемым системой, например с операционной системой, СУБД или любой прикладной программой, а также категории сотрудников, которым их необходимо предоставить;

Ь) предоставлять привилегии отдельным лицам только в случае крайней необходимости и в зависимости от ситуации, т. е. только тогда, когда они нужны для выполнения ими своих функций;

с) реализовать процесс определения полномочий и вести учет всех предоставленных привилегий. Не следует предоставлять привилегии до окончания процесса определения полномочий;

*б)* содействовать разработке и использованию системных программ, чтобы избежать необходи мости предоставления привилегий пользователям;

е) пользователи, которым предоставлены большие привилегии для специальных целей, для обычной работы должны использовать другой пользовательский идентификатор.

9.2.3 Управление пользовательскими паролями

В настоящее время пароли являются основным средством подтверждения полномочий доступа пользователей к компьютерным системам. Назначение паролей необходимо контролировать посредством формального процесса управления, требования к которому должны быть следующими:

а) потребовать от пользователей подписания обязательства по хранению в секрете персональных паролей и паролей рабочих групп исключительно членами этих групп (это требование должно быть включено в пункты и условия при найме на работу по 6.1.4);

Ь) в тех случаях, когда пользователи должны сами поддерживать свои пароли, обеспечить их первоначально надежным временным паролем при условии, что немедленно заменят их. Временные пароли также выдаются в случае, когда пользователи забывают свои пароли. Временные пароли должны выдаваться только после положительной идентификации пользователя;

с) предоставлять временные пароли пользователям надежным способом. Следует избегать передачи паролей через посредников или посредством незащищенных (незашифрованных) сообщений электронной почты. Пользователи должны подтвердить получение паролей.

Пароли нельзя хранить на компьютере в незащищенном виде. Существуют другие технологии для идентификации и аутентификации пользователя, такие как биометрия (проверка подлинности по отпечаткам пальцев); проверка подлинности подписи и использование аппаратных средств, например плат с интегральными схемами, которые следует рассмотреть, если это необходимо.

**9.2.4** Пересмотр прав доступа пользователей

Для обеспечения эффективного контроля за доступом к данным и информационным системам руководство должно реализовывать формальный процесс пересмотра прав доступа пользователей регулярно через определенные промежутки времени. Такой процесс должен обеспечивать следующее:

а) пересмотр прав доступа пользователей через определенные промежутки времени (рекомендуется период 6 месяцев) или после каких-либо изменений (9.2.1);

Ь) пересмотр разрешений на предоставление привилегированных специальных прав доступа (9.2.2) через более короткие промежутки времени, рекомендуемый период 3 мес;

с) проверка предоставленных привилегий через регулярные промежутки времени, для того чтобы не допустить получения пользователями несанкционированных прав доступа.

**9.3 Обязанности пользователей**

Задача: предотвратить несанкционированный доступ пользователей.

Крайне важным условием поддержания надлежащего режима безопасности является участие и помощь зарегистрированных пользователей.

Пользователям рекомендуется знать свои обязанности по обеспечению эффективного контроля доступа, особенно касающиеся использования паролей и защиты пользовательского оборудования.

**9.3.1** Использование паролей

Пользователи должны следовать установленным процедурам поддержания режима безопасности при выборе и использовании паролей.

Пароли являются основным средством подтверждения полномочий доступа пользователей к компьютерным системам. Предлагаются следующие рекомендации по выбору и использованию паролей:

а) хранить пароли в секрете;

Ь) не записывать пароли на бумаге, если не представляется возможным его хранение в защищенном месте;

с) изменять пароли всякий раз, когда есть указания на возможную компрометацию систем или паролей;

*б)* выбирать пароли, содержащие не менее шести символов, которые:

1. легки для запоминания;
2. не основаны на информации, связанной с пользователем, которую можно легко предполо жить или получить, например имена, номера телефонов, даты рождения и т.д.;
3. не состоят только из одних цифр или только из одних букв;

е) изменять пароли через регулярные промежутки времени или через определенное количество доступов в систему (пароли для привилегированных системных ресурсов следует менять чаще, чем обычные пароли) и избегать повторного или "циклического" использования старых паролей;

*1)* изменять временные пароли при первом входе в систему;

д) не включать пароли в сценарии автоматического входа в систему, например в макросы или функциональные клавиши;

п) не использовать совместно с кем-либо индивидуальные пользовательские пароли.

Если пользователям необходим доступ ко многим сервисам или платформам и требуется поддерживать нескольких паролей, то им следует рекомендовать использовать один надежный пароль [а1) выше] для всех сервисов, которые обеспечивают приемлемый уровень защиты хранящегося пароля.

**9.3.2** Пользовательское оборудование, оставленное без присмотра

Пользователи должны обеспечить надлежащую защиту оборудования, оставленного без присмотра. Оборудование, установленное на рабочих площадях, например рабочие станции или файловые серверы, может потребовать специальной защиты от несанкционированного доступа в тех случаях, когда оно остается без присмотра на продолжительное время. Все пользователи и подрядчики должны знать требования безопасности и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты. Предлагаются следующие рекомендации:

а) завершить активные сеансы связи по окончании работы, если их нельзя защитить посредством соответствующей блокировки, например пароля на открытие экрана;

Ь) по окончании сеанса связи с центральным процессором выполнить процедуру выхода из системы (т. е. не ограничиваться только выключением компьютера или терминала);

с) защитить неиспользуемые компьютеры или терминалы от несанкционированного использования с помощью блокировки с ключом или эквивалентного средства контроля, например доступом по паролю.

**9.4 Управление доступом к сети**

Задача: обеспечить защиту систем, объединенных в сеть.

Подключения к системам, объединенным в сеть, следует контролировать. Это необходимо для того, чтобы пользователи и компьютерные системы не нарушали безопасность других сетевых сервисов, для чего:

а) приспособить интерфейсы между сетью организации и сетями, принадлежащими другим организациям, или сетями общего пользования;

Ь) обеспечить надлежащие механизмы аутентификации пользователей и оборудования;

с) осуществлять контроль доступа пользователей к информационным системам.

**9.4.1** Политика использования сетевых сервисов

Подключение к сетевым сервисам без принятия мер защиты может сказаться на безопасности всей организации. Пользователям следует предоставить прямой доступ только к тем сервисам, использование которых им разрешено.

Такой контроль является особенно важным для сетевых подключений к конфиденциальным или критически важным производственным приложениям, а также для пользователей в зонах повышенного риска, например в общедоступных местах или местах, находящихся вне пределов досягаемости администраторов безопасности организации и контроля.

Политика должна быть сформулирована относительно использования сетей и сетевых сервисов. Она должна охватывать следующие аспекты:

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

Ь) процедуры определения полномочий для того, чтобы установить, кому разрешается доступ и к каким сетям и сетевым сервисам;

с) управление средствами контроля и процедурами для защиты доступа к сетям и сетевым сервисам.

Эта политика должна быть согласована с политикой управления доступом, принятой в организации (9.1).

**9.4.2** Принудительная маршрутизация

В ряде случаев путь от пользовательского терминала к компьютерной системе необходимо контролировать. Современные сети предоставляют максимальные возможности для распределения ресурсов и гибкости маршрутизации. Это также дает возможность несанкционированного доступа к производственным приложениям или несанкционированного использования информационных средств. Такой риск можно уменьшить, привлекая средства контроля для ограничения маршрута между пользовательским терминалом и компьютерными системами, доступ к которым пользователю разрешен, например создание принудительного маршрута.

Цель такой принудительной маршрутизации - предотвратить нежелательное "отклонение" пользователей от маршрута между пользовательским терминалом и системами, доступ к которым пользователю разрешен.

Для этого обычно требуется реализация ряда средств контроля в нескольких точках пути. Принцип состоит в том, чтобы ограничить возможности выбора маршрута в каждой точке сети посредством предопределенных вариантов.

Примерами такого ограничения пути являются:

а) предоставление выделенных линий связи или телефонных номеров;

Ь) автоматическое подключение портов к определенным приложениям или шлюзам безопасности;

с) ограничение возможностей выбора опций меню и подменю для отдельных пользователей;

а1) предотвращение неограниченного "блуждания" по сети;

е) предписание использования определенных приложений и/или шлюзов безопасности для внешних сетевых пользователей;

*Г)* активный контроль предоставленного источника для связи адресата через шлюзы безопасности, например межсетевые экраны;

д) ограничение доступа к сети путем установки отдельных логических доменов для групп пользователей в пределах организации, например виртуальных частных сетей (9.4.6).

В основе требований к принудительной маршрутизации должна лежать политика управления доступом, принятая в организации (9.1).

9.4.3 Аутентификация пользователей внешних подключений

Внешние подключения создают возможность несанкционированного доступа к производственной информации, например доступ с помощью методов коммутации. Поэтому необходима аутентификация подключений, осуществляемых удаленными пользователями. Существуют различные методы аутентификации, некоторые из них обеспечивают более высокий уровень защиты, чем другие методы, например методы, основанные на использовании криптографических средств, обеспечивают строгую аутентификацию. Важно оценить риск ущерба для определения уровня требуемой защиты. Это необходимо для определения выбора метода аутентификации.

Аутентификация удаленных пользователей может осуществляться с использованием, например, криптографических, основанных на технических приемах, аппаратных средств или протокола "запрос/ ответ". Использование выделенных частных линий связи или средств проверки сетевых адресов пользователей также дает уверенность в источнике подключений.

Процедуры обратного вызова и средства управления, например использование модемов обратного вызова, могут обеспечить защиту от несанкционированных или нежелательных подключений к средствам обработки информации организации. Этот тип средств управления аутентифицирует удаленных пользователей, пытающихся подключиться к сети организации. При использовании этого средства управления организация не должна использовать сетевые сервисы, которые содержат запрашиваемые данные, или, если использует, то заблокировать возможность применения таких свойств, способствующих использованию уязвимых мест, связанных с отправлением запрашиваемых данных. Также важно, чтобы процесс обратного запроса гарантировал, что действительно произошло разъединение на стороне организации. Иначе удаленный пользователь может захватить открытую линию, притворяясь, что верификация обратного вызова уже произошла. Процедуры обратного вызова и средства управления должны быть полностью протестированы на эту возможность.

9.4.4 Аутентификация узла

Несанкционированный доступ к производственным приложениям может быть осуществлен посредством автоматического подключения удаленного компьютера. Поэтому необходимо аутентифицировать подключения удаленных компьютерных систем. Это особенно важно, если подключение осуществляется через открытую сеть, находящуюся за пределами контроля управления безопасностью организации.

