

МЕЖДУНАРОДНЫЙ
СТАНДАРТ

ISO/IEC
27002

С учетом Технической поправки 1,
опубликованной 2007-07-01

Информационные технологии. Свод правил по управлению защитой информации

*Information technology — Security techniques —
Code of practice for information security management*

*Technologies de l'information —
Techniques de sécurité —
Code de pratique pour la gestion de sécurité d'information*

Номер для ссылки
ISO/IEC 27002:2005(E)

© ИСО/МЭК 2005
© Компания «Технорматив» Перевод на русский язык 2007

Содержание

ПРЕДИСЛОВИЕ	VII
0 ВВЕДЕНИЕ	VIII
0.1 ЧТО ТАКОЕ ЗАЩИТА ИНФОРМАЦИИ?	VIII
0.2 ЗАЧЕМ НУЖНА ЗАЩИТА ИНФОРМАЦИИ?	VIII
0.3 КАК СОЗДАТЬ ТРЕБОВАНИЯ ЗАЩИТЫ.....	IX
0.4 ОЦЕНКА РИСКОВ, СВЯЗАННЫХ С НАРУШЕНИЕМ ЗАЩИТЫ.....	IX
0.5 ВЫБОР СРЕДСТВ УПРАВЛЕНИЯ.....	X
0.6 Отправная точка защиты информации	X
0.7 КРИТИЧЕСКИЕ ФАКТОРЫ УСПЕХА	XI
0.8 РАЗРАБОТКА ВАШИХ СОБСТВЕННЫХ РУКОВОДЯЩИХ ПРИНЦИПОВ	XII
1 ОБЛАСТЬ ДЕЙСТВИЯ.....	1
2 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	2
3 СТРУКТУРА ЭТОГО СТАНДАРТА	5
3.1 РАЗДЕЛЫ	5
3.2 ОСНОВНЫЕ КАТЕГОРИИ ЗАЩИТЫ	6
4 ОЦЕНКА И ОБРАБОТКА РИСКОВ	7
4.1 ОЦЕНИВАНИЕ РИСКОВ, СВЯЗАННЫХ С НАРУШЕНИЕМ ЗАЩИТЫ	7
4.2 ОбРАБОТКА РИСКОВ, СВЯЗАННЫХ С НАРУШЕНИЕМ ЗАЩИТЫ	7
5 ПОЛИТИКА В ОБЛАСТИ ЗАЩИТЫ	10
5.1 Политика в области защиты информации.....	10
5.1.1 Программный документ в области защиты информации	10
5.1.2 Анализ политики в области защиты информации	11
6 ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ.....	13
6.1 ВНУТРЕННЯЯ ОРГАНИЗАЦИЯ.....	13
6.1.1 Обязательства руководства по защите информации.....	13
6.1.2 Координация защиты информации	14
6.1.3 Распределение обязанностей по защите информации.....	15
6.1.4 Процесс получения разрешения для средств обработки информации.....	16
6.1.5 Соглашения о конфиденциальности.....	16
6.1.6 Контакты с органами	18
6.1.7 Контакты со специальными группами	18
6.1.8 Независимый анализ защиты информации	19
6.2 ВНЕШНИЕ СТОРОНЫ	20
6.2.1 Выявление рисков, связанных с внешними сторонами	20
6.2.2 Рассмотрение защиты при работе с потребителями	23
6.2.3 Учет защиты в соглашениях с третьими сторонами.....	24

7 МЕНЕДЖМЕНТ АКТИВОВ	29
7.1 ОТВЕТСТВЕННОСТЬ ЗА АКТИВЫ.....	29
7.1.1 Опись активов.....	29
7.1.2 Собственность на активы	30
7.1.3 Приемлемое использование активов	31
7.2 КЛАССИФИКАЦИЯ ИНФОРМАЦИИ.....	32
7.2.1 Руководящие указания по классификации.....	32
7.2.2 Маркировка информации и обращение с информацией.....	33
8 ЗАЩИТА ЧЕЛОВЕЧЕСКИХ РЕСУРСОВ.....	35
8.1 ПЕРЕД НАЧАЛОМ РАБОТЫ ПО НАЙМУ	35
8.1.1 Роли и обязанности.....	35
8.1.2 Отбор.....	36
8.1.3 Условия работы по найму.....	37
8.2 ВО ВРЕМЯ РАБОТЫ ПО НАЙМУ	38
8.2.1 Обязанности руководства	38
8.2.2 Осведомленность, образование и подготовка в области защиты информации	39
8.2.3 Дисциплинарный процесс	40
8.3 ПРЕКРАЩЕНИЕ ИЛИ ПЕРЕМЕНА МЕСТА РАБОТЫ ПО НАЙМУ	41
8.3.1 Обязательства, связанные с прекращением работы по найму.....	41
8.3.2 Возврат активов.....	42
8.3.3 Удаление прав доступа.....	42
9 ФИЗИЧЕСКАЯ И ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ	44
9.1 БЕЗОПАСНЫЕ ЗОНЫ.....	44
9.1.1 Физический периметр безопасности	44
9.1.2 Средства управления физическим доступом	45
9.1.3 Защита офисов, комнат и средств.....	46
9.1.4 Защита от внешних и экологических угроз	47
9.1.5 Работа в безопасных зонах.....	47
9.1.6 Зоны открытого доступа, поставки и погрузки	48
9.2 ЗАЩИТА ОБОРУДОВАНИЯ.....	49
9.2.1 Расположение и защита оборудования	49
9.2.2 Вспомогательные коммунальные службы.....	50
9.2.3 Защита кабельных соединений	51
9.2.4 Обслуживание оборудования	52
9.2.5 Защита оборудования, находящегося за пределами рабочего места	53
9.2.6 Безопасная ликвидация или повторное использование оборудования	54
9.2.7 Вынос имущества	54
10 МЕНЕДЖМЕНТ СРЕДСТВ СВЯЗИ И ОПЕРАЦИЙ	56
10.1 ПРОЦЕДУРЫ ЭКСПЛУАТАЦИИ И РАБОЧИЕ ОБЯЗАННОСТИ.....	56
10.1.1 Документированные процедуры эксплуатации.....	56
10.1.2 Менеджмент изменений.....	57
10.1.3 Разделение обязанностей	58
10.1.4 Разделение средств разработки, испытания и эксплуатации	58
10.2 МЕНЕДЖМЕНТ ПРЕДОСТАВЛЕНИЯ УСЛУГ ТРЕТЬЕЙ СТОРОНЫ	60
10.2.1 Предоставление услуг	60
10.2.2 Постоянный контроль и анализ услуг третьей стороны	60
10.2.3 Менеджмент изменений в услугах третьей стороны	62
10.3 ПЛАНИРОВАНИЕ РЕАЛИЗАЦИИ И ПРИЕМКА СИСТЕМЫ	62
10.3.1 Менеджмент производительности	63
10.3.2 Приемка системы	63
10.4 ЗАЩИТА ОТ ЗЛОНАМЕРЕННОГО И МОБИЛЬНОГО КОДА	65
10.4.1 Средства управления против злонамеренного кода	65
10.4.2 Средства управления против мобильного кода	67

10.5	РЕЗЕРВНОЕ КОПИРОВАНИЕ	67
10.5.1	<i>Резервное копирование информации</i>	68
10.6	МЕНЕДЖМЕНТ ЗАЩИТЫ СЕТИ.....	69
10.6.1	<i>Средства управления сетью</i>	69
10.6.2	<i>Защита сетевых услуг</i>	70
10.7	ОБРАЩЕНИЕ С НОСИТЕЛЯМИ ИНФОРМАЦИИ.....	71
10.7.1	<i>Менеджмент сменных носителей информации</i>	71
10.7.2	<i>Ликвидация носителей информации.....</i>	72
10.7.3	<i>Процедуры обращения с информацией.....</i>	73
10.7.4	<i>Защита системной документации.....</i>	74
10.8	ОБМЕН ИНФОРМАЦИЕЙ	74
10.8.1	<i>Политика и процедуры обмена информацией</i>	74
10.8.2	<i>Соглашения об обмене</i>	77
10.8.3	<i>Физические носители при транспортировке</i>	78
10.8.4	<i>Электронный обмен сообщениями</i>	79
10.8.5	<i>Информационные системы для бизнеса</i>	80
10.9	УСЛУГИ ЭЛЕКТРОННОЙ ТОРГОВЛИ	81
10.9.1	<i>Электронная торговля.....</i>	81
10.9.2	<i>Онлайневые сделки</i>	83
10.9.3	<i>Общедоступная информация</i>	84
10.10	ПОСТОЯННЫЙ КОНТРОЛЬ.....	85
10.10.1	<i>Ведение контрольного журнала</i>	85
10.10.2	<i>Постоянный контроль использования систем.....</i>	86
10.10.3	<i>Защита данных журнала.....</i>	88
10.10.4	<i>Журналы оператора и администратора.....</i>	88
10.10.5	<i>Регистрация отказов.....</i>	89
10.10.6	<i>Синхронизации часов.....</i>	90
11	УПРАВЛЕНИЕ ДОСТУПОМ	91
11.1	ДЕЛОВЫЕ ТРЕБОВАНИЯ К УПРАВЛЕНИЮ ДОСТУПОМ	91
11.1.1	<i>Политика управления доступом</i>	91
11.2	МЕНЕДЖМЕНТ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ.....	92
11.2.1	<i>Регистрация пользователя.....</i>	93
11.2.2	<i>Менеджмент привилегий.....</i>	94
11.2.3	<i>Менеджмент паролей пользователя.....</i>	95
11.2.4	<i>Анализ прав доступа пользователя</i>	96
11.3	ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ.....	96
11.3.1	<i>Использование пароля</i>	97
11.3.2	<i>Оборудование пользователя, находящееся без присмотра</i>	98
11.3.3	<i>Политика чистого стола и чистого экрана.....</i>	99
11.4	УПРАВЛЕНИЯ ДОСТУПОМ В СЕТЬ.....	100
11.4.1	<i>Политика в отношении использования сетевых услуг</i>	100
11.4.2	<i>Аутентификация пользователя для внешних соединений.....</i>	101
11.4.3	<i>Идентификация оборудования в сетях</i>	102
11.4.4	<i>Защита удаленных диагностических и конфигурационных портов.....</i>	102
11.4.5	<i>Разделение в сетях</i>	103
11.4.6	<i>Управление сетевыми соединениями</i>	104
11.4.7	<i>Управление сетевой маршрутизацией</i>	105
11.5	УПРАВЛЕНИЕ ДОСТУПОМ К ОПЕРАЦИОННОЙ СИСТЕМЕ	106
11.5.1	<i>Безопасные процедуры входа в систему</i>	106
11.5.2	<i>Идентификация и аутентификация пользователей</i>	107
11.5.3	<i>Система менеджмента паролей</i>	108
11.5.4	<i>Использования системных утилит</i>	109
11.5.5	<i>Блокировка сеанса по превышению лимита времени [тайм-аут]</i>	110
11.5.6	<i>Ограничение времени соединения</i>	111
11.6	УПРАВЛЕНИЕ ДОСТУПОМ К ПРИЛОЖЕНИЯМ И ИНФОРМАЦИИ.....	112
11.6.1	<i>Ограничение доступа к информации</i>	112
11.6.2	<i>Изоляция важных систем.....</i>	113

11.7 МОБИЛЬНАЯ ОБРАБОТКА И ТЕЛЕОБРАБОТКА	114
11.7.1 <i>Мобильная обработка и связь</i>	114
11.7.2 <i>Телеобработка</i>	115
12 ПРИОБРЕТЕНИЕ, РАЗРАБОТКА И ОБСЛУЖИВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ	118
12.1 ТРЕБОВАНИЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ	118
12.1.1 <i>Анализ и спецификация требований защиты</i>	118
12.2 ПРАВИЛЬНАЯ ОБРАБОТКА В ПРИЛОЖЕНИЯХ.....	119
12.2.1 <i>Валидация входных данных</i>	119
12.2.2 <i>Управление внутренней обработкой</i>	120
12.2.3 <i>Целостность сообщений</i>	122
12.2.4 <i>Валидация выходных данных</i>	122
12.3 КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА УПРАВЛЕНИЯ	123
12.3.1 <i>Политика по использованию криптографических средств управления</i>	123
12.3.2 <i>Распределение ключей</i>	125
12.4 Защита системных файлов.....	127
12.4.1 <i>Управление системным программным обеспечением</i>	127
12.4.2 <i>Защита испытательных данных системы</i>	128
12.4.3 <i>Управления доступом к исходному коду программы</i>	129
12.5 Защита в процессах разработки и вспомогательных процессах	130
12.5.1 <i>Процедуры управления изменениями</i>	130
12.5.2 <i>Технический анализ приложений после изменений операционной системы</i>	132
12.5.3 <i>Ограничения на изменения в пакетах программ</i>	132
12.5.4 <i>Утечка информации</i>	133
12.5.5 <i>Аутсорсинговая разработка программного обеспечения</i>	134
12.6 МЕНЕДЖМЕНТ ТЕХНИЧЕСКИХ СЛАБЫХ МЕСТ	135
12.6.1 <i>Управление техническими слабыми местами</i>	135
13 МЕНЕДЖМЕНТ ИНЦИДЕНТОВ В СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ.....	138
13.1 СОСТАВЛЕНИЕ ОТЧЕТОВ О СОБЫТИЯХ И НЕДОСТАТКАХ В СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ	138
13.1.1 <i>Составление отчетов о событиях в системе защиты информации</i>	138
13.1.2 <i>Составление отчетов о недостатках защиты</i>	140
13.2 МЕНЕДЖМЕНТ ИНЦИДЕНТОВ И УЛУЧШЕНИЙ В СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ.....	141
13.2.1 <i>Обязанности и процедуры</i>	141
13.2.2 <i>Извлечение уроков из инцидентов в системе защиты информации</i>	143
13.2.3 <i>Сбор доказательств</i>	143
14 МЕНЕДЖМЕНТ НЕПРЕРЫВНОСТИ БИЗНЕСА	145
14.1 АСПЕКТЫ МЕНЕДЖМЕНТА НЕПРЕРЫВНОСТИ БИЗНЕСА, СВЯЗАННЫЕ С ЗАЩИТОЙ ИНФОРМАЦИИ.....	145
14.1.1 <i>Включение защиты информации в процесс менеджмента непрерывности бизнеса</i>	145
14.1.2 <i>Непрерывность бизнеса и оценка рисков</i>	147
14.1.3 <i>Разработка и реализация планов обеспечения непрерывности, включающих защиту информации</i>	147
14.1.4 <i>Структура планирования непрерывности бизнеса</i>	149
14.1.5 <i>Испытание, обслуживание и повторная оценка планов обеспечения непрерывности бизнеса</i>	150
15 СООТВЕТСТВИЕ	152
15.1 СООТВЕТСТВИЕ ЮРИДИЧЕСКИМ ТРЕБОВАНИЯМ	152
15.1.1 <i>Идентификация применимых законов</i>	152
15.1.2 <i>Права на интеллектуальную собственность (ПИС)</i>	152
15.1.3 <i>Защита организационных записей</i>	154
15.1.4 <i>Защита данных и секретность личной информации</i>	155
15.1.5 <i>Предотвращение неправильного использования средств обработки информации</i>	156
15.1.6 <i>Регулирование криптографических средств управления</i>	157
15.2 СООТВЕТСТВИЕ ПОЛИТИКЕ И СТАНДАРТАМ В ОБЛАСТИ ЗАЩИТЫ И ТЕХНИЧЕСКОЕ СООТВЕТСТВИЕ	158
15.2.1 <i>Соответствие политике и стандартам в области защиты</i>	158

<i>15.2.2</i>	<i>Проверка технического соответствия</i>	159
15.3	<i>Соображения, касающиеся аудита информационных систем</i>	159
<i>15.3.1</i>	<i>Средства управления аудитом информационных систем</i>	160
<i>15.3.2</i>	<i>Защита инструментальных средств аудита информационных систем</i>	161
БИБЛИОГРАФИЯ		162
ИНДЕКС		163

Предисловие

ИСО (Международная организация по стандартизации) и МЭК (Международная электротехническая комиссия) образуют специализированную систему всемирной стандартизации. Национальные организации, являющиеся членами ИСО или МЭК, участвуют в разработке международных стандартов посредством технических комитетов, учрежденных соответствующей организацией для того, чтобы обсуждать определенные области технической деятельности. Технические комитеты ИСО и МЭК сотрудничают в областях взаимного интереса. Другие международные организации, правительственные и неправительственные, контактирующие с ИСО и МЭК, также принимают участие в работе. В области информационных технологий, ИСО и МЭК учредили Совместный технический комитет, ИСО/МЭК СТК 1.

Проекты международных стандартов составляются в соответствии с правилами, определенными в Директивах ИСО/МЭК, часть 2.

Основная задача совместного технического комитета состоит в подготовке международных стандартов. Проекты международных стандартов, принятые объединенным техническим комитетом, рассылаются национальным организациям на голосование. Для опубликования документа в качестве международного стандарта необходимо как минимум 75% голосов членов-организаций, принимающих участие в голосовании.

Обращаем внимание на то, что некоторые элементы этого документа могут быть предметом патентных прав. ИСО и МЭК не несут ответственность за установление какого-либо или всех таких патентных прав.

Документ ISO/IEC 27002 был подготовлен Совместным техническим комитетом ISO/IEC JTC 1, «Информационные технологии», Подкомитет SC 27, «Методики защиты информационных технологий».

Данное второе издание отменяет и заменяет первое издание, которое было технически пересмотрено.

Семейство международных стандартов на Системы Управления Защитой Информации (СУЗИ) разрабатывается в подкомитете ИСО/МЭК СТК 1/ПК 27. В семейство входят международные стандарты по требованиям к системам управления защитой информации, по управлению рисками, по метрикам и измерениям, а также руководящие принципы по реализации. Это семейство примет схему нумерации, использующую серию номеров 27000 и следующие.

0 Введение

0.1 Что такое защита информации?

Информация – это актив, который, подобно другим значимым активам бизнеса, важен для ведения дела организации и, следовательно, необходимо, чтобы он соответствующим образом защищался. Это особенно важно во все больше и больше взаимосвязанной среде бизнеса. В результате этой возрастающей взаимосвязанности, информация в настоящее время подвергается воздействию возрастающего числа и растущего разнообразия угроз и слабых места в системе защиты (см. также Руководящие принципы OECD по Защите информационных систем и сетей).

Информация может существовать во многих формах. Она может быть напечатана или написана на бумаге, храниться в электронном виде, посыпаться по почте или путем использования электронных средств, показана на пленках или высказана в разговоре. Вне зависимости от того, какую форму информация принимает, какими средствами она распространяется или хранится, она всегда должна быть надлежащим образом защищена.

Защита информации – это охрана информации от большого разнообразия угроз, осуществляемая с целью обеспечить непрерывность бизнеса, минимизировать деловые риски и максимизировать возврат по инвестициям и возможности деловой деятельности.

Защита информации достигается реализацией соответствующего набора средств управления, включая политику, процессы, процедуры, организационные структуры и программные и аппаратные функции. Эти элементы управления необходимо создать, внедрить, постоянно контролировать, анализировать и улучшать, по необходимости, с целью обеспечить выполнение конкретных организационных задач защиты и бизнеса. Это следует делать вместе с другими процессами управления бизнесом.

0.2 Зачем нужна защита информации?

Информация и вспомогательные процессы, системы и сети являются важными активами бизнеса. Определение, достижение, поддержание в рабочем состоянии и улучшение защиты информации может быть существенным для поддержания конкурентного преимущества, движения ликвидности, рентабельности, соответствия законам и коммерческого имиджа.

Организации и их информационные системы и сети сталкиваются с угрозами для безопасности, исходящими из весьма разнообразных источников, включая компьютеризированное мошенничество, шпионаж, саботаж, вандализм, пожар или наводнение. Причины ущерба, например, злонамеренный код, компьютерное хакерство и воздействия, вызывающие отказ в обслуживании законных пользователей, становятся все более обыденными, амбициозными и изощренными.

Защита информации важна для предприятий как государственного, так частного сектора, а также для защиты ценных инфраструктур. В обоих секторах, защита информации будет работать как инструмент реализации, например, для ведения электронного управления или электронного бизнеса, и для того, чтобы избежать или снизить соответствующие риски. Взаимосвязь государственных и частных сетей и совместное использование информационных ресурсов увеличивает трудность достижения управления доступом. Курс на распределенную обработку данных также ослабляет результативность центрального, специализированного управления.

Множество информационных систем не было предназначено для того, чтобы быть безопасными. Защита, которая может быть достигнута техническими средствами, ограничена, и ее следует поддерживать соответствующим управлением и процедурами. Определение того, какие средства управления следует принять, требует тщательного планирования и внимания деталям. Управление защитой информации требует, как минимум, участия всех служащих в организации. Она также может потребовать участия акционеров, поставщиков, третьих сторон, потребителей или других внешних сторон. Также может понадобиться консультация специалиста извне организации.

0.3 Как создать требования защиты

Важно, чтобы организация выявила свои требования защиты. Есть три основных источника требований защиты.

1. Один источник получается из оценивания рисков для организации, с учетом общей деловой стратегии и целей организации. Посредством оценки рисков определяются угрозы активам, оценивается уязвимость по отношению к случаю и вероятность его возникновения, а также его возможное негативное влияние.
2. Другим источником являются требования закона, устава, другие обязательные требования и требования договоров, которые организация, ее торговые партнеры, подрядчики и поставщики услуги должны выполнить, а также их социально-культурная среда.
3. Дальнейшим источником является конкретный набор принципов, целей и деловых требований к обработке информации, которые организация разработала для поддержки своих операций.

0.4 Оценка рисков, связанных с нарушением защиты

Требования защиты выявляются методической оценкой исков, связанных с нарушением защиты. Надо, чтобы расходы на средства управления были пропорциональны ущербу деловой деятельности, который, вероятно может иметь место в результате нарушения защиты.

Результаты оценки рисков помогут направить и определить подходящее действие и приоритеты в области управления рисками для защиты информации, а также в области реализации средств управления, выбранных для защиты от этих рисков.

Оценку рисков следует периодически повторять, с целью учесть все изменения, которые могли бы повлиять на результаты оценки рисков.

Больше информации об оценке рисков, связанных с нарушением защиты, можно найти в разделе 4.1, «Оценивание рисков, связанных с нарушением защиты».

0.5 Выбор средств управления

Как только требования защиты и риски были выявлены, а решения по обработке рисков – приняты, следует выбрать и внедрить соответствующие средства управления, с целью обеспечить снижение рисков до приемлемого уровня. Средства управления могут быть выбраны из этого стандарта или из других наборов средств управления, или же могут быть разработаны новые средства управления, с целью удовлетворить конкретные потребности, по обстановке. Выбор средств управления защитой зависит от организационных решений, основанных на критериях приемки рисков, вариантах обработки рисков и на общем подходе к управлению рисками, применяемом в организации; выбор также должен подчиняться всем применимым национальным и международным законам и нормам.

Некоторые средства управления в этом стандарте могут рассматриваться как руководящие принципы для управления защитой информации и как применимые для большинства организаций. Ниже под заголовком «Отправная точка защиты информации» они объясняются более подробно ниже.

Больше информации о выборе средств управления и других вариантах обработки рисков можно найти в разделе 4.2 «Обработка рисков, связанных с нарушением защиты».

0.6 Отправная точка защиты информации

Ряд средств управления может рассматриваться как хорошая отправная точка для реализации защиты информации. Они или основаны на важных требованиях закона, или считаются общей практикой в области защиты информации.

Средства управления, считающиеся важными для любой организации с точки зрения закона, включают, в зависимости от применимого законодательства, следующее:

- a) защита данных и секретность личной информации (см. 15.1.4);
- b) защита организационных записей (см. 15.1.3);
- c) права на интеллектуальную собственность (см. 15.1.2).

Средства управления, считающиеся общей практикой в области защиты информации, включают следующее:

- a) программный документ в области защиты информации (см. 5.1.1);
- b) распределение обязанностей по защите информации (см. 6.1.3);

- c) осведомленность, образование и подготовка по защите информации (см. 8.2.2);
- d) правильная обработка в приложениях (см. 12.2);
- e) управление технической уязвимостью (см. 12.6);
- f) менеджмент непрерывности бизнеса (см. 14);
- g) управление инцидентами и улучшениями в системе защиты информации (см. 13.2).

Эти средства управления подходят большинству организаций и в большинстве сред.

Следует отметить, что хотя все средства управления в этом стандарте являются важными, и их следует рассмотреть, уместность любого средства управления следует определять в свете конкретных рисков, с которыми сталкивается организация. Поэтому, хотя вышеуказанный подход считается хорошей отправной точкой, он не заменяет выбор средств управления, основанных на оценке рисков.

0.7 Критические факторы успеха

Опыт показал, что следующие факторы часто являются критическими для успешной реализации защиты информации в организации:

- a) политика, цели и деятельность в области защиты информации, которые отражают цели бизнеса;
- b) метод и структура для реализации, поддержания в рабочем состоянии, постоянного контроля и улучшения защиты информации, которые соответствуют организационной культуре;
- c) видимая поддержка и обязательства всех уровней руководства;
- d) хорошее понимание требований защиты информации, оценки рисков и управления рисками;
- e) результативный маркетинг защиты информации всем менеджерам, служащим и другим сторонам, с целью достичь осведомленности;
- f) распространение руководящих принципов политики и стандартов в области защиты информации среди всех менеджеров, служащих и других сторон;
- g) резерв для финансирования деятельности по управлению защитой информации;
- h) обеспечение надлежащей осведомленности, подготовки и образования;
- i) создание результативных процессов управления инцидентами в системе защиты информации;
- j) внедрение системы измерения¹, которая используется для того, чтобы оценивать исполнение управления защитой информации и предложения по улучшению, поступающие по цепочке обратной связи.