Аутентификация узлов сети может также служить в качестве альтернативного средства аутентификации групп удаленных пользователей в случае, когда они подключены к защищенному, совместно используемому компьютерному средству (9.4.3).

9.4.5 Защита удаленного диагностического порта

Доступ к диагностическим портам необходимо контролировать. Многие компьютеры и компьютерные системы, используемые специалистами по техническому обслуживанию, оснащены портами для диагностики удаленного коммутируемого подключения. Если такие диагностические порты не защищены, то их можно использовать для несанкционированного доступа.

Поэтому диагностические порты следует защитить с помощью надлежащих механизмов безопасности, например посредством блокировки с ключом и процедуры, которая гарантирует, что эти порты становятся доступными только после получения санкции от администратора компьютерной системы на доступ специалистов по техническому обслуживанию программно-аппаратного обеспечения.

**9.4.6** Сегментация сетей

По мере формирования деловых партнерских отношений, которые могут потребовать объединения и коллективного использования компьютеров и сетевых сервисов, вычислительные сети все больше и больше выходят за пределы традиционных границ организации. Такое расширение границ может увеличить риск несанкционированного доступа к уже функционирующим информационным системам, подключенным к сети, некоторые из которых могут потребовать защиты от других пользователей сети вследствие их уязвимости или важности для организации.

В таких случаях необходимо рассмотреть возможность привлечения средств управления для разделения групп информационных сервисов, пользователей и информационных систем.

Один из методов управления безопасностью крупных сетей состоит в их разбиении на несколько логических сегментов, например внутренние сетевые сегменты организации и внешние сетевые сегменты, каждый из которых защищен заданным периметром безопасности. Такой периметр может быть определен при инсталляции шлюзов безопасности между двумя связанными сетями для управления доступом и информационными потоками между этими двумя доменами. Шлюз безопасности должен быть сконфигурирован для фильтрации передаваемых по сети данных между этими сегментами (9.4.7 и 9.4.8) и для блокировки несанкционированного доступа в соответствии с политикой управления доступом, принятой в организации (9.1). Примером такого типа шлюза является, как правило, межсетевой экран.

В основе критериев разбиения сетей на сегменты должна лежать политика управления доступом, принятая в организации, и соответствующие требования (9.1), а также должны быть учтены относительная стоимость и последствия внедрения подходящей сетевой маршрутизации или технологии межсетевого перехода (9.4.7 и 9.4.8).

**9.4.7** Контроль сетевых подключений

Требования политики управления доступом для коллективно используемых сетей, особенно тех, которые выходят за пределы границ организации, могут включать требования реализации средств контроля для ограничения возможности подключения пользователей. Такой контроль может быть осуществлен посредством межсетевых шлюзов, которые фильтруют передаваемые по сети данные с помощью предопределенных таблиц и правил. В основе ограничений на подключение пользователей должна лежать политика управления доступом и требования к производственным приложениям (9.1), которые должны быть осуществлены и соответствующим образом модернизированы.

Примерами приложений, к которым должны применяться такие ограничения, являются:

а) электронная почта;

Ь) односторонняя передача файлов;

с) двухсторонняя передача файлов;

д) интерактивный доступ;

е) доступ к сети только в определенное время суток или в определенную дату.

**9.4.8** Управление сетевой маршрутизацией

Совместно используемые сети и особенно те из них, которые выходят за пределы границ организации, могут потребовать привлечения средств контроля маршрутизации для гарантии того, что подключения компьютера и информационных потоков не нарушают политику управления доступом к производственным приложениям (9.1). Это средство контроля зачастую необходимо для сетей, доступ к которым имеют сторонние (не принадлежащие организации) пользователи.

Средства управления маршрутизацией должны быть основаны на механизмах проверки адреса источника данных и адреса назначения.

Очень полезным механизмом обособления сетей и предотвращения маршрутов распространения от сети одной организации в сеть другой организации является также трансляция сетевого адреса. Такие средства можно реализовать на программном или аппаратном уровне. Те, кто реализует средства контроля должны хорошо знать сильные стороны используемых механизмов.

**9.4.9** Защита сетевых сервисов

Существует целый ряд общедоступных и коммерческих сетевых сервисов, некоторые из которых предлагают дополнительные услуги. Сетевые сервисы могут иметь уникальные защитные характеристики или комплекс защитных характеристик. Организации, пользующиеся сетевыми сервисами, должны потребовать от своих поставщиков сетевых услуг четкого описания атрибутов безопасности всех используемых сервисов.

**9.5 Управление доступом к операционной системе**

Задача: предотвратить несанкционированный доступ к компьютерам.

Средства безопасности на уровне операционных систем должны использоваться для ограничения доступа к компьютерным ресурсам. Эти средства должны быть способны делать следующее:

а) идентифицировать и проверять подлинность пользователей, а также, по необходимости, идентифицировать терминал или местонахождение каждого зарегистрированного пользователя;

Ь) фиксировать случаи успешного и безуспешного доступа к системе;

с) предоставлять подходящие средства для аутентификации; если используется система управления паролями, то должен обеспечиваться выбор надежных паролей (9.3.1 а1);

с1) ограничивать, где это необходимо, время подключения пользователей.

Существуют другие методы управления доступом, такие как "запрос-ответ", использование которых обосновано производственным риском.

**9.5.1** Автоматическая идентификация терминала

Для аутентификации подключений к конкретным узлам сети и к переносному оборудованию следует рассмотреть возможность автоматической идентификации терминалов. Автоматическая идентификация терминалов - это средство, которое можно использовать для тех приложений, в которых важно, чтобы сеанс связи можно было инициировать только с конкретного терминала. Идентификатор, присвоенный терминалу, можно использовать для указания того, разрешено ли конкретному терминалу инициировать сеанс связи или производить определенные действия. Для обеспечения безопасности терминального идентификатора, возможно, потребуется физическая защита терминала. Существует также ряд других методов аутентификации пользователей (9.4.3).

**9.5.2** Процедуры начала сеанса работы с терминалом

Доступ к информационным сервисам следует осуществлять с помощью надежной процедуры начала сеанса работы.

Процедура входа в компьютерную систему должна сводить к минимуму риск несанкционированного доступа. Поэтому она должна давать минимум информации о системе, чтобы избежать оказания излишней помощи неавторизованному пользователю. Процедура входа в систему должна выполнять следующие функции:

а) не выводить на экран идентификаторы системы или приложения до тех пор, пока успешно не завершится процесс входа в систему;

Ь) выводить на экран общее предупреждение о том, что только авторизованные пользователи имеют право доступа к компьютеру;

с) не предоставлять справочную информацию во время выполнения процедуры входа в систему, которая могла бы оказать помощь неавторизованному пользователю;

а1) проверять достоверность регистрационной информации только по завершении ввода всех данных. При возникновении сбойной ситуации система не должна указывать, какая часть введенных данных правильная или неправильная;

е) ограничить разрешаемое количество неудачных попыток входа в систему (рекомендуется три попытки) и принять меры:

1. по регистрации неудавшейся попытки;
2. по принудительному введению временной задержки между дальнейшими попытками входа в систему или ограничение любых дальнейших попыток без специального санкционирования;
3. по разрыву канала связи;

т) задать максимальную и минимальную продолжительность процедуры входа в систему. При ее превышении система должна прервать сеанс работы с терминалом;

д) по завершении успешного входа в систему выводить на экран следующую информацию:

1. дату и время предшествующей успешной попытки входа в систему;
2. подробности о неудавшихся попытках входа в систему, предпринятых с момента последнего успешного входа в нее.

**9.5.3** Идентификация и аутентификация пользователей

Все пользователи (включая обслуживающий персонал, такой как операторы, системные администраторы, системные программисты и администраторы баз данных) должны иметь уникальные персональные идентификаторы, используемые в последствии для прослеживания действий пользователей ответственными лицами. Пользовательские идентификаторы не должны указывать на уровень привилегий пользователя (9.2.2), например администратор, диспетчер и т. п.

В исключительных ситуациях при явных преимуществах для организации можно использовать общий пользовательский идентификатор для группы пользователей или конкретного задания. Такие случаи должны быть утверждены руководством и документально оформлены. Для обеспечения подотчетности могут потребоваться дополнительные средства контроля.

Существуют различные процедуры аутентификации, которые используются для подтверждения подлинности пользователя. Пароли (9.3.1 и ниже) - наиболее общий способ обеспечения идентификации и аутентификации, основанный на секрете, известном только пользователю. Также могут использоваться криптографические средства и опознавательные протоколы.

Жетоны с памятью или интеллектуальные карточки, которыми обладают пользователи, также могут использоваться для идентификации и аутентификации. Биометрические технологии аутентификации, использующие уникальные индивидуальные характеристики или атрибуты, могут также использоваться для подтверждения подлинности пользователя. Совокупность технологий и механизмов подтверждения подлинности приведет к более строгой аутентификации.

9.5.4 Система управления паролями

Пароли являются основным средством подтверждения полномочий доступа пользователя к компьютерной системе. Системы управления паролями должны предоставлять эффективное интерактивное средство обеспечения надежных паролей (руководство по использованию паролей приведено в 9.3.1).

Некоторые приложения требуют назначения пользовательских паролей независимым лицом, наделенным соответствующими полномочиями. В большинстве случаев пароли выбираются и поддерживаются самими пользователями.

Хорошая система управления паролями должна:

а) обязывать пользователей применять индивидуальные пароли для обеспечения подотчетности; Ь) по необходимости позволять пользователям выбирать и изменять свои собственные пароли и

включать процедуру их подтверждения, чтобы избежать ошибок при их наборе; с) обязать пользователей выбирать надежные пароли, как описано в 9.3.1;

*б)* в тех случаях, когда пользователи поддерживают свои собственные пароли, обязывать их изме нять пароли, как описано в 9.3.1;

е) в тех случаях, когда пользователи сами выбирают свои пароли, обязывать их изменять временные пароли при первом входе в систему (9.2.3);

т) вести учет предыдущих пользовательских паролей, например, за последние 12 мес и не допускать их повторное использование пользователями;

д) не выводить пароли на экран при их наборе на клавиатуре;

п) хранить файлы паролей отдельно от основных данных приложений; I) хранить пароли в зашифрованном виде, используя односторонний алгоритм шифрования; ]) изменять пароли, заданные по умолчанию поставщиком программного обеспечения после его инсталляции.