¹ Отмечаем, что измерения защиты информации находятся за пределами области применения данного стандарта

0.8 Разработка ваших собственных руководящих принципов

Этот свод правил может рассматриваться как отправная точка для разработки руководящих принципов, особых для организации. Не все средства управления и руководящие принципы этого свода правил могут быть применимыми. Кроме того, могут потребоваться дополнительные средства управления и руководящие принципы, не включенные в этот стандарт. Когда разрабатываются документы, содержащие дополнительные руководящие принципы или средства управления, может быть полезным включить перекрестные ссылки на разделы этого стандарта, если это применимо, с целью облегчить проверку соответствия аудиторами и деловыми партнерами.

Информационные технологии. Свод правил по управлению защитой информации

1 Область действия

Этот международный стандарт устанавливает руководящие и общие принципы начинания, реализации, поддержания в рабочем состоянии и улучшения управления защитой информации в организации. Цели, очерченные этим международным стандартом, дают общие руководящие принципы по обычно принимаемым целям управления защитой информации.

Цели и средства управления этого международного стандарта разработаны для реализации, осуществляющей с целью выполнить требования, выявленные оценкой рисков. Этот международный стандарт может служить в качестве практического руководства по разработке организационных стандартов защиты и практик эффективного управления защитой, а также для того, чтобы помочь создать доверие в межорганизационной деятельности.

2 Термины и определения

Для целей этого документа применяются следующие термины и определения.

2.1

актив [asset]

что-либо, что имеет ценность для организации

[ISO/IEC 13335-1:2004]

2.2

средство управления [control]

средства управления рисками, включая политику, процедуры, руководящие принципы, практики или организационные структуры, которые могут носить административный, технический, управляемический или юридический характер.

ПРИМЕЧАНИЕ:

Термин «средство управления» также используется как синоним термина «мера безопасности» или «контрмера».

2.3

руководящий принцип [guideline]

описание, которое разъясняет, что и как следует сделать, чтобы достичь целей, установленных политикой

[ISO/IEC 13335-1:2004]

2.4

средства обработки информации [information processing facilities]

любая система, служба или инфраструктура обработки информации, или фактическое месторасположение, где они находятся.

2.5

защита информации [information security]

сохранение конфиденциальности, целостности и доступности информации; кроме того, также могут быть включены другие свойства, такие как аутентичность, подотчетность, неотрекаемость и надежность

2.6

событие в системе защиты информации [information security event]

выявленный случай системы, услуги или состояния сети, указывающий на возможное нарушение в политике защиты информации или в работе средств защиты, или прежде неизвестная ситуация, которая может иметь значение для защиты

[ISO/IEC TR 18044:2004]

2.7

инцидент в системе защиты информации [information security incident]
одно или серия нежелательных или неожиданных событий в системе защиты информации, которые имеют большой шанс подвергнуть риску деловые операции и поставить под угрозу защиту информации

[ISO/IEC TR 18044:2004]

2.8

политика [policy]
общее намерение и направление, официально выраженное руководством

2.9

риск [risk]
комбинация вероятности события и его последствий

[ISO/IEC Guide 73:2002]

2.10

анализ риска [risk analysis]
систематическое использование информации для выявления источников и для оценки степени риска

[ISO/IEC Guide 73:2002]

2.11

оценка риска [risk assessment]
целостный процесс анализа риска и оценки значительности риска

[ISO/IEC Guide 73:2002]

2.12

оценка значительности риска [risk evaluation]
процесс сравнения расчетного риска с заданными критериями риска, с целью определить значительность риска

[ISO/IEC Guide 73:2002]

2.13

менеджмент рисков [risk management]
согласованные виды деятельности по руководству и управлению организацией в том, что касается рисков

[ISO/IEC Guide 73:2002]

2.14

обработка риска [risk treatment]
процесс выбора и реализации мер по изменению риска

[ISO/IEC Guide 73:2002]

2.15

третья сторона [third party]

лицо или организация, которые признаются независимыми от вовлеченных сторон в том, что касается рассматриваемой проблемы

[ISO/IEC Guide 2:1996]

2.16

угроза [threat]

возможная причина нежелательного инцидента, который может закончиться ущербом для системы или организации

[ISO/IEC 13335-1:2004]

2.17

слабое место [vulnerability]

слабость актива или группы активов, которой могут воспользоваться одна угроза или более

[ISO/IEC 13335-1:2004]

3 Структура этого стандарта

Этот стандарт содержит 11 разделов по средствам управления защитой информации, вместе содержащих в общей сложности 39 основных категорий защиты и один вступительный раздел, вводящий в оценку и обработку рисков.

3.1 Разделы

Каждый раздел содержит некоторое количество основных категорий защиты. Одиннадцать разделов (вслед за названием указано количество основных категорий защиты, включенных в каждый раздел) таковы:

- a) Политика в области защиты (1);
- b) Организация защиты информации (2);
- c) Менеджмент активов (2);
- d) Защита человеческих ресурсов (3);
- e) Физическая и экологическая безопасность (2);
- f) Управление средствами связи и операциями (10);
- g) Управление доступом (7);
- h) Приобретение, разработка и поддержание в рабочем состоянии информационных систем (6);
- i) Управление инцидентами в системе защиты информации (2);
- j) Менеджмент непрерывности бизнеса (1);
- k) Соответствие (3).

Примечание:

Порядок разделов в этом стандарте не означает их важность. В зависимости от обстоятельств, все статьи могут быть важны; поэтому каждой организации, применяющей этот стандарт, следует определить применимые разделы, то, насколько они важны, а также их приложение к отдельным деловым процессам. Также все списки в этом стандарте даны не в порядке приоритета, если это не указано.

3.2 Основные категории защиты

Каждая основная категория защиты содержит следующее:

- a) цель управления, формулирующая, чего надо достичь; и
- b) одно или более средств управления, которые могут быть применены для достижения цели управления.

Описания средств управления структурированы следующим образом:

Средство управления

Определяет конкретную стратегию управления для выполнения цели управления.

Руководство по реализации

Дает более подробную информацию для того, чтобы поддержать реализацию средства управления и выполнение цели управления. Некоторые из этих руководств могут не быть подходящими во всех случаях, так что другие способы реализации средств управления могут оказаться более подходящими.

Прочая информация

Дает дополнительную дальнейшую информацию, которую может понадобиться рассмотреть, например, вопросы юридического характера и ссылки на другие стандарты.

4 Оценка и обработка рисков

4.1 Оценивание рисков, связанных с нарушением защиты

Оценка рисков должна выявить, количественно определить и расположить в соответствии с приоритетом риски по отношению к критериям принятия рисков и целям, значимым для организации. Результаты должны направлять и определять соответствующее действие по управлению и приоритеты управления рисками, связанными с нарушением защиты информации, а также приоритеты реализации выбранных средств управления, с целью защититься от этих рисков. Процесс оценивания рисков и выбора средства управления может понадобиться выполнить несколько раз, чтобы охватить различные части организации или отдельные информационные системы.

Оценка рисков должна включать систематический метод оценки величины рисков (анализ рисков) и процесс сравнения предполагаемых рисков по отношению к критериям рисков, с целью определить значительность рисков (оценка значительности риска).

Также, оценки рисков должны выполняться периодически, чтобы учесть изменения в требованиях защиты и в рисковых ситуациях, например, в активах, угрозах, слабых местах, негативных воздействиях, оценке значительности рисков, а также когда происходят значительные изменения. Эти оценки рисков должны предприниматься методическим способом, способным дать сравнимые и воспроизводимые результаты.

Оценка рисков, связанных с нарушением защиты информации, должна иметь четко определенную область действия для того, чтобы быть результативной, и должна включать взаимосвязь с оценками рисков в других областях, если это уместно.

Областью действия оценки рисков может быть целая организация, части организации, отдельные информационные системные, конкретные компоненты систем или услуги там, где она осуществима, реалистична и полезна. Примеры методик оценки рисков обсуждаются в ISO/IEC TR 13335-3 (Руководящие принципы управления защитой информационных технологий: Методы управления защитой информационных технологий).

4.2 Обработка рисков, связанных с нарушением защиты

Прежде чем рассматривать обработку рисков, организация должна определить критерии для определения того, могут ли риски быть приняты или нет. Риски могут быть приняты, если, например, оценено, что риск является низким, или что стоимость обработки экономически невыгодна для организации. Такие решения должны быть записаны.

Для каждого выявленного риска вслед за оценкой риска должно быть принято решение об обработке риска. Возможные варианты обработки рисков включают следующее:

- a) применение подходящих средств управления для того, чтобы снизить риск;
- b) сознательное и объективное принятие рисков, при условии, что они четко соответствуют организационной политике и критериям для принятия рисков;
- c) избегание рисков путем недопущения действий, которые вызовут появление риска;
- d) передача связанных рисков другим сторонам, например, страховщикам или поставщикам.

Для тех рисков, для которых решение по обработке рисков состояло в применении подходящих средств управления, эти средства управления должны быть выбраны и реализованы, чтобы выполнить требования, выявленные оценкой рисков. Средства управления должны обеспечивать, чтобы риск снижался до приемлемого уровня, с учетом следующего:

- a) требования и ограничения национального и международного законодательства и норм;
- b) организационные цели;
- c) эксплуатационные требования и ограничения;
- d) стоимость реализации и работы в том, что касается снижаемых рисков, и оставаясь пропорциональным требованиям и ограничениям организации;
- e) потребность сбалансировать инвестиции в реализацию и работу средств управления по отношению к ущербу, который, вероятно может иметь место в результате нарушения защиты.

Средства управления можно выбрать из этого стандарта или из других наборов средств управления, или можно разработать новые средства управления для того, чтобы удовлетворить конкретные потребности организации. Необходимо осознавать, что некоторые средства управления могут быть неприменимы к каждой информационной системе или среде, и могут быть неосуществимыми для всех организаций. В качестве примера, в 10.1.3 описано, как можно разделить обязанности для того, чтобы предотвратить мошенничество и ошибку. Для организаций меньшего размера может оказаться невозможным разделить все обязанности, и могут понадобиться другие пути, достигающей той же самой цели управления. В качестве другого примера, в 10.10 описано, как можно постоянно контролировать использование системы и собирать доказательства. Описанные средства управления, например, ведение журнала регистрации событий, могут противоречить применимым законам, таким как обеспечение секретности для потребителей или на рабочем месте.

Средства управления защитой информации следует учитывать в системах, технических заданиях проектов на стадии проектирования. Неосуществление этого может привести к дополнительным издержкам и менее результативным решениям, и, может быть, в худшем случае, к неспособности достичь адекватной защиты.

Надо иметь в виду, что никакой набор средств управления не может достичь полной защиты, и что должно реализовываться дополнительное действие по управлению, с целью постоянно контролировать, оценивать и улучшать эффективность и результативность средств управления защитой, чтобы способствовать достижению целей организации.

5 Политика в области защиты

5.1 Политика в области защиты информации

Цель: Обеспечить направление управления защитой информации и поддержку защиты информации в соответствии с деловыми требованиями и применимыми законами и нормы.

Руководство должно установить четкое направление политики в соответствии с деловыми целями и демонстрировать поддержку защиты информации, а также обязательства по защите информации посредством выпуска и поддержания политики в области защиты по всей организации.

5.1.1 Программный документ в области защиты информации

Средство управления

Программный документ в области защиты информации должен быть утвержден руководством, опубликован и доведен до сведения всех служащих и внешних сторон, имеющих отношение к делу.

Руководство по реализации

В программном документе в области защиты информации должны быть указаны обязательство руководства и сформулирован подход организации к управлению защитой информации. В программном документе в области защиты информации должны содержаться заявления относительно следующего:

- a) определение защиты информации, ее общих целей, а также области действия и важности защиты как механизма, дающего возможность совместного использования информации (см. введение);
- b) формулировка намерений руководства, поддерживающих цели и принципы защиты информации в соответствии с деловой стратегией и целями;
- c) структура для установления целей и средств управления, включая структуру оценки рисков и управления рисками;
- d) краткое разъяснение политики, принципов, стандартов и требований соответствия в области защиты, особо важных для организации, включая:
 - 1) соответствие требованиям закона, норм и договоров;
 - 2) требования к образованию, подготовке и осведомленности в области защиты;
 - 3) менеджмент непрерывности бизнеса;

- 4) последствия нарушений политики в области защиты информации;
- e) определение общих и специальных обязанностей по управлению защитой информации, включая отчеты об инцидентах в системе защиты информации;
- f) ссылки на документацию, которая может поддержать политику, например, более подробные политика и процедуры в области защиты для конкретных информационных систем или правила защиты, которым должны следовать пользователи.