9.5.5 Использование системных сервисных программ

Большинство компьютерных систем поддерживают одну или несколько системных сервисных программ - утилит, которые могли бы обойти системные и прикладные средства контроля. Необходимо ограничить и тщательно контролировать использование таких системных сервисных программ. Предлагается использовать следующие меры управления:

а) использование процедур аутентификации для системных сервисных программ;

Ь) изоляция системных сервисных программ от прикладного программного обеспечения;

с) предоставление доступа к системным сервисным программам минимальному числу надежных авторизованных пользователей;

с)) санкционирование специального использования системных сервисных программ;

е) ограничение доступности системных сервисных программ, например продолжительность внесения санкционированного изменения;

т) регистрация всех случаев использования системных сервисных программ; д) определение и документирование уровней полномочий доступа к системным сервисным программам;

й) удаление всех ненужных служебных и системных программ.

9.5.6 Сигнал тревоги, предупреждающий пользователей о принуждении

Для пользователей, которые могли бы стать целью насилия, должно быть предусмотрено сигнальное устройство.

Решение о том, снабжать ли таким сигнальным устройством, следует принимать, исходя из оценки рисков. Для реагирования на сигнал тревоги необходимо определить обязанности и процедуры.

9.5.7 Время простоя терминалов

Неактивные терминалы в зонах повышенного риска, например в общедоступных местах или местах, находящихся вне пределов досягаемости администраторов безопасности организации, или обслуживающие системы повышенного риска необходимо отключить через определенный промежуток времени для предотвращения доступа незарегистрированных пользователей. Средство установления времени простоя должно очищать экран терминала и завершать сеансы связи с приложениями и сетевыми сервисами после заданного периода бездействия. Время простоя должно задаваться исходя из риска нарушения режима безопасности пользовательского терминала.

Некоторые компьютеры можно обеспечить средством установления времени простоя терминала, которое позволяет очистить экран и предотвратить несанкционированный доступ, однако оно не позволяет завершить сеанс связи с приложениями и сетевыми сервисами.

9.5.8 Ограничение времени подключения

Дополнительную защиту приложений повышенного риска можно обеспечить посредством ограничения времени подключения. Ограничение разрешаемого периода подключения терминала к компьютерным системам позволяет уменьшить вероятность несанкционированного доступа. Применение такого средства контроля следует рассмотреть для компьютерных систем, поддерживающих конфиденциальные приложения, особенно для систем с терминалами, установленными в зонах повышенного риска, например в общедоступных местах или местах, находящихся вне пределов досягаемости администраторов безопасности организации. Примерами таких ограничений являются:

а) использование предопределенных интервалов времени разрешенного доступа, например для пакетной передачи файлов или регулярных интерактивных сеансов связи небольшой продолжительности;

Ь) ограничение времени подключения обычными часами работы организации, если не требуется работа в сверхурочное время.

**9.6 Управление доступом к приложениям**

Задача: предотвратить несанкционированный доступ к информации, хранимой в компьютерных системах.

Для ограничения доступа к системным приложениям должны использоваться средства безопасности.

Логический доступ к программному обеспечению и данным следует предоставлять только авторизованным пользователям. Прикладные системы должны:

а) контролировать доступ пользователей к данным и прикладным системам в соответствии с политикой управления доступом, принятой в организации;

Ь) обеспечивать защиту любой служебной программе и программному обеспечению операционной системы от несанкционированного доступа средствами системного и прикладного контроля;

с) не компрометировать безопасность других систем, с которыми они имеют общие информационные ресурсы;

а1) быть способными обеспечить доступ к информации только ее владельцу, другим уполномо- ченным пользователям или определенным группам пользователей.

**9.6.1** Ограничение доступа к информации

Пользователям прикладных систем, в том числе обслуживающему персоналу, следует предоставлять доступ к данным и функциям прикладных систем в соответствии с политикой управления доступом, основанной на требованиях, характерных и используемых на производстве, и совместимой с принятой в организации политикой доступа к информации (9.1). Для удовлетворения требований ограничения доступа необходимо рассмотреть следующие меры по управлению:

а) предоставление меню для контроля доступа к функциям прикладных систем;

Ь) ограничение знаний пользователей о данных и функциях приложений, доступ к которым им не разрешен, посредством соответствующего редактирования пользовательской документации;

с) контроль полномочий доступа пользователей, например прав на чтение, запись, удаление, выполнение;

с!) гарантирование того, что результаты манипулирования конфиденциальной информацией прикладными системами содержат только данные, предназначенные для вывода и передачи только на терминалы и в помещения, доступ к которым разрешен, включая периодический анализ результатов для обеспечения удаления избыточной информации.

9.6.2 Изоляция уязвимых систем

Для уязвимых систем требуется специально предназначенная (изолированная) вычислительная среда. Некоторые прикладные системы настолько уязвимы по отношению к возможной потере, что требуют специального обращения. Наличие уязвимых мест может указывать на необходимость запуска прикладной системы на специально выделенном компьютере, на необходимость разделения ресурсов только с надежными приложениями или на то, что на работу системы не должны накладываться никакие ограничения. Предлагаются следующие рекомендации:

а) уязвимость прикладной системы должна быть явно определена и документально оформлена ее владельцем (4.1.3);

Ь) в случае, когда уязвимая прикладная система запускается в коллективно используемой среде, необходимо идентифицировать приложения, с которыми она будет разделять ресурсы, и согласовать их использование с владельцем уязвимой прикладной системы.

**9.7 Текущий контроль доступа к системе и его использование**

Задача: выявить несанкционированные действия.

Системам необходим текущий контроль для обнаружения отступления от политики управления доступом и для учета всех событий в системе в случае нарушения безопасности.

Системный мониторинг позволяет определить эффективность средств управления, выбранных для испытания, и сверить на соответствие модели политики управления доступом.

**9.7.1** Регистрация событий

Все чрезвычайные ситуации и события, связанные с нарушением режима безопасности, необходимо регистрировать в контрольном журнале. Записи в таком журнале следует хранить в течение заданного промежутка времени для оказания помощи в будущих расследованиях и осуществлении контроля доступа. Контрольный журнал должен включать следующие данные:

а) идентификаторы пользователей;

Ь) дату и время начала и конца сеанса работы с терминалом;

с) идентификатор терминала или местонахождение, если возможно;

с1) запись успешных и безуспешных попыток доступа к системе;

е) запись успешных и безуспешных попыток доступа к данным и другим ресурсам.

Как часть политики сохранения записей или в силу требований сбора доказательств могут потребоваться определенные протоколы аудита (глава 12).

**9.7.2** Использование текущего контроля 9.*7.2.1 Процедуры и области риска*

Необходимо установить процедуры текущего контроля использования средств обработки информации. Такие процедуры требуются для обеспечения выполнения пользователями только явно разрешенных действий. Уровень контроля, требуемый для отдельных действий, следует определить с помощью оценки риска. Необходимо рассмотреть следующие области риска:

а) санкционированный доступ, включая такие детали, как:

1. идентификатор пользователя;
2. дату и время ключевых событий;
3. типы событий;
4. файлы, доступ к которым осуществлен;
5. используемые программы/сервисные программы; Ь) все привилегированные операции, такие как:
6. использование учетных записей супервизора;
7. запуск и остановка системы;
8. подключение/отключение устройства ввода/вывода; с) попытки несанкционированного доступа, такие как:
9. неудачные попытки доступа;
10. нарушения политики доступа и уведомления для сетевых шлюзов и межсетевых экранов;
11. предупреждения от собственных систем обнаружения вторжения;

с!) системы тревоги или сбоя, такие как:

1. пульт для сигналов тревоги или сообщений;
2. система регистрации исключительных ситуаций;
3. сетевое управление сигнальными устройствами.

9.*7.2.2 Факторы риска*

Результат текущего контроля действий системы рекомендуется регулярно анализировать. Частота процедуры анализа должна зависеть от последствий рисков. Рассматриваемые факторы риска включают: а) критичность прикладных процессов;

Ь) значение, чувствительность или критичность, содержащиеся в информации; с) прошлый опыт проникновения в систему или неправильное использование; с1) степень сетевых соединений системы (особенно сети общего пользования).

*9.7.2.3 Регистрация и анализ событий*

Процесс регистрации и анализа событий включает понимание осуществленных угроз системе и условия, при которых они возникли. Примеры событий, которые могут потребовать дальнейшего расследования в случае инцидентов безопасности, приводятся в 9.7.1.

Системный журнал регистрации часто содержит большой объем информации, причем многое является лишним для контроля безопасности. Для идентификации существенных для контроля безопасности событий нужно выполнить автоматическое копирование соответствующих типов сообщений в другой журнал регистрации и/или использовать подходящие системные сервисные программы или средства аудита для выполнения опроса файла.

При распределении ответственности за журнал регистрации разделение ролей должно рассматриваться между человеком, выполняющим просмотр журнала, и теми, чьи действия контролируются.

Особое внимание следует уделить безопасности средств регистрации, потому что неправильное их использование может исказить смысл безопасности. Средства управления должны стремиться защитить от несанкционированных изменений и при эксплуатации, включая:

а) наличие отключаемого средства регистрации;

Ь) регистрацию преобразований типов сообщений;

с) отредактированные или удаленные записи журнала регистрации;

а1) носители данных журнала регистрации исчерпали свой ресурс, чтобы делать запись или перезапись событий.

**9.7.3** Синхронизация системных часов

Для обеспечения точности контрольных журналов, которые могут потребоваться для расследований или в качестве свидетельства во время судебных разбирательств и при наложении дисциплинарных взысканий, важно правильно установить системные часы компьютеров. Неточные контрольные журналы могут помешать таким расследованиям и подорвать доверие к такому свидетельству.

В тех случаях, когда компьютер или коммуникационное устройство поддерживает часы реального времени, необходимо их установить в соответствии с принятым стандартом, например на универсальное координированное время (1ЮТ) или местное декретное время. Поскольку некоторые часы со временем, как известно, теряют точность, необходимо иметь процедуру их проверки и коррекции в случае значительного отклонения.

**9.8 Мобильное вычисление и телеобработка**

Задача: гарантировать информационную безопасность при использовании средств мобильного вычисления и средств телеобработки.

Требуемая защита должна быть соразмерна с риском этих специальных путей работы. При исполь зовании мобильного вычисления должен рассматриваться риск работы в незащищенной среде и соответ ствующая применяемая защита. В случае телеобработки организация должна защищать сайт телеоб- работки и гарантировать, что соответствующее устройство подходит для этого пути работы.

**9.8.1** Мобильное вычисление

При использовании мобильных вычислительных средств, например ноутбуков, карманных и портативных компьютеров, портативных телефонов, следует соблюдать осторожность, чтобы гарантировать, что производственная информация не скомпрометирована. Необходимо принять формальную политику, которая учитывает риск работы с мобильными вычислительными средствами, особенно в незащищенных средах. Например, такая политика должна включать требования для физической защиты управления доступом, методов криптографии, дублирования информации и вирусной защиты.

Эта политика должна также включить правила и рекомендации по подключению мобильных средств к сетям и руководство по использованию этих средств в общественных местах.

Необходимо соблюдать осторожность при использовании мобильных вычислительных средств в общественных местах, включая и другие незащищенные области вне помещений организации. Защита необходима, чтобы избежать несанкционированного доступа к информации или раскрытия информации, сохраненной и обработанной этими средствами, например, используя криптографические методы (10.3).

Важно с осторожностью использовать эти средства в общественных местах, чтобы избежать риска просматривания, прослушивания посторонними людьми. Всегда нужно иметь антивирусные программы, которые должны своевременно обновляться. Оборудование должно быть доступно, чтобы иметь возможность быстрого и легкого дублирования информации. Это дублирование должно дать адекватную защиту, например от воровства или потери информации.

Подходящую защиту нужно обеспечить при использовании мобильных средств, подключенных к сетям. Удаленный доступ к производственной информации через общедоступные сети с использованием мобильных вычислительных средств должен осуществляться только после успешной идентификации и аутентификации и с подходящими механизмами управления доступом на месте (9.4).

Мобильные вычислительные средства также должны быть физически защищены от воровства, особенно когда они оставлены, например в автомобиле или другом транспорте, в гостинице, конференц-зале и других местах. Оборудование, несущее важную, конфиденциальную и/или критическую производственную информацию, не должно быть оставлено без присмотра, и если возможно, должно быть физически заблокировано при отсутствии собственника или должна использоваться специальная блокировка для защиты оборудования. Более подробную информацию о физической защите мобильных средств можно найти в 7.2.5.

Персоналу, использующему мобильные средства вычислений, рекомендуется пройти специальное обучение, чтобы повысить понимание ими дополнительного риска при использовании мобильных средств и средств управления, которые должны быть реализованы.

9.8.2 Телеобработка

Телеобработка использует такую технологию связи, которая дает возможность персоналу работать дистанционно от установленной станции вне их организации. Необходима соответствующая защита сайта телеобработки, чтобы избежать воровства оборудования и информации, неполномочного раскрытия информации, несанкционированного удаленного доступа к внутренним системам организации или неправильного использования ее средств. Важно, что процесс телеобработки поддается регистрации и контролю со стороны средств управления и что для выполнения этого вида работы имеются соответствующие средства безопасности.

В организациях должны быть разработаны политика, процедуры и стандарты управления процессом телеобработки. Деятельность по телеобработке допустима только в случае, когда организация уверена в наличии соответствующих средств защиты и управления, согласующихся с ее политикой безопасности. Необходимо рассмотреть следующее:

а) существование физической безопасности сайта телеобработки, принимая во внимание физическую безопасность формирования и локализации среды;

Ь) предложенную среду телеобработки;

с) требования безопасности связи, принимая во внимание потребность в удаленном доступе к внутренним системам организации, чувствительность информации, к которой будут обращаться, прогон подключения и чувствительность внутренней системы;

а1) угрозы несанкционированного доступа к информации или ресурсам других людей, например членов семьи, друзей.

Нужно рассмотреть следующие меры по управлению безопасностью:

а) предоставление соответствующего оборудования и сохранение имеющегося для действий телеобработки;

Ь) Определение разрешенной работы, времени работы, классификации информации, которая может быть проведена, внутренние системы и сервисы, к которым оператор телеобработки имеет доступ;

с) предоставление соответствующего оборудования для связи, включая методы для обеспечения удаленного доступа;

с1) физическую безопасность;

е) правила и рекомендации относительно доступа к оборудованию и информации членов семьи и посетителей;

г) предоставление аппаратных и программных средств поддержки и сопровождения;

д) процедуры для дублирования информации и непрерывности производственного процесса; п) аудит и контроль безопасности;

|) аннулирование полномочий, прав доступа и возвращение оборудования после прекращения действий телеобработки.

**10 Разработка и сопровождение систем**

**10.1 Требования безопасности для систем**

Задача: обеспечить встроенность средств защиты в информационные системы.

Рассматриваются вопросы защиты инфраструктуры производственных прикладных программ и прикладных программ, разработанных пользователем. Процесс разработки и применения производственных прикладных программ или услуг может быть критичным с точки зрения безопасности. Требования безопасности должны быть идентифицированы и согласованы до разработки информационных систем.

Все требования безопасности, включая требование возврата системы в безопасное исходное состояние после аварийного режима, рекомендуется идентифицировать на стадии разработки проекта, обосновать, согласовать и документально оформить в рамках общего плана работ по созданию информационной системы.

**10.1.1** Анализ и задание требований безопасности

При формулировании производственных требований к новым системам или модернизации существующих систем, необходимо задать требования к средствам управления безопасностью. Они должны включать требования к автоматизированным средствам управления, встроенным в систему, а также поддерживать возможность ручного управления. Аналогичные соображения следует также принимать во внимание при оценке пакетов программ для производственных приложений. По возможности следует использовать независимо оцененные и сертифицированные продукты.

Требования к безопасности системы и средствам управления ею должны отражать ценность используемых информационных активов, а также возможные последствия нарушения режима безопасности или отсутствия средств защиты производственных процессов. Анализ требований безопасности и идентификация необходимого управления основываются на оценке риска и управлении риском.

Реализация и сопровождение средств управления, вводимых на этапе проектирования, требуют значительно меньших стоимостных затрат, чем реализация и сопровождение средств управления, вводимых в ходе разработки или после завершения этого этапа.

**10.2 Безопасность в прикладных системах**

Задача: предотвратить потерю, изменение или неправильное применение данных пользователя в прикладных системах.

В прикладные системы, включая написанные пользователем прикладные программы, должны быть включены соответствующие средства управления, средства проведения аудита и регистрации входов в систему. Они должны включать функции проверки правильности входных данных, промежуточных данных и выходных данных.

Дополнительные средства управления могут потребоваться для систем, которые обрабатывают ценные или критические для организации активы. Такие функции управления должны быть определены на основе оценки риска и требований безопасности.

**10.2.1** Валидация входных данных

Данные, вводимые в прикладные программы, должны подвергаться проверке с целью обеспечения их корректности и адекватности. Проверке должны подвергаться данные производственных транзакций, постоянные данные (имена и адреса, размеры кредитов, идентификаторы клиентов) и другие параметры (коммерческие цены, расценки, курсы валют, налоговые нормы).

Рекомендуется предусмотреть следующие средства контроля:

а) двойной ввод или другие входные проверки с целью обнаружения следующих ошибок:

1. выход величины из допустимого диапазона;
2. неправильные символы в полях данных;
3. пропуск или неполноту данных;
4. превышение верхних и нижних пределов, налагаемых на объем вводимых данных;
5. несанкционированные или противоречивые управляющие данные;

Ь) периодический просмотр содержания ключевых полей или файлов данных для подтверждения их достоверности и целостности;

с) просмотр печатной входной документации на предмет обнаружения несанкционированных изменений входных данных (на внесение любого изменения во входные документы необходимо получить разрешение);

о!) процедуры реагирования на ошибки, связанные с валидацией входных данных;

е) процедуры тестирования входных данных на наличие ошибок;

т) определение ответственности всех сотрудников, участвующих в процессе ввода данных.

**10.2.2** Управление внутренней обработкой данных

*10.2.2.1 Зоны риска*

Данные, которые были правильно введены в прикладную программу, могут быть повреждены в результате ошибок обработки или преднамеренных действий. Чтобы выявить подобные повреждения данных, в систему необходимо встроить соответствующие средства проверки. При проектировании прикладных программных средств необходимо реализовать ограничения, минимизирующие риск сбоя, возникающего при обработке данных и ведущего к потере целостности. Примерами средств проверки, которые можно встроить в системы, являются:

а) встраивание в приложения функций добавления и удаления информации для осуществления изменения данных;

Ь) процедуры, предотвращающие неправильный запуск или работу приложения после сбоя, предшествующего обработке данных (8.1.1);

с) использование корректирующих программ для восстановления после отказов с целью обеспечения правильной обработки данных.

*10.2.2.2 Средства проверки и управления*

Необходимые средства контроля определяются характером прикладной системы и возможными последствиями от повреждения данных для организации. Примерами средств проверки, которые можно встроить в системы, являются:

а) контроль сеанса связи и пакетной обработкой с целью согласования файлов данных с платежными балансами после проведения операций с ними;

Ь) контроль платежного баланса для сверки начального сальдо с предыдущим конечным сальдо:

1. контроль выполнения операций;
2. подведение итогов по обновлению файлов;
3. контроль выполнения программ;

с) валидация данных, сгенерированных системой (10.2.1);

а1) проверка целостности загружаемых данных или программного обеспечения или пересылаемых данных между центральным и удаленными компьютерами (10.3.3);

е) подведение итогов по обновлению файлов;

т) проверка того, что прикладные программы выполняются за приемлемое время;

д) проверка с целью обеспечения выполнения прикладных программ в правильном порядке и их приостановки в случае отказа, а также приостановки обработки данных до момента разрешения проблемы.

**10.2.3** Аутентификация сообщений

Аутентификация сообщений - это метод, используемый для выявления несанкционированных изменений или повреждений содержания передаваемых электронных сообщений. Аутентификацию можно реализовать на аппаратном или программном уровне с помощью физического устройства аутентификации сообщений или программного алгоритма.

Вопрос аутентификации сообщений возникает в том случае, когда жизненно важным является обеспечение целостности сообщений, например электронные передачи информации о денежных средствах или другие электронные обмены данными. Для определения необходимости проведения аутентификации сообщений и выбора наиболее подходящего метода ее реализации необходимо провести оценку риска нарушения режима безопасности.

Аутентификация сообщений не предназначена для защиты содержания сообщений от перехвата. Для этих целей могут использоваться методы шифрования данных (10.3.2 и 10.3.3), как подходящее средство реализации аутентификации сообщений.