Этот программный документ области защиты информации следует распространить по всей организации пользователям в форме, которая являлась бы соответствующей, доступной и понятной для предполагаемого читателя.

Прочая информация

Программный документ в области защиты информации может быть частью общего программного документа. Если политика в области защиты информации распространяется за пределы организации, то следует позаботиться о том, чтобы не раскрыть важную информацию². Дополнительную информацию можно найти в ISO/IEC 13335-1:2004.

5.1.2 Анализ политики в области защиты информации

Средство управления

Политику в области защиты информации следует анализировать через запланированные промежутки времени или в случае возникновения значительных изменений, с целью обеспечить ее продолжающееся соответствие, адекватность и результативность.

Руководство по реализации

Политика в области защиты информации должна иметь владельца, который утвердил ответственность руководства за разработку, анализ и оценку политики в области защиты. Анализ должен включать в себя оценивание возможностей для улучшения организационной политики в области защиты информации и подход к управлению защитой информации в ответ на изменения в организационном окружении, деловых обстоятельствах, юридических условиях или в технической среде.

Анализ политики в области защиты должен учитывать результаты анализа со стороны руководства. Должны быть определены процедуры анализа со стороны руководства, включая график или период анализа.

² важная [значимая, секретная, конфиденциальная, критичная] информация (sensitive information) — информация, потеря, раскрытие или уничтожение которой по тем или иным причинам нежелательны для бизнеса, функционирования системы, или её владельца.

Входные данные для анализа со стороны руководства должны включать информацию по следующим вопросам:

- a) обратная реакция заинтересованных сторон;
- b) результаты независимых анализов (см. 6.1.8);
- c) статус предупреждающих и корректирующих действий (см. 6.1.8 и 15.2.1);
- d) результаты предыдущего анализа со стороны руководства;
- e) выполнение процессов и соответствие политике в области защиты информации;
- f) изменения, которые могут повлиять на подход организации к управлению защитой информации, включая изменения в организационном окружении, деловых обстоятельствах, доступности ресурсов, договорных, нормативных и юридических условиях или в технической среде;
- g) тенденции, связанные с угрозами и слабыми местами;
- h) полномочные инциденты в системе защиты информации (см. 13.1);
- i) рекомендации, предоставленные соответствующими органами (см. 6.1.6).

Выходные данные для анализа со стороны руководства должны включать любые решения и действия, касающиеся следующего:

- a) улучшение подхода организации к управлению защитой информации и ее процессами;
- b) улучшение целей и средств управления;
- c) улучшение в распределении ресурсов и/или обязанностей.

Должна поддерживаться в рабочем состоянии запись анализа со стороны руководства.

Должно быть получено утверждение руководства для пересмотренной политики.

6 Организация защиты информации

6.1 Внутренняя организация

Цель: Управлять защитой информации в организации.

Для того чтобы начать и контролировать реализацию защиты информации в организации, следует создать схему управления.

Руководство должно одобрить политику в области защиты информации, назначать роли в области защиты, а также координировать и анализировать реализацию защиты по всей организации.

Если необходимо, то следует создать источник консультаций специалиста по защите информации и сделать его доступным в организации. Следует развивать контакты с внешними специалистами по защите или группами, включая соответствующие органы, чтобы идти в ногу с тенденциями развития сферы деятельности, наблюдать за стандартами и методами оценки и обеспечивать наличие подходящего контактного лица при обработке инцидентов в системе защиты информации.

Следует поощрять междисциплинарный подход к защите информации.,

6.1.1 Обязательства руководства по защите информации

Средство управления

Руководству следует активно поддерживать защиту в организации посредством четких распоряжений, демонстрируемых обязательств, точного назначения и признания обязанностей в области защиты информации.

Руководство по реализации

Руководству следует:

- a) обеспечивать, чтобы были определены цели в области защиты информации, чтобы они отвечали организационным требованиям и были встроены в соответствующие процессы;
- b) формулировать, анализировать и утверждать политику в области защиты информации;
- c) анализировать результативность реализации политики в области защиты;
- d) обеспечивать четкие распоряжения и видимую поддержку со стороны руководства в отношении инициатив в области защиты;
- e) обеспечивать ресурсы, необходимые для защиты информации;

- f) утверждать назначение конкретных ролей и обязанностей для защиты информации по всей организации;
- g) инициировать планы и программы для поддержки осведомленности в области защиты информации;
- h) обеспечивать, чтобы реализация средств управления защитой информации была скоординирована по всей организации (см. 6.1.2).

Руководству следует идентифицировать потребность в консультациях внутреннего или внешнего специалиста в области защиты информации, а также анализировать и координировать результаты консультаций по всей организации.

В зависимости от размера организации, такие обязанности могут контролироваться специальным заседанием форума по проблемам управления или существующим органом управления, таким как совет директоров.

Прочая информация

Дополнительная информация содержится в ISO/IEC 13335-1:2004.

6.1.2 Координация защиты информации

Средство управления

Деятельность по защите информации следует скоординировать с представителями различных частей организации с соответствующими ролями и рабочими функциями.

Руководство по реализации

Обычно, в координацию защиты информации следует включить сотрудничество и совместную работу менеджеров, пользователей, администраторов, разработчиков прикладных программ, аудиторов и персонал службы защиты, а также опыт специалистов в таких областях, как, например, страхование, юридические вопросы, человеческие ресурсы, информационные технологии (ИТ) или менеджмент рисков. Эта деятельность должна:

- a) обеспечивать, чтобы деятельность по защите выполнялась в соответствии с политикой в области защиты информации;
- b) определять, как обращаться с несоответствиями;
- c) утверждать методики и процессы для защиты информации, например, оценку рисков, классификацию информации;
- d) выявлять значительные изменения угроз, а также подверженность информации и средств обработки информации угрозам;
- e) оценивать адекватность и координировать реализацию средств управления защитой информации;

- f) результативно продвигать образование, подготовку и осведомленность в области защиты информации по всей организации;
- g) оценивать информацию, полученную из постоянного контроля и анализа инцидентов в системе защиты информации, и рекомендовать подходящие действия в ответ на выявленные инциденты в системе защиты информации.

Если организация не использует отдельную многофункциональную группу, например, поскольку такая группа не подходит для размера организации, то действия, описанные выше, должны осуществляться другим подходящим органом управления или отдельным менеджером.

6.1.3 Распределение обязанностей по защите информации

Средство управления

Все обязанности по защите информации следует четко распределить.

Руководство по реализации

Распределение обязанностей по защите информации должно быть сделано в соответствии с политикой в области защиты информации (см. раздел 4). Должны быть четко определены обязанности по защите отдельных активов и по выполнению конкретных процессов защиты. Эти обязанности должны быть дополнены, если это необходимо, более подробным руководством для конкретных местоположений и средств обработки информации. Должны быть четко определены локальные обязанности по защите активов и по выполнению конкретных процессов защиты, таких как планирование непрерывности бизнеса.

Лица с назначенными обязанностями по защите могут передавать задания по защите другим. Тем не менее, они остаются ответственными и должны определять, что любое переданное задание было выполнено правильно.

Должны быть четко сформулированы области, за которые лица несут ответственность; в частности, должно иметь место следующее:

- a) должны быть выявлены и четко определены активы и процессы защиты, связанные с каждой конкретной системой;
- b) должен быть назначен объект, ответственный за каждый актив или процесс защиты, а подробности этой ответственности должны быть документально подтверждены (см. также 7.1.2);
- c) должны быть четко определены и документально подтверждены уровни полномочий.

Прочая информация

Во многих организациях, будет назначен менеджер по защите информации, чтобы взять на себя полную ответственность за разработку и реализацию защиты, а также за поддержку определения средств управления.

Тем не менее, ответственность за комплектование штата и реализацию средств управления часто останется за отдельными менеджерами. Одна из общих практик состоит в том, чтобы назначить владельца для каждого актива, который затем становится ответственным за его повседневную защиту.

6.1.4 Процесс получения разрешения для средств обработки информации

Средство управления

Должен быть определен и осуществлен процесс выдачи разрешения руководства для новых средств обработки информации.

Руководство по реализации

Для процесса выдачи разрешения должны быть приняты во внимание следующие руководящие принципы:

- a) новые средства должны иметь надлежащее разрешение руководства пользователя, объясняющее их цель и использование. Также должно быть получено разрешение менеджера, ответственного за поддержание в рабочем состоянии среды защиты локальной информационной системы, чтобы обеспечить выполнение соответствующей политики и требований в области защиты;
- b) если это необходимо, то аппаратное и программное обеспечение должны быть проверены, с целью гарантировать, что они совместимые с другими компонентами системы;
- c) использование для обработки деловой информации личных или находящихся в частной собственности средств обработки информации, например, небольших портативных компьютеров, домашних компьютеров или карманных устройств, может привнести новые слабые места, и необходимо определять и реализовывать необходимые средства управления.

6.1.5 Соглашения о конфиденциальности

Средство управления

Должны выявляться и регулярно анализироваться соглашения о требованиях конфиденциальности или о неразглашении, отражающие потребности организации в защите информации.

Руководство по реализации

Соглашения о конфиденциальности или о неразглашении должны учитывать требование защитить конфиденциальную информацию, используя законно осуществимые условия. Для того чтобы определить соглашения о требованиях конфиденциальности или о неразглашении, надо рассмотреть следующие элементы:

- a) определение информации, которую нужно защищать (например, конфиденциальная информация);

- b) ожидаемая продолжительность соглашения, включая случаи, когда может оказаться, что конфиденциальность необходимо поддерживать неограниченно;
- c) необходимые действия при расторжении соглашения;
- d) обязанности и действия подписавших сторон, с целью избежать неразрешенного раскрытия информации (например, «принцип необходимого знания»);
- e) собственность на информацию, секреты производства и интеллектуальная собственность, и как это связано с защитой конфиденциальной информации;
- f) разрешенное использование конфиденциальной информации, и права подписавшей стороны использовать информацию;
- g) право проверять и постоянно контролировать деятельность, которая вовлекает конфиденциальную информацию;
- h) процесс для извещения и составления отчета о неразрешенном раскрытии или о неразрешенном доступе к конфиденциальной информации;
- i) условия возвращения информации или уничтожения информации при прекращении действия соглашения; и
- j) ожидаемые действия, которые нужно предпринять в случае нарушения этого соглашения.

В соглашении о конфиденциальности или неразглашении могут понадобиться другие элементы, основанные на организационных требованиях защиты.

Соглашения о конфиденциальности или о неразглашении должны подчиняться всем применимым законам и нормам юрисдикции, к которой они применяются (см. также 15.1.1).

Соглашения о требованиях конфиденциальности или о неразглашении должны анализироваться периодически и при возникновении изменений, которые влияют на эти требования.

Прочая информация

Соглашения о конфиденциальности или о неразглашении защищают организационную информацию и извещают подписавшие стороны об их ответственности, с целью защищать, использовать и раскрывать информацию ответственным и разрешенным способом.

При разных обстоятельствах, организация может иметь потребность в использовании различных форм соглашений о конфиденциальности или о неразглашении.

6.1.6 Контакты с органами

Средство управления

Должны поддерживаться надлежащие контакты с соответствующими органами.

Руководство по реализации

Организации должны иметь в рабочем состоянии процедуры, которые точно определяют, когда и кому надлежит вступать в контакт с органами (например, правоохранительные органы, пожарное отделение, органы надзора), и то, как следует своевременно сообщить о выявленных инцидентах в системе защиты информации, если есть подозрение, что закон мог быть нарушен.

Организациям, атакуемым из Интернета, может понадобиться, чтобы внешние трети стороны (например, поставщик услуг Интернета или оператор связи) предприняли меры против источника атаки.

Прочая информация

Поддержание таких контактов может быть требованием поддерживать менеджмент инцидентов в системе защиты информации (Раздел 13.2) или непрерывности бизнеса и процесс планирования чрезвычайных обстоятельств (Раздел 14). Контакты с регулятивными органами также полезны для того, чтобы предполагать предстоящие изменения в законе или нормах, которым организации надлежит следовать, и готовиться к ним. Контакты с другими органами включают коммунальные предприятия, аварийные службы и охрану труда, например, пожарные команды (в связи с деловой непрерывностью), поставщики телекоммуникационных услуг (в связи с прокладкой и доступностью линий связи), поставщики воды (в связи со средствами охлаждения для оборудования).

6.1.7 Контакты со специальными группами

Средство управления

Должны поддерживаться надлежащие контакты со специальными группами (группами по конкретной проблеме) или другими форумами специалистов по защите информации и профессиональными объединениями.