**10.2.4** Валидация выходных данных

Выходные данные прикладных программ должны подвергаться проверке с целью обеспечения корректной и адекватной обработки хранимой информации. Как правило, системы создаются в предположении корректности предпринимаемых проверок и тестирования выходных данных. Однако это не всегда имеет место. Проверка правильности выходных данных может включать:

а) проверку данных на наличие ошибок для того, чтобы протестировать их приемлемость;

Ь) подсчеты, связанные с контролем согласованности данных для того, чтобы гарантировать обработку всех данных;

с) предоставление пользователю или последующей системе обработки данных информации, достаточной для того, чтобы они могли оценить правильность, полноту, точность и категорию этой информации;

с!) процедуры реагирования на тесты, осуществляющие валидацию выходных данных;

е) определение обязанностей персонала, вовлеченного в процесс получения выходных данных.

**10.3 Криптографические средства контроля**

Задача: обеспечение конфиденциальности, подлинности и целостности информации. Криптогра фические системы и методы должны использоваться для защиты информации в условиях, когда другие средства контроля не обеспечивают адекватную защиту.

**10.3.1** Политика использования криптографических средств контроля

Принятие решения о приемлемости криптографического решения должно рассматриваться как часть общего процесса оценки рисков и выбора средств управления. Для того чтобы определить требуемый уровень защиты информации, должна быть произведена оценка риска. Эта оценка может использоваться для определения степени соответствия применяемых криптографических средств поставленным целям и рассматриваемым производственным процессам.

Для защиты своей информации организация должна разработать политику по использованию криптографических средств. Такая политика необходима, чтобы максимизировать преимущества и минимизировать риски использования криптографических методов, а также избежать неправильного их использования. При разработке политики необходимо рассматривать:

а) принятый в организации подход к управлению процессом использования криптографических средств, включая общие принципы защиты производственной информации;

Ь) подход к управлению ключами, включая методы восстановления зашифрованной информации в случае потери, компрометации или повреждения ключей;

с) распределение ролей и обязанностей, например определение лиц, ответственных за:

1. реализацию политики;
2. управление ключами;
3. определение соответствующего уровня криптографической защиты;
4. стандарты, которые нужно принять для эффективной реализации криптографической защиты (с указанием того, какое решение используется для тех или иных производственных процессов).

**10.3.2** Шифрование

Шифрование - это криптографический метод, который может использоваться для обеспечения конфиденциальности чувствительной или критической информации.

Требуемый уровень защиты определяется на основе оценки риска и с учетом специфики используемого алгоритма шифрования и длины криптографических ключей.

При реализации криптографической политики организации должны быть учтены инструкции и национальные особенности передачи потоков шифрованной информации и применения криптографических методов. Кроме того, необходимо учесть средства, используемые для управления экспортом и импортом криптографической технологии (12.1.6).

Специалисты должны определить приемлемый уровень защиты, выбрать программные продукты, которые смогут обеспечить требуемую защиту и безопасное управление ключами (10.3.5). Кроме того, организация должна юридически обосновать необходимость использования шифрования.

**10.3.3** Цифровая подпись

Цифровые подписи обеспечивают способ защиты подлинности и целостности электронных документов. Например, они могут использоваться в электронной торговле, где имеется потребность в проверке того, кто подписал электронную версию документа и было ли содержимое подписанного документа изменено.

Цифровые подписи могут применяться к любому, представленному в электронном виде документу, например они могут использоваться для подписи электронных платежей, передачи денежных средств, контрактов и соглашений. Цифровые подписи осуществляются с помощью криптографических методов, основанных на использовании однозначно связанной пары ключей, где один ключ применяется для создания сигнатуры (секретного ключа), а другой для проверки сигнатуры (открытого ключа).

Необходимо следить за сохранностью конфиденциальности секретного ключа. Этот ключ должен сохраняться в секрете, так как любой имеющий доступ к этому ключу может подписывать документы от лица владельца ключа. Кроме того, важно обеспечить целостность открытого ключа. Эта защита обеспечивается с помощью использования сертификата открытого ключа (10.3.5).

Необходимо рассмотреть тип и качество используемого алгоритма формирования электронной подписи и длины используемых ключей. Криптографические ключи, используемые для цифровой подписи, должны отличаться от ключей, используемых для шифрования (10.3.2).

При использовании цифровых подписей необходимо учитывать законодательство, определяющее юридическую основу формирования цифровых подписей. Например, в случае электронной торговли важно знать законное месторасположение цифровой подписи. Для использования цифровой подписи в условиях отклонения от законной схемы могут потребоваться контракты или другие соглашения. Необходимо указать законы и инструкции, которые могут применяться в организации при использовании цифровых подписей.

**10.3.4** Услуги защиты от отказов передачи/приема

В случае, когда необходимо разрешить споры относительно использования цифровой подписи на электронном документе, должны использоваться услуги защиты от отказов приема/передачи, например спор в связи с использованием цифровой подписи в контракте или платежном документе, представленных в электронном виде. Эти услуги помогают доказать факт совершения конкретного события или действия, например отказ от посылки по электронной почте инструкции с цифровой подписью. Эти услуги основаны на использовании методов шифрования и цифровой подписи (10.3.2 и 10.3.3).

**10.3.5** Управление ключами

*10.3.5.1 Защита криптографических ключей*

Управление криптографическими ключами существенно влияет на эффективность использования криптографических методов. Компрометация или потеря криптографических ключей могут привести к потере конфиденциальности, подлинности и/или целостности информации. Система управления должна поддержать два типа криптографических методов:

а) методы секретных ключей, когда две или большее количество сторон совместно используют один и тот же ключ, который используется как для шифрования, так и для расшифровки информации. Этот ключ должен держаться в секрете, так как любое лицо, имеющее к нему доступ, может расшифровать всю зашифрованную с помощью этого ключа информацию или ввести несанкционированную информацию;

Ь) методы открытых ключей, когда каждый пользователь имеет пару ключей: открытый ключ (который доступен всем) и секретный ключ (который должен держаться в секрете). Методы открытого ключа могут использоваться для шифрования (10.3.2) и генерирования цифровой подписи (10.3.3).

Все ключи должны быть защищены от изменения и разрушения, а секретные и частные ключи -от неполномочного раскрытия. Для этой цели могут также использоваться криптографические методы. Чтобы предохранить оборудование, применяемое для генерации, сохранения и архивации ключей, должна использоваться физическая защита.

*10.3.5.2 Правила, процедуры и методы*

Система управления ключами должна основываться на согласованном наборе правил, процедур и надежных методов для:

а) генерации ключей для различных криптографических систем и различных приложений;

Ь) генерации и получения сертификатов открытых ключей;

с) распределения ключей между пользователями, включая способ активизации ключей при получении;

д) хранения ключей, включая способ получения доступа к ключам полномочными пользователями;

е) замены и обновления ключей, включая правила, определяющие, когда и каким образом долж на производиться замена ключей;

{) работы со скомпрометированными ключами;

д) отмены ключей, включая процедуры изымания и отмены, например, когда ключи скомпрометированы или пользователь покинул организацию (в случае чего ключи должны также архивироваться);

п) восстановления ключей, которые были потеряны или разрушены, как составляющей процесса обеспечения непрерывности производства, например для восстановления зашифрованной информации;

*\)* архивирования ключей, например для заархивированной или скопированной информации;

]) разрушения ключей;

к) регистрации и аудита действий, связанных с управлением ключами.

Для того чтобы уменьшить вероятность раскрытия ключей надо определить даты их активизации и отмены для того, чтобы ключи могли использоваться только в течение ограниченного периода времени. Этот период времени должен зависеть от условий, в которых осуществляется криптографическое управление, и от предполагаемого риска.

Процедуры должны предусматривать возможность предоставления юридически обоснованного доступа к криптографическим ключам, например для расшифровки информации, выступающей в качестве доказательства в суде.

Помимо проблемы надежного управления секретными и закрытыми ключами следует рассмотреть также проблему защиты открытых ключей. Существует угроза подделки злоумышленником цифровой подписи путем замены открытого ключа пользователя своим собственным. Эта проблема решается посредством использования сертификата открытых ключей. Эти сертификаты должны производиться таким образом, чтобы информация о владельце пары отрытого/закрытого ключей однозначно связывается с открытым ключом. Поэтому важно, чтобы процесс создания этих сертификатов был надежным. Обычно он осуществляется органом по сертификации, представляющим официальную организацию, в которой реализованы соответствующий контроль и процедуры, обеспечивающие требуемую степень надежности.

Содержание соглашений или контрактов с поставщиками криптографических услуг должно охватывать проблемы генерации, надежности услуг и времени действия услуг (4.2.2).

**10.4 Безопасность системных файлов**

Задача: обеспечить безопасное проектирование и сопровождение информационной технологии. Доступ к системным файлам должен контролироваться.

Поддержку целостности системы рекомендуется ввести в круг обязанностей пользователя или группы поддержки, которой прикладная система или программное обеспечение принадлежит.

**10.4.1** Управление эксплуатационным программным обеспечением

В эксплуатируемых системах рекомендуется предусмотреть управление используемым программным обеспечением. Для минимизации риска искажения эксплуатационных систем должны быть рассмотрены следующие средства управления:

а) изменение эксплуатационных библиотечных программ должно осуществляться только назначенным библиотекарем, наделенным соответствующими полномочиями на управление (10.4.3);

Ь) по возможности эксплуатационные системы должны содержать только выполнимые коды;

с) выполнимый код не должен использоваться в эксплуатационной системе до тех пор, пока не будет получено доказательство его успешного тестирования и приема пользователем и не будет произведено обновление соответствующих библиотек программ;

а1) для всех обновлений эксплуатационных библиотек программ должен поддерживаться контрольный файл регистрации;

е) на случай непредвиденных обстоятельств должны быть сохранены предыдущие версии программного обеспечения.

Поставщик должен обеспечить продавца программного обеспечения всеми необходимыми доказательствами безопасности. Любое решение об обновлении должно учитывать вопросы безопасности версии, т. е. введения новых функциональных возможностей безопасности или оценки количества и серьезности проблем защиты, связанных с этой версией. Когда это способствует удалению или понижению уязвимости системы, следует использовать программные заплаты.

Физический или логический доступ предоставляется поставщику только в случае необходимости и с одобрения руководства. За действиями поставщика необходимо установить мониторинг.

**10.4.2** Защита системных тестовых данных

Тестовые данные рекомендуется защищать и контролировать. Тестирование системы и испытания при приемке обычно требуют использования существенных объемов тестовых данных, которые должны быть максимально приближены к эксплутационным данным. Нужно избегать использования эксплутационных баз данных, содержащих личную информацию. Если такая информация используется,то она не должна быть связана с пользователем. Для защиты информации операционной системы при тестировании рекомендуются следующие процедуры контроля:

а) процедуры управления доступом, которые относятся к эксплуатационным прикладным системам, рекомендуется применять также при тестировании прикладным системам;

Ь) необходимо получить отдельное разрешение каждый раз, когда рабочие данные копируются в тестируемую прикладную систему;

с) рабочую информацию рекомендуется удалять из тестируемой прикладной системы немедленно после завершения испытания;

с1) копирование и использование рабочей информации должно быть зарегистрировано в журнале аудита.

**10.4.3** Управление доступом к библиотеке исходных модулей

Чтобы уменьшить возможность повреждения компьютерных программ необходимо осуществлять следующий строгий контроль доступа к библиотекам исходных программных модулей (8.3):

а) по возможности библиотеки программ не должны храниться в эксплуатационных системах;

Ь) для каждого приложения должен назначаться библиотекарь программ;

с) персонал поддержки информационной технологии не должен иметь неограниченный доступ к библиотекам программ;

с1) программы, находящиеся на стадии разработки или технического обслуживания, не должны содержаться в эксплуатационных библиотеках программ;

е) внесение изменений в библиотеки исходных программных модулей и предоставление программных модулей программистам может осуществляться только назначенным библиотекарем при санкционировании его администратором по поддержке информационной технологии для приложения;

т) распечатки программ должны проводиться в безопасной среде (8.6.4);

д) каждый факт доступа к исходным библиотекам должен регистрироваться;

п) старые версии исходных программ должны быть заархивированы с указанием точных даты и времени, когда они находились в эксплуатации, а также вместе со всем сопровождающим программным обеспечением, рабочим контролем, определением данных и процедурами;

I) сопровождение и копирование библиотек исходных модулей должны осуществляться в соответствии со строгими процедурами управления изменениями (10.4.1).

**10.5 Безопасность процессов разработки и поддержки**

Задача: поддерживать безопасность программного обеспечения и информации в прикладных системах.

Среды проектирования и сопровождения должны строго контролироваться. Администраторы, ответственные за прикладные системы, должны также нести ответственность за безопасность среды проектирования и сопровождения. Они должны обеспечить рассмотрение всех предложенных изме-нений системы и гарантировать, что изменения не компрометируют безопасность системы или среды.

**10.5.1** Процедуры управления изменениями

Для минимизации искажения информационных систем надо организовать строгий контроль над выполнением изменений. Должны быть определены формальные процедуры управления изменениями. Они должны гарантировать, что безопасность и процедуры управления не скомпрометированы, что программисты имеют доступ только к тем частям системы, которые необходимы для их работы, и что на каждое изменение получено формальное соглашение и одобрение. Изменение прикладного программного обеспечения может приводить к конфликтам с эксплуатационной средой. Везде, где это возможно, прикладные процедуры и процедуры управления эксплуатационными изменениями должны быть интегрированы (8.1.2). Этот процесс должен включать:

а) поддержку записи согласованных уровней предоставления полномочий;

Ь) обеспечение того, что изменения проведены полномочными пользователями;

с) анализ контроля и процедур обеспечения целостности, для того чтобы гарантировать, что они не скомпрометированы этими изменениями;

с!) идентификацию всего программного обеспечения, информации, объектов, баз данных и аппаратных средств, которые требуют исправлений;

е) получение формального одобрения сделанных детальных предложений до начала работы по модернизации;

т) обеспечение того, чтобы полномочный пользователь получил информацию об изменениях до выполнения каких-либо работ;

д) обеспечение выполнения работы по минимизации производственных сбоев;

п) обеспечение того, что все изменения полностью внесены в системную документацию, а старая документация заархивирована или ликвидирована;

|) поддержку контроля в текущей версии всех изменений программного обеспечения;

.1) поддержание журнала аудита всех запросов на изменения;

к) обеспечение соответствия необходимых изменений эксплуатационной документации (8.1.1) и пользовательских процедур;

I) обеспечение проведения изменений в надлежащее время и без нарушения затрагиваемых ими производственных процессов.

Многие организации поддерживают среду, в которой пользователи проводят тестирование нового программного обеспечения и которая отделена от среды разработки и промышленной среды. Это обеспечивает средства контроля над новым программным обеспечением и позволяет ввести дополнительную защиту эксплуатационной информации, используемой для тестирования.

10.5.2 Технический обзор изменений операционной системы

Необходимо осуществлять периодическое обновление операционной системы, например устанавливать новую версию программного обеспечения или новые программные заплаты. После внесения изменений в операционную систему необходимо осуществить анализ и тестирование прикладных систем, для того чтобы исключить неблагоприятное воздействие изменений на их работу и безопасность. Этот процесс должен охватывать:

а) анализ процедур прикладного управления и процедур обеспечения целостности с целью проверки того, что они не были скомпрометированы изменениями в операционной системе;

Ь) обеспечение того, что годовой план поддержки и бюджет включают анализ и тестирование системы в случае внесения изменений в операционную систему;

с) обеспечение того, что уведомление об изменениях в операционной системе появляется вовремя, что позволяет произвести соответствующий анализ до начала работы;

с!) обеспечение внесения соответствующих изменений в планы бесперебойной работы организации (раздел 11).

10.5.3 Ограничения на внесение изменений в пакеты программ

Внесение изменений в пакеты программ должно проводиться в исключительных случаях. По возможности пакеты программ должны использоваться без изменения. В случае, когда внесение изменений представляется необходимым, следует рассмотреть следующие пункты:

а) риск нарушения правильного функционирования встроенных средств управления и средств обеспечения целостности;

Ь) необходимость получения согласия поставщика;

с) возможность получения необходимых изменений от поставщика в рамках стандартного обновления программ;

с1) возможность взятия организацией ответственности за дальнейшее сопровождение программного обеспечения в результате внесенных изменений.

Если изменения представляются существенными, первоначальное программное обеспечение должно быть сохранено, а изменения должны быть применены к четко идентифицированной его копии. Все изменения должны быть полностью протестированы и документально оформлены, для того чтобы в случае необходимости они могли быть повторно применены при будущем обновлении программного обеспечения.

10.5.4 Скрытые каналы и "троянский" код

Скрытый канал может способствовать раскрытию информации с помощью некоторых неявных и скрытых средств. Он может быть активизирован с помощью изменения параметра, доступного с помощью надежных и ненадежных элементов вычислительной системы или с помощью внедрения информации в поток данных.

"Троянский" код разработан для воздействия на систему несанкционированным, незаметным путем, без запроса получателя или пользователя программы. Скрытые каналы и "троянский" код редко возникают случайно. В качестве мер, направленных на предупреждение внедрения скрытых каналов и "троянского" кода, выступают:

а) закупка программ только из доверенного источника;

Ь) закупка программ с возможностью проверки исходных текстов программ;

с) использование оцененных программных продуктов;

с)) инспекция всех исходных текстов программ перед эксплуатационным использованием; е) управление доступом и внесением изменений в уже инсталлированный код; () использование для работы на ключевых системах проверенного персонала.

**10.5.5** Разработка программного обеспечения внешними организациями

При разработке программного обеспечения внешними организациями необходимо рассмотреть:

а) лицензирование соглашений, кода владельца и прав интеллектуальной собственности (12.1.2);

Ь) сертификат качества выполненной работы;

с) трехсторонние соглашения на случай несостоятельности третьей стороны;

с!) права доступа для контроля качества и точности выполненной работы;

е) договорные требования к качеству кода;

*Т)* тестирование перед инсталляцией с целью обнаружения "троянского" кода.

**11 Управление бесперебойной работой организации**

**11.1 Вопросы управления бесперебойной работой организации**

Задача: предотвращать перебои в производственной деятельности и защищать критические производственные процессы от воздействия основных видов сбоев или аварийных состояний.

Процесс управления бесперебойной работой осуществляется с целью уменьшения повреждений, вызванных бедствиями и сбоями в системе защиты (которые могут быть результатом, например, природных бедствий, несчастных случаев, отказов оборудования или умышленных действий) и сведения их к приемлемому уровню за счет сочетания профилактических мер и мер управления восстановлением.

Последствия аварий, сбоев в системе защиты и отказов в обслуживании должны быть проанализированы.

Должны быть разработаны и реализованы планы обеспечения бесперебойной работы, обеспечивающие восстановление производственных процессов в течение требуемых временных интервалов. Такие планы должны внедряться и поддерживаться, для того чтобы стать неотъемлемой частью всех других процессов управления.

Правила управления бесперебойной работой должны включать контроль с целью идентификации и снижения рисков, ограничения последствий инцидентов, причиняющих ущерб, и обеспечение свое- временного возобновления основных операций.

**11.1.1** Процессы управления бесперебойной работой

Для управления и поддержки бесперебойной работы должен быть реализован управляемый процесс, охватывающий все сферы деятельности организации. Он должен объединить следующие ключевые элементы управления бесперебойностью в работе:

а) определение рисков и вероятности их возникновения, а также идентификацию критически важных производственных процессов и их ранжирование по приоритетам;

Ь) определение возможного воздействия аварий различных типов на производственную деятельность (важно найти решения, которые могут использоваться в случае небольших инцидентов, а также в случае серьезных инцидентов, угрожающих жизнеспособности организации) и установление производственного назначения средств обработки информации;

с) приобретение соответствующей страховки как составляющей процесса бесперебойной работы;

с1) формулировка и документирование стратегии бесперебойной работы, согласованной с задачами и приоритетами производственной деятельности;

е) формулировка и документирование планов бесперебойной работы в соответствии с согласованной стратегией;

() регулярное тестирование и обновление используемых планов и процессов;

д) внедрение управления бесперебойной работой в структуру и производственные процессы организации.

Ответственность за координирование процессов управления бесперебойной работой в организации должна быть распределена на соответствующем уровне, например на собрании по информационной безопасности (4.1.1).

11.1.2 Анализ планирования бесперебойной работы

Анализ планирования бесперебойности работы должен начинаться с идентификации событий, которые могут вызывать перебои в производственной деятельности, например отказ оборудования, наводнение или пожар. Он должен сопровождаться оценкой риска, для того чтобы определить последствия перебоев (в терминах масштаба повреждения и периода восстановления). В данную деятельность должны быть вовлечены владельцы производственных ресурсов и процессов. Оценка риска охватывает все производственные процессы, а не ограничивается средствами обработки информации.