Руководство по реализации

Членство в специальных группах или форумах должно рассматриваться как средство для следующего:

- a) улучшать знание о наилучших практиках и оставаться в курсе значимой информации по безопасности;
- b) обеспечивать, чтобы понимание среды защиты информации было современным и полным;

- c) получать ранние предупреждения о тревогах, консультантах и вставках в программы, имеющих отношение к атакам и слабым местам;
- d) получить доступ к консультациям специалиста по защите информации;
- e) совместно использовать информацию о новых технологиях, продуктах, угрозах или слабых местах и обмениваться этой информацией;
- f) обеспечить подходящие точки контакта при работе с инцидентами в системе защиты информации (см. также 13.2.1).

Прочая информация

Для того чтобы улучшить сотрудничество и согласование вопросов защиты, могут быть заключены соглашения по совместному использованию информации. Такие соглашения должны определять требования по защите важной информации.

6.1.8 Независимый анализ защиты информации

Средство управления

Подход организации к управлению защитой информации и ее реализации (т. е. цели управления, средства управления, политика, процессы и процедуры для защиты информации) должны независимо анализироваться через запланированные промежутки времени, или когда происходят значительные изменения в реализации защиты.

Руководство по реализации

Независимый анализ должен быть инициирован руководством. Такой независимый анализ необходим для того, чтобы обеспечить дляящуюся годность, адекватность и результативность подхода организации к управлению защитой информации. Анализ должен включать оценивание возможностей для улучшения и потребность в изменениях в подходе к защите, включая политику и цели в области управления.

Такой анализ должен выполняться лицами, независимыми от анализируемых областей, например, отделом внутреннего аудита, независимым менеджером или сторонней организацией, специализирующейся на таком анализе. Лица, выполняющие этот анализ, должны иметь подходящие навыки и опыт.

Результаты независимого анализа должны быть записаны и сообщены руководству, которое инициировало анализ. Эти записи должны поддерживаться в рабочем состоянии.

Если независимый анализ выявляет, что организационный подход к управлению защитой информации и реализации этой защиты неадекватен или не соответствует направлением защиты информации, установленным в программном документе по защите информации (см. 5.1.1), то руководство должно рассмотреть корректирующие действия.

Прочая информация

Область, которую должны регулярно анализировать менеджеры (см. 15.2.1), также может анализироваться независимо. Методы анализа могут включать опросы руководства, контролирующие записи или анализ программных документов по защите. ИСО 19011:2002, «Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента», также может дать полезные руководящие указания по выполнению независимого анализа, включая создание и реализацию программы анализа. В разделе 15.3 определяются средства управления, значимые для независимого анализа операционных информационных систем и использования средств аудита систем.

6.2 Внешние стороны

Цель: Поддерживать в рабочем состоянии защиту информации и средства обработки информации организации, к которым имеют доступ внешние стороны, которые обрабатываются внешними сторонами, передаются внешним сторонам или управляются внешними сторонами.

Защита информации и средств обработки информации организации не должна уменьшаться вследствие ввода продуктов или услуг внешних стороны.

Любой доступ внешних сторон к средствам обработки информации организации, а также обработка и передача информации внешними сторонами, должны контролироваться.

Если есть деловая потребность в работе с внешними сторонами, которая может потребовать доступа к информации и средствам обработки информации организации, или при получении или предоставлении продукции и услуги от внешней стороны или внешней стороне, то должна быть выполнена оценка рисков, с целью определить включение защиты и требования контроля. Средства управления должны быть согласованы и определены в соглашении с внешней стороной.

6.2.1 Выявление рисков, связанных с внешними сторонами

Средство управления

До предоставления доступа должны быть выявлены риски для информации и средств обработки информации организации, проистекающие из деловых процессов, вовлекающих внешние стороны, и должны быть реализованы соответствующие средства управления.

Руководство по реализации

Если есть потребность в разрешении допуска внешней стороны к средствам обработки информации или информации организации, то должна быть выполнена оценка рисков (см. также раздел 4), с целью определить любые требования для конкретных средств управления. Выявление рисков, связанных с доступом внешних сторон, должно учитывать следующие вопросы:

- a) средства обработки информации, к которым требуется иметь доступ внешней стороне;
- b) тип доступа, который внешняя сторона будет иметь к информации и средствам обработки информации, например, следующее:
 - 1) физический доступ, например, в офисы, компьютерные комнаты, картотечные шкафы;
 - 2) логический доступ, например, к базам данных, информационным системам организации;
 - 3) связность узлов в сети между сетью(сетями) организации и внешней стороны, например, неразъемное соединение, удаленный доступ;
 - 4) происходит ли доступ на месте или со стороны;
- c) ценность и конфиденциальность вовлеченной информации, а также ее критичность для деловых операций;
- d) средства управления, необходимые для защиты информации, которая не предназначена для того, чтобы быть доступной внешним сторонам;
- e) персонал внешний стороны, вовлеченный в работу с информацией организации;
- f) как могут быть обозначены организация или персонал, которым был разрешен доступ, как может быть верифицировано наличие разрешения, и как часто его необходимо подтверждать;
- g) различные способы и средства управления, применяемые внешней стороной при хранении, обработке, передаче, совместном использовании информации и обмене информацией;
- h) негативное влияние ситуации, когда внешней стороне не предоставляется требуемый доступ, и когда внешняя сторона вводит или получает неточную или вводящую в заблуждение информацию;
- i) практики и процедуры по работе с инцидентами в системе защиты информации и возможными повреждениями, а также условия для продолжения доступа внешней стороны в случае инцидента в системе защиты информации;

- j) требования закона, прочие обязательные требования, а также другие договорные обязательства, значимые для внешней стороны, которые должны быть учтены;
- k) как эти меры могут повлиять на интересы любых других заинтересованных сторон.

Доступ внешних сторон к информации организации не должен предоставляться до тех пор, пока не будут реализованы надлежащие средства управления, и, если выполнимо, до тех пор, пока не будет подписан договор, определяющий постановления и условия для соединения или доступа, а также рабочий механизм. Обычно, все требования защиты, проистекающие из работы с внешними сторонами, или внутренние средства управления должны быть отражены соглашением с внешней стороной (см. также 6.2.2 и 6.2.3).

Следует обеспечить, чтобы внешняя сторона отдавала себе отчет о своих обязательствах и принимала обязанности и ответственность, связанные с осуществлением доступа, обработкой, передачей или управлением информацией и средствами обработки информации организации.

Прочая информация

Информация может подвергаться риску внешними сторонами с ненадлежащим управлением защитой. Должны быть определены и применены средства управления для того, чтобы руководить доступом внешней стороны к средствам обработки информации. Например, если есть особая потребность в конфиденциальности информации, то можно использовать соглашения о неразглашении.

Организации могут столкнуться с риском, связанным с межорганизационными процессами, управлением и обменом информацией, если применяется высокая степень аутсорсинга³, или если вовлечено несколько внешних сторон.

Средства управления 6.2.2 и 6.2.3 охватывают различные соглашения с внешними сторонами, включая, например, следующие:

- a) поставщики услуги, таких как поставщики Интернет-услуг, поставщики сетевых услуг, услуг телефонной связи, услуг по текущему обслуживанию и поддержке;
- b) управляемые услуги защиты;
- c) потребители;
- d) аутсорсинг оборудования и/или операций, например, информационных систем, услуг по сбору данных, операций центра обработки вызовов;
- e) консультанты по вопросам управления и бизнеса, а также аудиторы;

³ аутсорсинг [outsourcing] — использование внешних ресурсов для решения собственных задач (Прим. перевода)

- f) разработчики и поставщики, например, программных продуктов и информационных систем;
- g) сторонние услуги по очистке, обслуживанию и другие вспомогательные услуги;
- h) временный персонал, размещение студентов, а также другие временные краткосрочные договоры.

Такие соглашения могут помочь снизить риски, связанные с внешними сторонами.

6.2.2 Рассмотрение защиты при работе с потребителями

Средство управления

Следует рассмотреть все выявленные требования защиты прежде, чем предоставлять потребителям доступ к информации или активам организации.

Руководство по реализации

Для того чтобы рассмотреть защиту перед предоставлением доступа потребителям к любому из активов организации (в зависимости от типа и степени предоставляемого доступа данных, не все из нижеследующего можно применить) следует рассмотреть следующие условия:

- a) защита актива, включая следующее:
 - 1) процедуры для защиты активов организации, включая информацию и программное обеспечение, а также управление известными слабыми местами;
 - 2) процедуры для определения того, не произошла ли какая-либо компрометация активов, например, потеря или изменение данных;
 - 3) целостность;
 - 4) ограничения на копирование и раскрытие информации;
- b) описание продукта или услуги, которые предстоит предоставить;
- c) различные причины, требования и выгоды для доступа потребителя;
- d) политика управления доступом, охватывающая следующее:
 - 1) разрешенные методы доступа, а также управление уникальными идентификаторами, такими как, идентификаторы и пароли пользователя, и их использование;
 - 2) процесс выдачи разрешения для доступа и привилегий пользователя;
 - 3) заявление о том, что весь доступ, который прямо не разрешен, запрещен;

- 4) процесс отмены прав доступа или прерывания связи между системами;
- e) мероприятия по составлению отчетов и по уведомлению об информационных неточностях (например, персональных данных), об инцидентах и нарушениях в системе защиты информации, а также мероприятия по расследованию вышеперечисленного;
- f) описание каждой услуги, которую предстоит сделать доступной;
- g) заданный уровень обслуживания и неприемлемые уровни обслуживания;
- h) право постоянно контролировать и отменять любую деятельность, имеющую отношение к активам организации;
- i) соответствующие обязательства организации и потребителя;
- j) обязанности в том, что касается юридических вопросов, и как обеспечивается выполнение требований закона, например, законов по защите данных, особенно с учетом различных национальных правовых систем, если соглашение включает сотрудничество с потребителями в других странах (см. также 15.1);
- k) передача прав на интеллектуальную собственность (ПИС) и авторских прав (см. 15.1.2), а также защита любой совместной работы (см. также 6.1.5).

Прочая информация

Требования защиты, имеющие отношение к потребителям, получающим доступ к активам организации, могут значительно различаться в зависимости от средств обработки информации и информации, к которым осуществляется доступ. Эти требования защиты можно учесть, используя соглашения с потребителями, которые содержат все выявленные риски и требования защиты (см. 6.2.1).

Соглашения с внешними сторонами могут также вовлекать другие стороны. Соглашения, предоставляющие доступ внешним сторонам, должны включать в себя допущение назначения других подходящих сторон и условий для их доступа и участия.

6.2.3 Учет защиты в соглашениях с третьими сторонами

Средство управления

Соглашения с третьими сторонами, включающие доступ, обработку, передачу информации или средств обработки информации организации или управление информацией или средствами обработки информации организации, или добавление продукции или услуг к средствам обработки информации, должны включать в себя все значимые требования защиты.

Руководство по реализации

Соглашение должно гарантировать отсутствие недоразумений между организацией и третьей стороной. Организации должны убедиться в том, что касается гарантии от убытков третьей стороны.

Для того чтобы выполнить выявленные требования защиты (см. 6.2.1), для включения в соглашение следует рассмотреть следующие условия:

- a) политика в области защиты информации;
- b) средства управления для обеспечения защиты активов, включая следующее:
 - 1) процедуры для защиты активов организации, включая информацию, программное обеспечение и аппаратные средства;
 - 2) любые необходимые средства управления и механизм физической защиты;
 - 3) средства управления для обеспечения защиты от злонамеренного программного обеспечения (см. 10.4.1);
 - 4) процедуры для определения того, не произошло ли какой-либо компрометации активов, например, потери или изменения информации, программного обеспечения и аппаратных средств;
 - 5) средства управления для обеспечения возврата или уничтожения информации и активов в конце соглашения или в согласованный момент времени в ходе соглашения;
 - 6) конфиденциальность, целостность, доступность и любое другое важное свойство (см. 2.1.5) активов;
 - 7) ограничения на копирование и раскрытие информации, а также использование соглашений о конфиденциальности (см. 6.1.5);
- c) подготовка пользователей и администраторов по методам, процедурам и защите;
- d) обеспечение осведомленности пользователя об обязанностях и проблемах в области защиты;
- e) обеспечение перевода персонала, если это необходимо;
- f) обязанности, касающиеся установки и текущего обслуживания аппаратных средств и программного обеспечения;
- g) четкая структура отчетности и согласованные форматы составления отчетов;
- h) четкий и точно определенный процесс управления изменениями;

- i) политика управления доступом, включая следующее:
 - 1) различные причины, требования и преимущества, которые делают доступ третьей стороны необходимым;
 - 2) разрешенные методы доступа, а также управление уникальными идентификаторами, такими как идентификаторы и пароли пользователя, и их использование;
 - 3) процесс выдачи разрешения для доступа и привилегий пользователей;
 - 4) требование поддерживать список лиц, которым разрешено использовать услуги, сделанные доступными, и каковы их права и привилегии в том, что касается такого использования;
 - 5) заявление о том, что весь доступ, который прямо не разрешен, запрещен;
 - 6) процесс отмены прав доступа или прерывания связи между системами;
- j) мероприятия по составлению отчетов и по уведомлению об инцидентах и нарушениях в системе защиты информации, равно как и о нарушениях требований, сформулированных в соглашении, а также расследование вышеперечисленного;
- k) описание продукции или услуги, которую предстоит предоставлять, а также описание информации, которую предстоит сделать доступной вместе с ее категорией защиты (см. 7.2.1);
- l) заданный уровень обслуживания и неприемлемые уровни обслуживания;
- m) определение верифицируемых критериев исполнения, их постоянный контроль и отчет о них;
- n) право постоянно контролировать и отменять любую деятельность, имеющую отношение к активам организации;
- o) право осуществлять аудит обязанностей, определенных в соглашении, право иметь результаты этих аудитов, выполненных третьей стороной, и право перечислить законные права аудиторов;
- p) установление порядка рассмотрения вышестоящими инстанциями для решения внутренних проблем;
- q) требования непрерывности услуги, включая меры доступности и надежности, в соответствии с деловыми приоритетами организации;
- r) соответствующие обязательства участников соглашения;

- s) обязанности в том, что касается юридических вопросов, и в том, как обеспечивается выполнение требований закона, например, законов по защите данных, особенно с учетом различных национальных правовых систем, если соглашение включает сотрудничество с потребителями в других странах (см. также 15.1);
- t) передача прав на интеллектуальную собственность (ПИС) и авторских прав (см. 15.1.2), а также защита любой совместной работы (см. также 6.1.5).
- u) участие третьей стороны с субподрядчиками, и средства управления защитой, которые необходимо реализовать этим субподрядчикам;
- v) условия для пересмотра/прекращения действия соглашений:
 - 1) должен быть принят чрезвычайный план на случай, если какая либо из сторон захочет прекратить отношения до конца соглашения;
 - 2) пересмотр соглашений, если требования защиты организации изменяются;
 - 3) текущая документация списков активов, лицензий, соглашений или связанных с ними прав.