В зависимости от результатов оценки риска должна быть разработана стратегия, определяющая общий подход к обеспечению бесперебойной работы. План утверждается руководством.

11.1.3 Разработка и реализация планов обеспечения бесперебойной работы организации Планы разрабатываются для сопровождения или восстановления производственной деятель ности в течение заданного периода времени после прерывания или сбоев критических производст венных процессов. Процесс планирования непрерывной работы должен включать:

а) идентификацию и согласование всех обязанностей и чрезвычайных мер;

Ь) выполнение чрезвычайных мер для восстановления в течение заданного интервала времени. Особое внимание должно быть уделено оценке зависимостей от внешних факторов и контрактов;

с) документирование согласованных процедур и процессов;

а1) обучение персонала в соответствии с согласованными процедурами и процессами восстановления, включая управление в кризисных ситуациях;

е) тестирование и обновление планов.

Процесс планирования должен концентрироваться на возникающих производственных задачах, например восстановление отдельных предоставляемых клиентам услуг за приемлемое время. Следует рассмотреть привлекаемые для этого услуги и ресурсы, включая укомплектование персоналом, не связанные с обработкой информации ресурсы, а также соглашения по переходу на аварийный режим работы для средств обработки информации.

11.1.4 Схема планирования бесперебойной работы организации

Чтобы обеспечить согласованность всех уровней планирования и определить приоритеты при проведении тестирования и эксплуатации, необходимо иметь единую схему планирования бесперебойной работы организации. В каждом плане обеспечения бесперебойной работы организации следует четко задать условия его активации, а также указать сотрудников, отвечающих за реалии-зацию каждого пункта плана. При идентификации новых требований устанавливаемые процедуры реагирования на чрезвычайные ситуации, например планы эвакуации или известные схемы перехода на аварийный режим, должны соответствующим образом редактироваться.

Схема планирования бесперебойной работы должна включать:

а) условия активизации планов, описывающие процессы, которые предшествуют приведению плана в действие (как оценить ситуацию, кто должен быть вовлечен в работу и т. д.);

Ь) процедуры работы в аварийном режиме, описывающие действия, которые должны быть приняты в случае инцидентов, подвергающих опасности производственную деятельность и/или человеческую жизнь. Они должны включать меры общественного оповещения и эффективной связи с соответствующими органами государственной власти, например полицией, пожарной службой и местными властями;

с) процедуры восстановления, описывающие действия, которые нужно предпринять для возобновления нормальной производственной деятельности или временного перевода сервиса в другие места с последующим возобновлением производственной деятельности в течение заданного периода времени;

а1) процедуры возобновления, описывающие действия, которые нужно предпринять для возврата к нормальной производственной деятельности;

е) график сопровождения, в котором определяется, где и когда должно производиться тестирование плана, а также описывается процесс сопровождения плана;

() деятельность по обучению и уведомлению, которая осуществляется с целью формирования понимания и обеспечения эффективности процессов поддержки бесперебойной работы организации;

д) документ с описанием обязанностей персонала, в котором по каждому пункту плана указываются ответственные за него лица. В случае необходимости должны быть указаны альтернативные кандидатуры.

Каждый план должен иметь определенного владельца. Процедуры работы в аварийном режиме и планы восстановления производственной деятельности должны находиться в компетенции владельцев соответствующих производственных ресурсов или рассматриваемых процессов. Вопросы восстановления альтернативных технических услуг, таких как обработка информации и средства связи, находятся обычно в зоне ответственности поставщиков услуг.

11.1.5 Тестирование, сопровождение и повторная оценка планов обеспечения бесперебойной работы организации

*11.1.5.1 Тестирование планов*

Многие планы обеспечения бесперебойной работы организации терпят неудачу при их тестировании вследствие неправильных исходных допущений, просчетов или изменений, внесенных в оборудование, и просчетов персонала. Поэтому для обеспечения своевременности и эффективности эти планы должны регулярно тестироваться. Такое тестирование должно также гарантировать, что все члены группы по восстановлению систем после аварий и другие сотрудники, имеющие к этому отношение, будут постоянно осведомлены о плане.

График тестирования планов обеспечения бесперебойной работы организации должен указывать, как и когда будет тестироваться каждый элемент плана. Рекомендуется проводить многократное тестирование отдельных компонентов плана. Для обеспечения действенности и эффективности плана в реальных условиях необходимо использовать ряд разнообразных методов тестирования. Тестирование должно включать:

а) настольное тестирование различных сценариев (обсуждение мер восстановления производственной деятельности с использованием примеров прерываний);

Ь) моделирование ситуаций (особенно для обучения персонала ролям, связанным с управлением в кризисных ситуациях и после возникновения инцидента);

с) тестирование технического восстановления (обеспечивающее возможность эффективного восстановления информационных систем);

а1) тестирование возможности восстановления в альтернативном месторасположении (выполнение производственных процессов вне основного месторасположения параллельно с выполнением действий по восстановлению);

е) тестирование средств поставщика и услуг (обеспечение того, что поставляемые извне услуги и программные продукты соответствуют предусмотренным в контракте обязательствам);

т) генеральные проверки (проверки схемы организации, персонала, оборудования, средств и процессов на их способность ликвидировать перебои в работе).

Данные методы могут использоваться в любой организации и должны учитывать особенности конкретного плана восстановления.

*11.1.5.2 Сопровождения и повторная оценка планов*

Для поддержки постоянной эффективности планов обеспечения бесперебойной работы организации эти планы должны сопровождаться с помощью проведения регулярного пересмотра и обновления (11.1.5.1 - 11.1.5.3). В программу управления производимыми в организации изменениями должны быть включены процедуры, обеспечивающие надлежащее рассмотрение вопросов обеспечения бесперебойной работы организации.

Для осуществления регулярного пересмотра плана обеспечения бесперебойной работы организации рекомендуется назначить ответственного, идентифицировать изменения в производственных схемах, еще не отраженных в планах обеспечения бесперебойной работы, внести соответствующие изменения в план. Этот формальный процесс контроля за изменениями должен способствовать распространению и усовершенствованию обновленных планов на основе регулярного пересмотра всего плана.

Примерами ситуаций, в которых может потребоваться усовершенствование планов, являются приобретение нового оборудования, усовершенствование операционных систем и изменения:

а) персонала;

Ь) адресов или номеров телефонов;

с) производственной стратегии;

а1) месторасположения аппаратуры и ресурсов;

е)законодательства;

т) подрядчика, поставщика и основных клиентов;

д) риска (эксплуатационного и финансового);

п) процессов (а также введение новых или устранение прежних процессов).

**12 Соответствие законодательству и нормам безопасности**

**12.1 Соответствие правовым требованиям**

Задача: избежать нарушения уголовного и гражданского права, предусмотренного законом, регулирующих или договорных обязательств и требований информационной безопасности.

Проектирование, функционирование, использование и управление информационными системами должно подчиняться законодательным, регулирующим и договорным требованиям безопасности.

Рекомендации по специфическим правовым требованиям должны давать юридические консуль танты организации или юристы-практики, обладающие соответствующей квалификацией. Законода тельные требования разных стран существенно различаются, что необходимо учитывать при органи- зации международных информационных потоков.

**12.1.1** Идентификация соответствующего законодательства

Для каждой информационной системы рекомендуется четко определить и документально оформить все подходящие законодательные, регулирующие и договорные требования безопасности. Соответствующим образом должны быть определены и документально оформлены специальные средства контроля и персональные обязанности, направленные на обеспечение этих юридических норм.

**12.1.2** Права интеллектуальной собственности

*12.1.2.1 Авторское право*

Для обеспечения соответствующих юридических ограничений на использование материала, относительно которого могут иметься права интеллектуальной собственности, типа авторского права и торговых марок, рекомендуется реализовать соответствующие процедуры. Нарушение авторского права может вести к судебному иску.

Законодательные, правовые или договорные требования могут содержать ограничения на копирование материала, составляющего собственность. В частности, они могут требовать, чтобы использовался только разработанный организацией материал либо материал, который лицензирован или предоставлен организации разработчиком.

*12.1.2.2 Авторское право на программное обеспечение*

Программное обеспечение обычно снабжается лицензионным соглашением, которое ограничивает использование программного продукта только кругом определенных ПЭВМ, и может ограничивать копирование только созданием резервных копий. Следует предусмотреть следующие средства контроля:

а) опубликование политики соблюдения авторских прав в области программного обеспечения, определяющей правовые нормы использования программных и информационных продуктов;

Ь) издание стандартов по процедурам приобретения программных продуктов;

с) пропаганда авторского права на программное обеспечение, а также поддержка понимания правил его приобретения и дисциплинарных мер, которые должны предприниматься к персоналу, нарушающему их;

а1) поддержка соответствующих регистров активов;

е) поддержка доказательства права собственности на лицензии, эталонные диски, справочники и т. д.;

т) контроль за тем, что максимально допустимое количество пользователей не превышено;

д) контроль за тем, что устанавливается только лицензионное или санкционированное программное, обеспечение;

п) проведение политики по выполнению соответствующих лицензированных условий;

|) проведение политики по размещению и передаче программного обеспечения другим сторонам;

*\)* использование соответствующих средств аудита;

к) исполнение сроков и условий использования программного обеспечения и информации, полученных по сетям общего пользования (8.7.6).

**12.1.3** Защита документации организации

Важную для организации документацию рекомендуется защищать от потери, уничтожения и фальсификации. Для реализации правовых требований, а также для выполнения основной производственной деятельности может возникнуть необходимость в хранении некоторых документов в защищенном месте. В качестве таких документов могут выступать, например, документы, свидетельствующие о том, что организация работает в соответствии с правовыми нормами, или документы, используемые для обеспечения надлежащей защиты от возможных гражданских или уголовных исков, для подтверждения финансового состояния организации перед держателями акций, партнерами и аудиторами. Срок хранения и информационное содержание данных документов устанавливаются в соответствии с государственными законами или правилами.

Документы рекомендуется разделить на категории, например отчетные документы, базы данных, журналы транзакций, журналы аудита и эксплуатационные процедуры. Для каждого документа нужно подробно указать срок хранения и тип носителей информации, например статья, микрофиша, магнитное запоминающее устройство, оптическое запоминающее устройство. Криптографические ключи, связанные с зашифрованными архивами или цифровыми подписями (10.3.2 и 10.3.3), должны надежно храниться и быть доступными только для санкционированных лиц.