Прочая информация

Соглашения могут значительно различаться для разных организаций и для различных типов третьих сторон. Следовательно, следует позаботиться о том, чтобы включить в соглашения все выявленные риски и требования защиты (см. также 6.2.1). Если это необходимо, требуемые средства управления и процедуры могут быть расширены в план по управлению защитой.

Если осуществляется аутсорсинг управления защитой информации, то соглашения должны учитывать то, как третья сторона будет обеспечивать поддержание в рабочем состоянии требуемой защиты, определенной оценкой рисков, и как защита будет приспосабливаться для выявления изменений в рисках и работы с ними.

Некоторые различия между аутсорсингом и другими формами предоставления услуг третьих сторон включают вопрос ответственности, планирование переходного периода и возможное прерывание операций в течение этого периода, мероприятия по планированию чрезвычайных обстоятельств и анализ должностной старательности, а также сбор информации об инцидентах в системе защиты и управление этой информацией. Следовательно, важно, чтобы организация планировала и управляла переходом к мероприятиям, осуществляемым извне, и имела в действии подходящие процессы для управления изменениями и пересмотром/прекращением действия соглашений.

В соглашении необходимо учсть процедуры для продолжающейся обработки в том случае, если третья сторона становится не в состоянии поставить свои услуги, с целью избежать любой задержки в организации запасных услуг.

Соглашения с третьими сторонами могут также вовлекать другие стороны. Соглашения, предоставляющие доступ третьим сторонам, должны включать возможность назначения других подходящих сторон и условий их доступа и участия.

Обычно соглашения первоначально разрабатываются организацией. В некоторых обстоятельствах могут быть случаи, когда где соглашение может быть разработано и навязано организации третьей стороной. Организации необходимо гарантировать, что требования третьей стороны, оговариваемые в продиктованных соглашениях, не оказывают излишнего негативного влияния на ее собственную защиту.

7 Менеджмент активов

7.1 Ответственность за активы

Цель: Достичь и поддерживать в рабочем состоянии надлежащую защиту организационных активов.

Все активы должны быть учтены и должны иметь назначенного владельца.

Владельцы должны быть определены для всех активов, и должна быть назначена ответственность за поддержание в рабочем состоянии подходящих средств управления. Реализация конкретных средств управления может быть делегирована владельцем, по обстоятельствам, но владелец остается ответственным за должную защиту активов.

7.1.1 Опись активов

Средство управления

Все активы должны быть четко определены, должна быть составлена и должна поддерживаться в рабочем состоянии опись всех важных активов.

Руководство по реализации

Организация должна выявить все активы и документально подтвердить важность этих активов. Опись активов должна включать всю информацию, необходимую для восстановления после бедствия, включая тип актива, формат, местоположение, дублирующую информацию, информацию о лицензиях, а также ценность для бизнеса. Опись не должна излишне дублировать другие описи, но следует обеспечить, чтобы содержимое было синхронизировано.

Кроме того, собственность (см. 7.1.2) и классификация информации (см. 7.2) должны быть согласованы и документально подтверждены для каждого из активов. На основе важности актива, должны быть определены его ценность для бизнеса и категория защиты, уровни защиты, соразмерные с важностью активов (дополнительную информацию о том, как оценивать активы для того, чтобы представить их важность, можно найти в ISO/IEC TR 13335-3).

Прочая информация

Существует много типов активов, включая следующее:

- a) информация: базы данных и файлы данных, договоры и соглашения, системная документация, научно-исследовательская информация, руководства пользователя, учебный материал, процедур эксплуатации или вспомогательные процедуры, планы обеспечения непрерывности бизнеса, мероприятия по нейтрализации неисправности, контрольные журналы и архивированная информация;
- b) программные активы: прикладные программы, системные программы, инструментальные средства разработки и утилиты;
- c) физические активы: компьютерное оборудование, аппаратура связи, сменные носители информации и другое оборудование;
- d) услуги: обработка данных и услуги связи, общие коммунальные услуги, например, обогрев, освещение, энергия и кондиционирование воздуха;
- e) люди, их квалификация, способности и опыт;
- f) нематериальные активы, такие как репутация и имидж организации.

Описи активов помогают обеспечить наличие результативной защиты активов и также могут быть необходимы для других деловых целей, таких как техника безопасности и охрана труда, страхование или финансовые причины (менеджмент активов). Процесс составления описи активов является важным предварительным условием управления рисками (см. также раздел 4).

7.1.2 Собственность на активы

Средство управления

Вся информация и активы, связанные со средствами обработки информации, должны находиться во владении⁴ определенной части организации.

Руководство по реализации

Владелец актива должен нести ответственность за следующее:

- a) обеспечение того, чтобы информация и активы, связанные со средствами обработки информации, были надлежащим образом классифицированы;
- b) определение и периодический анализ ограничений и классификаций доступа, с учетом применимой политики в области управления доступом.

⁴ Термин «владелец» означает личность или объект, которые утвердили административную ответственность за управление производством, разработкой, поддержанием в рабочем состоянии, использованием и защитой активов. Термин «владелец» не означает, что человек действительно имеет какие-либо права собственности в отношении актива.

Собственность может быть назначена на следующее:

- a) деловой процесс;
- b) определенный набор видов деятельности;
- c) приложение; или
- d) определенный набор данных.

Прочая информация

Рутинные задачи можно делегировать, например, хранителю, ежедневно присматривающему за активом, но ответственность остается на владельце.

В сложных информационных системах может быть полезным определить группы активов, которые действуют вместе для того, чтобы обеспечить конкретную функцию как «услуги». В этом случае, владелец услуги ответственен за предоставление услуги, включая функционирование активов, которые обеспечивают ее предоставление.

7.1.3 Приемлемое использование активов

Средство управления

Правила приемлемого использования информации и активов, связанных со средствами обработки информации, должны быть определены, документально подтверждены и реализованы.

Руководство по реализации

Все служащие, подрядчики и пользователи третьих сторон должны следовать правилам приемлемого использования информации и активов, связанных со средствами обработки информации, включая следующие правила:

- a) правила использования электронной почты и Интернет (см. 10.8);
- b) руководящие принципы использования мобильных устройств, особенно для использования за пределами помещений организации (см. 11.7.1);

Конкретные правила или руководящие указания должны предоставляться соответствующим руководством. Служащие, подрядчики и пользователи третьих сторон, использующие или имеющие доступ к активам организации, должны быть осведомлены о пределах, существующих для их пользования информацией и активами организации, связанными со средствами обработки информации, а также ресурсами организации. Они должны быть ответственными за пользование любыми ресурсами по обработке информации, и любого такого пользования, осуществленного под их ответственность.

7.2 Классификация информации

Цель: Обеспечить, чтобы информация получала надлежащий уровень защиты.

Информация должна быть классифицирована, с целью указывать потребность в защите, приоритеты защиты и ожидаемую степень защиты при обращении с информацией.

Информация имеет различные степени важности и критичности. Некоторые элементы могут потребовать дополнительного уровня защиты или специального обращения. Для определения подходящего набора уровней защиты и сообщения о потребности в мерах по специальному обращению должна быть использована схема классификации информации.

7.2.1 Руководящие указания по классификации

Средство управления

Информация должна быть классифицирована с точки зрения ее значимости, требований закона, конфиденциальности и критичности для организации.

Руководство по реализации

Классификации и связанные с ней защитные средства управления для информации должны учитывать потребности бизнеса в разделении или ограничении информации, а также негативное влияние на бизнес, связанное с такими потребностями.

Руководящие указания по классификации должны включать соглашения о начальной классификации и повторной классификации с течением времени; в соответствии с некоторой предварительно определенной политикой в области управления доступом (см. 11.1.1).

Владелец актива должен быть ответственен (см. 7.1.2) за определение классификации актива, ее периодический анализ и обеспечение того, что она поддерживается на уровне современных требований и на подходящем уровне. Классификация должна учитывать эффект агрегации, упоминаемый в 10.7.2.

Следует уделить внимание числу категорий классификации и выгодам, которые нужно получить из их использования. Чрезмерно сложные схемы могут стать громоздкими и неэкономичными для использования или на практике оказаться невыполнимыми. Следует быть внимательным при интерпретации классификационных этикеток на документах из других организаций, которые могут иметь другие определения для этикеток с тем же самым или аналогичным названием.

Прочая информация

Уровень защиты может быть оценен путем анализа конфиденциальности, целостности и доступности, а также любых других требований для рассматриваемой информации.

Информация часто перестает быть важной или критической спустя определенный период времени, например, когда информация была сделана общеизвестной. Эти аспекты должны быть приняты во внимание, поскольку чрезмерная классификация может привести к реализации необязательных средств управления, дающих в результате дополнительные расходы.

Рассмотрение документов с аналогичными требованиями защиты вместе с назначением уровней классификации может помочь упростить задачу классификации.

В общих чертах, классификация, придаваемая информации – это краткий способ определить то, как надлежит обращаться с этой информацией, и как ее надо защищать.

7.2.2 Маркировка информации и обращение с информацией

Средство управления

В соответствии со схемой классификации, принятой организацией, должен быть разработан и реализован соответствующий набор процедур для маркировки информации и обращения с информацией.

Руководство по реализации

Необходимо, чтобы процедуры для маркировки информации охватывали информационные активы в физических и электронных форматах.

Выход из систем, содержащих информацию, которая классифицируется как важная или критичная, должен иметь на себе соответствующую классификационную этикетку (на выходе). Маркирование должно отражать классификацию в зависимости от правил, установленных в 7.2.1. Объекты, которые надо принять во внимание, включают напечатанные отчеты, экранные устройства отображения, записанные носители (например, ленты, диски, компакт-диски), электронные сообщения и передачи файлов.

Для каждого классификационного уровня должны быть определены процедуры обращения, включая защищенную обработку, хранение, передачу, рассекречивание и уничтожение. Сюда также следует включить процедуры последовательности заботы о сохранности информации и регистрации любого значимого события в системе защиты.

Соглашения с другими организациями, которые включают совместное использование информации, должны включать процедуры для идентификации классификации этой информации и для интерпретации классификационных этикеток других организаций.

Прочая информация

Маркировка и защищенное обращение с важной информацией является ключевым требованием для мероприятий по совместному использованию информации. Физические этикетки являются обычной формой маркировки. Тем не менее,

некоторые информационные активы, например, документы в электронной форме, не могут быть помечены физически, и должны быть использованы электронные средства маркировки. Например, уведомляющая маркировка может появляться на экране или на устройстве отображения. Если маркировка не осуществима, то можно применить другие средства определения классификации, например, посредством процедур или метаданных.

8 Защита человеческих ресурсов

8.1 Перед началом работы по найму

Цель: Обеспечить, чтобы служащие, подрядчики и пользователи третьей стороны понимали свои обязанности и подходили для ролей, на которые они рассматриваются, а также снизить риск кражи, мошенничества или неправильного использования средств.

Перед началом работы по найму следует рассмотреть обязанности по защите в соответствующих должностных инструкциях и в условиях работы по найму.

Все кандидаты в служащие, в субподрядчики и в пользователи третьей стороны должны адекватно отбираться, особенно для важных работ.

Служащие, подрядчики и сторонние пользователи средств обработки информации должны подписать соглашение об своих ролях и обязанностях в области защиты.

8.1.1 Роли и обязанности

Средство управления

Роли и обязанности служащих, подрядчиков и пользователей третьей стороны в области защиты должны быть определены и документально подтверждены в соответствии с организационной политикой в области защиты информации.

Руководство по реализации

Роли и обязанности в области защиты должны включать в себя требование делать следующее:

- a) реализовывать и действовать в соответствии с организационной политикой в области защиты (см. 5.1);
- b) защищать активы от неразрешенного доступа, раскрытия, изменения, разрушения или помех;
- c) выполнять конкретные процессы или виды деятельности в области защиты;
- d) обеспечивать, чтобы была назначена ответственность лицам за предпринятые действия;
- e) сообщать о событиях или возможных событиях в системе защиты или других рисков для защиты в организацию.

Роли и обязанности в области защиты должны быть определены и четко сообщены кандидатам на работу в ходе процесса, предшествующего приему на работу по найму.

Прочая информация

Для того чтобы документально подтвердить роли и обязанности в области защиты, могут быть использованы должностные инструкции. Роли и обязанности в области защиты для лиц, не нанятых через организационный процесс приема на работу по найму, например, нанятых через организацию третьей стороны, также должно быть четко определены и сообщены.

8.1.2 Отбор

Средство управления

В соответствии с соответствующими законами, нормами и этикой, а также соразмерно требованиям бизнеса, классификации информации, к которой будет осуществляться доступ, и воспринимаемым рискам, должны проводиться фоновые верификационные проверки по всем кандидатам в служащие, подрядчики и пользователи третьей стороны.

Руководство по реализации

Верификационные проверки должны принимать во внимание всю соответствующую уязвимость, защиту личных данных и/или законодательство по занятости, и должны, если это разрешено, включать следующее:

- a) наличие удовлетворительных рекомендаций, например, одной деловой и одной личной;
- b) проверка (на полноту и точность) биографии кандидата;
- c) подтверждение заявленной учебной и профессиональной квалификации;
- d) независимая проверка личности (паспорт или аналогичный документ);
- e) более подробные проверки, такие как проверки репутации или судимостей.

Если работа, или по первоначальному назначению, или по повышению в должности, вовлекает лицо, имеющее доступ к средствам обработки информации и, в частности, если оно обрабатывает важную информацию, например, финансовую информацию или информацию высшей категории конфиденциальности, то организация также должна рассмотреть дополнительные, более подробные проверки.

Процедуры должны определять критерии и ограничения для верификационных проверок, например, кто имеет право осуществлять отбор людей, а также как, когда и почему выполняются верификационные проверки.

Процесс отбора также должен выполняться для подрядчиков и пользователей третьей стороны. Если подрядчики предоставляются через агентство, то в договоре с агентством должны быть четко определены обязанности агентства по отбору и процедуры уведомления, которым им надлежит следовать, если отбор не был завершен или если результаты дают причину для сомнения или беспокойства. Тем

же самым образом, в соглашении с третьей стороной (см. также 6.2.3) должны быть четко определены все обязанности и процедуры уведомления для отбора.

Информация обо всех кандидатах, рассматриваемых на места в организации, должна быть собрана и обработана в соответствии с каким-либо подходящим законодательством, существующим в соответствующей юрисдикции. В зависимости от применимого законодательства, кандидаты должны быть заранее уведомлены о деятельности по отбору.

8.1.3 Условия работы по найму

Средство управления

Как часть договорного обязательства, служащие, подрядчики и пользователи третьей стороны должны согласиться и подписать условия договора личного найма, которые должны указывать обязанности, их и организации, по защите информации.

Руководство по реализации

Условия занятости должны отражать организационную политику в области защиты, в дополнение к разъяснению и утверждению следующего:

- a) что все служащие, подрядчики и пользователи третьей стороны, которым предоставлен доступ к важной информации, должны подписать соглашение о конфиденциальности или о неразглашении перед тем, как им будет предоставлен доступ к средствам обработки информации;
- b) законные обязанности и права служащих, подрядчиков и других пользователей, например, касающиеся законов об авторском праве или законов по защите данных (см. также 15.1.1 и 15.1.2);
- c) ответственность за классификацию информации и менеджмент активов организации, связанными с информационными системами и услугами, с которыми обращается служащий, подрядчик или пользователь третьей стороны (см. также 7.2.1 и 10.7.3);
- d) обязанности служащего, подрядчика или пользователя третьей стороны по обращению с информацией, полученной от других компаний или от внешних сторон;
- e) обязанности организации по обращению с личной информацией, включая личную информацию, созданную в результате или в ходе работы по найму в организации (см. также 15.1.4);
- f) обязанности, которые распространяются за пределы помещений организации, и за пределы стандартного рабочего дня, например, в случае работы на дому (см. также 9.2.5 и 11.7.1);

- g) действия, которые нужно предпринять, если служащий, подрядчик или пользователь третьей стороны игнорирует организационные требования защиты (см. также 8.2.3).

Организация должна обеспечить, чтобы все служащие, подрядчики и пользователи третьей стороны согласились с условиями, касающимися защиты информации, соответствующими характеру и объему доступа, который они будут иметь к активам организации, связанным информационными системами и услугами.

Если это необходимо, то обязанности, содержащиеся в условиях работы по найму, должны сохраняться в течение определенного периода после окончания работы по найму (см. также 8.3).

Прочая информация

Для того чтобы охватить обязанности служащих, подрядчиков или пользователей третьей стороны, касающиеся конфиденциальности, защиты данных, этики, надлежащего использования оборудования и средств организации, а также известные практики, ожидаемые организацией, можно использовать кодекс поведения. Подрядчик или пользователи третьей стороны могут быть связаны с внешней организацией, которой, в свою очередь, может потребоваться войти в договорные мероприятия от имени лица, обусловленного договором.

8.2 Во время работы по найму

Цель: Обеспечить, чтобы служащие, подрядчики и пользователи третьей стороны были осведомлены об угрозах и заботах в области защиты информации, о своих обязанностях и обязательствах и были снаряжены, с целью поддерживать организационную политику в области защиты в ходе своей обычной работы, а также снизить риск человеческой ошибки.

Должны быть определены обязанности руководства для того, чтобы обеспечить применение защиты во всей работе лиц по найму в организации.

Для того чтобы минимизировать возможные риски для защиты, всем служащим, подрядчикам и пользователям третьей стороны должны быть предоставлены адекватный уровень осведомленности, образования и подготовки по процедурам в области защиты и по правильному использованию средств обработки информации. Должен быть создан официальный дисциплинарный процесс для обращения с нарушениями в системе защиты.

8.2.1 Обязанности руководства

Средство управления

Руководство должно требовать от служащих, подрядчиков и пользователей третьей стороны применять защиту в соответствии с установленными политикой и процедурами организации.

Руководство по реализации

Обязанности руководства должны включать обеспечение того, чтобы служащие, подрядчики и пользователи третьей стороны были таковы:

- a) правильно проинструктированы по их ролям и обязанностям в области защиты перед предоставлением доступа к важной информации или информационным системам;
- b) обеспечены руководящими указаниями, с целью указать ожидания в области защиты от их роли в организации;
- c) мотивированы, чтобы выполнять политику организации в области защиты;
- d) достигли уровня осведомленности в области защиты, соответствующего их ролям и обязанностям в организации (см. также 8.2.2);
- e) соответствовали условиям работы по найму, которые включают политику организации в области защиты информации и соответствующие методы работы;
- f) продолжали обладать соответствующими навыками и квалификацией.

Прочая информация

Если служащие, подрядчики и пользователи третьей стороны не были осведомлены о своих обязанностях в области защиты, то они могут причинить значительный ущерб организации. Мотивированный персонал, скорее всего, будет более надежным и вызовет меньше инцидентов в системе защиты информации.

Плохое руководство может заставить персонал чувствовать себя недооцененным, что в результате приведет к негативному влиянию на защиту в организации. Например, плохое руководство может привести к тому, что защитой будут пренебрегать, или к возможному неправильному использованию активов организации.

8.2.2 Осведомленность, образование и подготовка в области защиты информации

Средство управления

Все служащие организации и, где уместно, подрядчики и пользователи третьей стороны должны получать подходящую подготовку по осведомленности и регулярные обновления в организационной политике и процедурах настолько, насколько это имеет отношение к их должностным функциям.

Руководство по реализации

Подготовка по осведомленности должна начинаться с официального ознакомительного процесса, предназначенного для того, чтобы познакомить с

политикой и ожиданиями организации в области защиты до того, как будет предоставлен доступ к информации или услугам.

Постоянная подготовка должна включать требования защиты, установленные законом обязанности и средства управления бизнесом, равно как и подготовку по правильному использованию средств обработки информации, например, процедуры входа в систему, использование комплектов программного обеспечения и информация по дисциплинарному процессу (см. 8.2.3).

Прочая информация

Деятельность по обеспечению осведомленности, образования и подготовки в области защиты должна быть подходящей и значимой для роли лица, его обязанностей и навыков, и должна включать информацию об известных угрозах, о том, к кому надо обращаться за дополнительной консультацией по защите, и о соответствующих каналах подачи отчетов об инцидентах в системе защиты информации (см. также 13.1).

Подготовка с целью повышения осведомленности предназначена для того, чтобы дать возможность лицам осознать проблемы и инциденты в системе защиты информации и реагировать на них в соответствии с потребностями их рабочей роли.

8.2.3 Дисциплинарный процесс

Средство управления

Должен существовать официальный дисциплинарный процессом для служащих, которые совершили нарушение защиты.

Руководство по реализации

Дисциплинарный процесс не должен начинаться без предшествующей верификации того, что нарушение защиты произошло (см. также 13.2.3 для сбора доказательств).

Официальный дисциплинарный процесс должен обеспечивать корректное и справедливое рассмотрение дел служащих, которые подозреваются в нарушении защиты. Официальный дисциплинарный процесс должен предусматривать подразделенный ответ, который учитывает такие факторы, как характер и тяжесть нарушения, а также его влияние на бизнес, является ли это нарушение первым или повторным, был ли нарушитель надлежащим образом подготовлен, соответствующие законы, договоры в сфере бизнеса и другие факторы, если требуется. В серьезных случаях должностного преступления, процесс должен предусматривать мгновенное удаление обязанностей, прав и привилегий доступа и безотлагательное увольнение с должности, если это необходимо.

Прочая информация

Дисциплинарный процесс также должен использоваться как средство сдерживания, чтобы предостерегать служащих, подрядчиков и пользователей третьей стороны от

нарушения политик и процедур организации в области защиты, а также от любых других нарушениях в области защиты.

8.3 Прекращение или перемена места работы по найму

Цель: Обеспечить, чтобы служащие, подрядчики и пользователи третьей стороны покидали организацию или меняли работу по найму в организованном порядке.

Должны быть определены обязанности для обеспечения того, что выход служащего, подрядчика или пользователя третьей стороны из организации управляем, и что возврат всего оборудования и удаление всех прав доступа завершены.

Изменение обязанностей и работ по найму в рамках организации должно управляться как прекращение соответствующей ответственности или занятости в соответствии с этим разделом, а любые новые работы по найму должны управляться, как описано в разделе 8.1.

8.3.1 Обязательства, связанные с прекращением работы по найму

Средство управления

Должны быть ясно определены и распределены обязательства по осуществлению прекращения или перемены места работы по найму.

Руководство по реализации

Информация об обязательствах по прекращению работы по найму должна включать текущие требования защиты, законные обязанности и, если это необходимо, обязательства, содержащиеся в любом соглашении о конфиденциальности (см. 6.1.5), а также условия работы по найму (см. 8.1.3), остающиеся в силе в течение определенного периода после окончания работы по найму служащего, подрядчика или пользователя третьей стороны.

Обязательства и обязанности, все еще остающиеся в силе после прекращения работы по найму, должны содержаться в договорах служащего, подрядчика или пользователя третьей стороны.

Изменения ответственности или работы по найму должны управляться как прекращение соответствующей ответственности или работы по найму, а новая ответственность или работа по найму должны управляться, как описано в разделе 8.1.

Прочая информация

Отдел кадров обычно ответственен за общий процесс прекращения работы по найму и связанные с ним дела, вместе с надзирающим менеджером уходящего лица, оставляющего, с целью управлять вопросами защиты соответствующих процедур. В случае подрядчика, этот процесс прекращения ответственности может быть

предпринят агентством, ответственным за подрядчика, а в случае другого пользователя он регулироваться его организацией.

Может оказаться необходимым уведомлять служащих, потребителей, подрядчиков или пользователей третьей стороны об изменениях в личных и рабочих договоренностях.

8.3.2 Возврат активов

Средство управления

Все служащие, подрядчики и пользователи третьей стороны должны возвратить все организационные активы, находящиеся в их владении, по окончании срока работы по найму, договора или соглашения.