Необходимо учитывать возможность старения носителей, использованных для хранения данных. Хранение и обработка данных должны осуществляться в соответствии с рекомендациями изготовителя.

При использовании электронных носителей необходимо обеспечить возможность доступа к данным (в смысле доступности носителя и удобочитаемости формата) в течение оговоренного срока хранения с использованием защиты от возможной потери информации вследствие будущих технологических изменений.

Система хранения данных должна выбираться таким образом, чтобы обеспечить восстановление данных за приемлемый период времени и в нужном формате.

Система хранения и обработки должна обеспечивать четкую идентификацию данных и установленного либо автоматически регулируемого периода хранения. Система должна допускать уничтожение данных после окончания срока их хранения при условии, что данные становятся ненужными.

Для выполнения указанных требований в организации следует разработать:

а) рекомендации по определению сроков хранения, хранению, обработке и уничтожению данных и информации;

Ь) список типов данных и время их хранения;

с) опись источников основной информации;

о!) порядок контроля для защиты важных данных и информации от потери, уничтожения и фальсификации.

12.1.4 Защита данных и персональной информации

В ряде стран введено законодательство, устанавливающее контроль за обработкой и передачей персональных данных (обычно это информация о существующих лицах, по которой их можно идентифицировать). Такой контроль налагает обязательства на сбор, обработку и распространение персональной информации и может ограничивать возможность ее передачи в другие страны.

В соответствии с законодательством по защите данных это требует использования соответствующей управляющей структуры и средств управления. Для этого обычно лучше всего привлечь специалиста по защите данных, который предоставит администратору, пользователю и поставщику услуг руководства с указанием их личных обязанностей и предлагаемых для них специальных рекомендаций. В обязанности владельца данных входит информирование специалиста по защите данных о любом предложении хранения персональной информации в структурированном файле и обеспечение понимания принципов защиты данных, определяемых соответствующим законодательством.

12.1.5 Предотвращение неправильного использования средств обработки информации Средства обработки информации организации предназначены для производственных целей. Их

использование должно быть санкционировано руководством. Неуправляемое использование этих средств для непроизводственных или несанкционированных целей должно запрещаться. В случае обнаружения такой деятельности с помощью мониторинга или других средств о ней должно быть сообщено руководителю, отвечающему за соответствующее дисциплинарное действие.

Правила контроля за использованием средств обработки информации зависят от страны, и в соответствии с этим может потребоваться уведомление служащих о таком контроле или получение их согласия на осуществление подобного контроля. Правовое согласие рекомендуется получить до начала осуществления контроля.

Многие страны имеют или находятся на этапе введения законодательства по защите от компьютерных злоупотреблений. Использование компьютера в несанкционированных целях может преследоваться по закону. Поэтому важно, чтобы все пользователи четко понимали границы разрешенного им доступа. Этого можно достигнуть, например, путем предоставления пользователям письменных полномочий, копии которых должны быть подписаны пользователями и храниться в организации. Служащие организации и сторонние пользователя должны осознавать недопустимость несанкционированного доступа.

При входе в систему на экран компьютера должно выдаваться сообщение, предупреждающее о том, что загружаемая система является частной и что несанкционированный доступ к ней не разрешен. Чтобы продолжить процесс входа в систему, пользователь должен подтвердить свои полномочия и адекватно отреагировать на сообщение.

**12.1.6** Регулирование криптографического управления

Некоторые страны приняли соглашения, законы, правила или другие нормы для управления доступом к криптографическим средствам управления или их использования. Это управление может включать:

а) импорт и/или экспорт аппаратных средств и программного обеспечения для реализации криптографических функций;

Ь) импорт и/или экспорт аппаратных средств и программного обеспечения, предназначенного для присоединения криптографических средств;

с) обязательные или произвольные для страны методы доступа к информации, зашифрованной с помощью аппаратных средств или программного обеспечения с целью обеспечения конфиденциальности содержания информации.

Для обеспечения согласованности с национальным законодательством необходимо обратиться за юридической консультацией. Юридическую консультацию рекомендуется провести также в случае передачи зашифрованной информации или криптографического средства управления в другую страну.

**12.1.7** Сбор доказательства соответствия законодательству и нормам безопасности

*12.1.7.1 Правила доказательства соответствия законодательству и нормам безопасности* Для подтверждения действий, направленных против личности или организации, необходимо

представлять адекватное доказательство. Всякий раз, когда подобное действие является внутренним дисциплинарным делом, доказательство должно описываться с помощью внутренних процедур.

Когда предпринимаемые действия затрагивают гражданское или уголовное право, представляемое доказательство должно соответствовать действующему законодательству или правилам специального судопроизводства. В общем случае эти правила охватывают:

а) допустимость доказательства: действительно ли доказательство может использоваться в суде;

Ь) значимость доказательства: качество и полнота доказательства;

с) адекватное обоснование того, что в течение времени, когда доказательство хранилось и обрабатывалось системой, средства контроля работали корректно и последовательно.

*12.1.7.2 Приемлемость доказательства*

Для достижения приемлемости доказательства организация должна подтвердить, что ее информационные системы соответствуют действующему стандарту или кодексу установившейся практики при получении должного доказательства.

*12.1.7.3 Качество и законченность доказательства*

Для достижения качества и полноты доказательства необходимо осуществлять четкое ведение журнала, в котором излагаются факты, способные выступать в качестве доказательства. В общем случае такой журнал может быть установлен при следующих условиях:

а) для бумажных документов: оригинал надежно хранится, а лица, получившие к нему доступ, регистрируются с указанием даты и обстоятельств, при которых это произошло, а также лица, осуществившего регистрацию. При проведении любого исследования должны быть предоставлены гарантии того, что не будут использоваться оригиналы;

Ь) для информации на компьютерных носителях: для того чтобы гарантировать доступность информации, должны быть сделаны копии каждого съемного носителя, а также информации, находящейся на жестких дисках или в памяти. Должен храниться файл регистрации всех действий, осуществляемых в ходе копирования, а сам процесс копирования должен регистрироваться. Копия носителя и файл регистрации должны надежно храниться.

Если инцидент случился впервые, то может быть неочевидным, что это приведет к возможному судебному разбирательству. Поэтому до осознания серьезности инцидента существует опасность случайного разрушения необходимого доказательства. В любое ожидаемое судебное разбирательство желательно подключить адвоката или полицию и получить от них консультацию относительно требуемого доказательства.

**12.2 Анализ политики безопасности и технической согласованности**

Задача: гарантировать соответствие информационных систем организационной политике безопасности и существующим стандартам.

Необходимо проводить регулярный анализ безопасности информационных систем.

Такой анализ рекомендуется проводить относительно соответствующей политики безопасности и технических платформ, а также проводить регулярный аудит информационных систем относительно выполнения стандартов безопасности.

**12.2.1** Согласованность с политикой безопасности

Администраторы должны гарантировать, что все процедуры безопасности в пределах их области ответственности выполняются правильно. Кроме того, все области в пределах организации должны подвергаться регулярному анализу, для того чтобы гарантировать их согласованность с политикой безопасности и существующими стандартами. Такой анализ должен включить:

а) информационные системы;

Ь) поставщиков систем;

с) владельцев информации и информационных активов;

а1) пользователей;

е)управление.

Владельцы информационных систем (5.1) должны поддерживать регулярные анализы согласованности этих систем с соответствующей политикой безопасности, стандартами и любыми другими требованиями безопасности. Вопросы эксплуатационного контроля за использованием систем рассматриваются в 9.7.

**12.2.2** Техническая проверка на соответствие

Информационные системы должны регулярно проверяться на соответствие существующим стандартам реализации безопасности. Техническая проверка на соответствие включает проверку рабочих систем с целью обеспечения корректного контроля за аппаратными и программными средствами. Этот тип проверки на соответствие требует специальных технических средств. Она должна выполняться вручную опытным системным инженером (в случае необходимости с поддержкой соответствующих программных инструментальных средств) или с помощью автоматизированного пакета программ, который составляет технический отчет для последующего толкования его техническим специалистом.

Проверка на соответствие охватывает также, например, тестирование возможности нарушения защиты, которое может выполняться специально нанятыми для этого независимыми экспертами. Такое тестирование может быть полезно для обнаружения уязвимых мест в системе и проверки эффективности контроля с целью предотвращения несанкционированного доступа на основании этих уязвимых мест. Необходимо предпринять соответствующие меры предосторожности на случай, чтобы успешное тестирование возможности нарушения защиты не могло способствовать нарушению безопасности системы и непреднамеренному использованию других уязвимых мест.

Любая техническая проверка на соответствие должна проводиться компетентными полномочными лицами или под их управлением.

**12.3 Положения, касающиеся аудита систем**

Задача: максимизировать эффективность и минимизировать помехи процесса аудита при входе в систему или выходе из системы.

В ходе проведения аудита системы необходимо осуществлять контроль за безопасностью рабочих систем и инструментальных средств.

Необходимо также осуществлять защиту целостности инструментальных средств аудита и предот- вращать их неправильное использование.

**12.3.1** Контроль за проведением аудита системы

Требования аудита и действия, включающие проверку рабочих систем, должны тщательно планироваться и согласовываться, для того чтобы минимизировать риск сбоев производственных процессов. Нужно выполнить следующие условия:

а) требования к аудиту должны быть согласованы с руководством;

Ь) сфера действия проверки должна быть согласована и контролироваться;

с) проверка должна ограничиваться доступом к программному обеспечению и данным только для чтения;

а1) виды доступа, отличные от доступа только для чтения, должны разрешаться только для отдельных копий системных файлов, которые после окончания процесса аудита должны уничтожаться;

е) ресурсы информационной технологии, используемые для выполнения проверки, должны быть четко идентифицированы и доступны;

т) должны быть идентифицированы и согласованы требования к специальной или дополнительной проверке;

д) предоставляемый доступ должен отслеживаться и регистрироваться в журнале обращений;

п) все процедуры, требования и обязанности должны быть документально оформлены.

12.3.2 Защита системных инструментальных средств аудита

Доступ к системным инструментальным средствам аудита, т. е. программному обеспечению или файлам данных, должен защищаться, для того чтобы предотвратить возможное неправильное их использование или компрометацию. Такие инструментальные средства должны быть отделены от систем разработки и рабочих систем и не должны содержаться в библиотеках, на магнитных лентах или областях пользователя без обеспечения соответствующего уровня дополнительной защиты.