Руководящие указания

Процесс прекращения должен быть формализован для того, чтобы включить возврат всего прежде выпущенного программного обеспечения, корпоративных документов и оборудования. Другие активы организации, такие как мобильные вычислительные устройства, кредитные карточки, карточки доступа, программное обеспечение, руководства и информация, хранящаяся на электронном носителе, также должны быть возвращены.

В тех случаях, когда служащий, подрядчик или пользователь третьей стороны покупают оборудование организации или использует свое собственное личное оборудование, должны выполняться процедуры для того, чтобы обеспечить, что вся важная информация передана организации и надежно стерта с оборудования (см. также 10.7.1).

В тех случаях, когда служащий, подрядчик или пользователь третьей стороны обладает знанием, которое имеет значение для текущих операций, эта информация должна быть документирована и передана организации.

8.3.3 Удаление прав доступа

Средство управления

Права доступа всех служащих, подрядчиков и пользователей третьей стороны к информации и средствам обработки информации должны быть удалены при прекращении их работы по найму, по договора или по соглашению, или же скорректированы при изменении [места работы по найму].

Руководство по реализации

По прекращении, права доступа лица к активам, связанным с информационными системами и услугами, должны быть пересмотрены. Это определит, необходимо ли удалить права доступа. Изменения места работы по найму должны быть отражены в удалении всех прав доступа, которые не были утверждены для новой работы по найму. Права доступа, которые должны быть удалены или адаптированы, включают

физический и логический доступ, ключи, удостоверения личности, средства обработки информации (см. также 11.2.4), подписи, а также удаление из любой документации, которая определяет их как существующего члена организации. Если уходящий служащий, подрядчик или пользователь третьей стороны знал пароли для активов, остающихся действующими, то эти пароли должны быть изменены при прекращении или изменении места работы по найму, договора или соглашения.

Права доступа для информационных активов и средств обработки информации должны быть уменьшены или удалены прежде, чем работа по найму прекратится или изменится, в зависимости от оценки факторов рисков, таких как следующие:

- a) инициировано ли прекращение или изменение служащим, подрядчиком или пользователем третьей стороны, или же руководством, и причина прекращения;
- b) текущие обязанности служащего, подрядчика или любого другого пользователя;
- c) ценность активов, доступных в данный момент.

Прочая информация

При определенных обстоятельствах, права доступа могут быть назначены исходя того, что они являются доступными большему количеству людей, нежели уходящий служащий, подрядчик или пользователь третьей стороны, например, групповые идентификаторы. В таких обстоятельствах, уходящие лица должны быть удалены из любых групповых списков доступа, и должны быть предприняты меры для того, чтобы рекомендовать всем остальным вовлеченным служащим, подрядчикам и пользователям третьей стороны больше не использовать эту информацию совместно с уходящим человеком.

В случаях прекращения, инициированного руководством, раздраженные служащие, подрядчики или пользователи третьей стороны могут умышленно повредить информацию или средства обработки информации. В случае лиц, уходящих в отставку, они могут соблазниться сбором информации для будущего использования.

9 Физическая и экологическая безопасность

9.1 Безопасные зоны

Цель: предотвратить неразрешенный физический доступ в помещения организации и к ее информации, ущерб и мешающие воздействия для помещений организации и для ее информации.

Средства обработки критической или важной информации должны быть расположены в безопасных зонах, защищенных определенными периметрами безопасности, с подходящими барьерами безопасности и средствами управления доступом. Они должны физически быть защищены от неразрешенного доступа, ущерба и помех.

Предоставляемая защита должна быть соразмерна выявленным рискам.

9.1.1 Физический периметр безопасности

Средство управления

Для защиты зон, которые содержат информацию и средства обработки информации, должны использоваться периметры безопасности (барьеры, такие как стены, управляемый карточками турникет на входе или управляемые персоналом столы регистрации).

Руководство по реализации

Следующие руководящие принципы должны быть рассмотрены и реализованы, если это уместно, для физических периметров безопасности:

- a) периметры безопасности должны быть четко определены, размещение и мощность каждого из периметров должны зависеть от требований к защите активов в пределах периметра и от результатов оценки риска;
- b) периметры здания или места, содержащие средства обработки информации, должны быть физически целыми (то есть не должно быть никаких брешей в периметре или зон, где могло бы легко произойти проникновение); внешние стены места должны иметь твердую конструкцию, а все внешние двери должны быть надлежащим образом защищены от неразрешенного доступа при помощи механизмов управления, например, решеток, сигнализации, замков и т.п.; двери и окна должны быть заперты, когда находятся без присмотра, и должна быть учтена внешняя защита для окон, особенно на первом этаже;
- c) должны быть созданы управляемые персоналом столы регистрации или другие средства для управления физическим доступом к месту или; доступ к местам и зданиям должен быть ограничен только полномочным персоналом;

- d) там, где это применимо, должны быть построены физические преграды, с целью предотвратить неразрешенный физический доступ и экологическое загрязнение окружающей среды;
- e) все пожароустойчивые двери в периметре безопасности должны быть оснащены сигнализацией, постоянно контролироваться и испытываться вместе со стенами для того, чтобы установить необходимый уровень сопротивления в соответствии с подходящими региональными, национальными и международными стандартами; они должны работать безаварийно в соответствии с местными нормами пожарной безопасности;
- f) в соответствии с национальными, региональными или международными стандартами должны быть установлены и должны регулярно испытываться системы обнаружения вторжения для того, чтобы охватить все внешние двери и доступные окна; незанятые зоны должны быть под сигнализацией в любое время; также должно быть предусмотрено покрытие для других областей, например, помещений с установленными в них компьютерами и помещений узлов связи;
- g) средства обработки информации, управляемые организацией, должны физически быть отделены от средств обработки информации, управляемых третьими сторонами.

Прочая информация

Физическая защита может быть достигнута путем создания одного или более физического барьера вокруг организационных зданий и средства обработки информации. Использование нескольких барьеров дает дополнительную защиту, если сбой в работе одного барьера не означает, что защита немедленно подвергнется риску.

Безопасная зона может быть запираемым офисом, или несколькими комнатами, окруженными непрерывным внутренним физическим барьером безопасности. Между зонами с различными требованиями к безопасности внутри периметра безопасности могут понадобиться дополнительные барьеры и периметры для управления физическим доступом.

Особое внимание к безопасности физического доступа должно быть уделено зданиям, где размещено несколько организаций.

9.1.2 Средства управления физическим доступом

Средство управления

Безопасные зоны должны быть защищены подходящими средствами управления доступом для того, чтобы обеспечить, что доступ разрешен только полномочному персоналу.

Руководство по реализации

Должны быть рассмотрены следующие руководящие указания:

- a) дата и время входа и выхода посетителей должны записываться, а все посетители должны находиться под надзором, если их доступ раньше не утверждался; им должен предоставляться доступ только для конкретных, разрешенных целей, они должны выпускаться с инструкциями по требованиям безопасности зоны и по чрезвычайным процедурам.
- b) доступ к зонам, где обрабатывается или хранится важная информация, должен управляться и быть ограничен только полномочными лицами; средства управления аутентификацией, например, карточка управления доступом плюс персональный идентификационный номер [PIN], должны использоваться, чтобы разрешать и подтверждать любой доступ; контрольный журнал всего доступа должен содержаться в надежном месте;
- c) от всех служащих, подрядчиков и пользователей третьей стороны и от всех посетителей надо требовать носить некоторую форму видимого идентификационного документа, и они должны немедленно сообщать персоналу службы безопасности, если они сталкиваются с посетителями без сопровождающего и с кем-либо, кто не носит видимого идентификационного документа;
- d) персоналу вспомогательных служб третьей стороны должен быть предоставлен ограниченный доступ в зоны безопасности или к средствам обработки важной информации только тогда, когда требуется; этот доступ должен быть разрешен и должен постоянно контролироваться;
- e) права доступа в зоны безопасности должны регулярно анализироваться и обновляться, и отменяться, если необходимо (см. 8.3.3).

9.1.3 Защита офисов, комнат и средств

Средство управления

Должна быть разработана и должна применяться физическая защита офисов, комнат и средств.

Для того чтобы защитить офисы, комнаты и средства, должны быть рассмотрены следующие руководящие указания:

- a) должны быть учены соответствующие нормы и стандарты по технике безопасности и охране труда;
- b) ключевые средства должны быть расположены так, чтобы избежать доступа к ним широкой публики;

- c) там, где это применимо, здания должны быть скромными и должны давать минимальное указание на их цель, без ярких надписей, снаружи здания или внутри него, указывающих на наличие видов деятельности по обработке информации;
- d) указатели и внутренние телефонные книги, указывающие на местоположения средств обработки важной информации, не должны быть легко доступны широкой публике.

9.1.4 Защита от внешних и экологических угроз

Средство управления

Должна быть разработана и должна применяться физическая защита против ущерба от огня, наводнения, землетрясения, взрыва, общественных беспорядков и других форм естественного или искусственного бедствия.

Руководство по реализации

Внимание должно быть уделено любым угрозам нарушения безопасности, которые представляют соседние помещения, например, огонь в соседнем помещении, протечка воды с крыши или в перекрытиях ниже уровня земли, или взрыв на улице.

Следующие руководящие указания должны быть рассмотрены для того, чтобы избежать ущерба от огня, наводнения, землетрясения, взрыва, общественных беспорядков и других форм естественного или искусственного бедствия:

- a) опасные или горючие материалы должны храниться на безопасном расстоянии от безопасной зоны. Несортированная продукция, такая как канцтовары, не должна храниться в безопасной зоне;
- b) Резервное оборудование и резервные копии должны быть расположены на безопасном расстоянии для того, чтобы избежать ущерба от бедствия, влияющего на основное местоположение;
- c) должно быть предусмотрено и подходящим образом размещено противопожарное оборудование.

9.1.5 Работа в безопасных зонах

Средство управления

Должны быть разработаны и применяются физическая защита и руководящие указания для работы в безопасных зонах.

Руководство по реализации

Должны быть рассмотрены следующие руководящие указания:

- a) персонал должен быть осведомлен о существовании безопасной зоны или о деятельности в безопасной зоне только на основе принципа служебной необходимости;
- b) надо избегать безнадзорной работы в безопасных зонах, как по причинам безопасности, так и для того, чтобы предотвратить возможности для злонамеренной деятельности;
- c) пустые безопасные зоны должны физически запираться и периодически проверяться;
- d) фотографическое, видео, аудио или другое записывающее оборудование, такое как камеры на мобильных устройствах, не должны допускаться, если только не разрешено;

Организация работы в безопасных зонах включает средства управления для служащих, подрядчиков и пользователей третьей стороны, работающих в безопасной зоне, а также другую деятельность третьей стороны, происходящую там.

9.1.6 Зоны открытого доступа, поставки и погрузки

Средство управления

Места доступа, такие как зоны поставки и погрузки, а также другие места, где посторонние лица могут проникнуть в помещения, должны управляться и, если возможно, должны быть изолированы от средств обработки информации, чтобы избежать неразрешенного доступа.

Руководство по реализации

Должны быть рассмотрены следующие руководящие указания:

- a) доступ к зонам поставки и погрузки снаружи здания должен ограничиваться определенным и полномочным персоналом;
- b) зоны поставки и погрузки должны быть спроектированы так, чтобы поставки могли быть разгружены без предоставления персоналу, осуществляющему поставку, доступа к другим частям здания;
- c) внешние двери зоны поставки и погрузки должны охраняться, когда открыты внутренние двери;
- d) поступающий материал должен быть проверен на возможные угрозы (см. 9.2.1d)) прежде, чем этот материал будет перемещен из зоны поставки и погрузки в место использования;

- e) поступающий материал должен быть зарегистрирован в соответствии с процедурами управления активами (см. также 7.1.1) на входе на место расположения;
- f) поступающие и исходящие грузы должны быть физически отделены, если это возможно.

9.2 Защита оборудования

Цель: Предотвратить потерю, ущерб, кражу или раскрытие активов и прерывание в деятельности организации.

Оборудование должно быть защищено от физических и экологических угроз.

Защита оборудования (включая, оборудование, используемое вне рабочего места, и вынос имущества), необходима для того, чтобы снизить риск неразрешенного доступа к информации и защититься от потери или ущерба. Защита также должна учитывать размещение и расположение оборудования. Особые средства управления могут потребоваться для защиты от физических угроз, а также для охраны вспомогательных средств, таких как электроснабжение и кабельная инфраструктура.

9.2.1 Расположение и защита оборудования

Средство управления

Оборудование должно быть расположено или защищено так, чтобы снизить риски возникновения экологических угроз и опасностей, а также количество возможностей для неразрешенного доступа.

Руководство по реализации

Для того чтобы защитить оборудование, должны быть рассмотрены следующие руководящие указания:

- a) оборудование должно быть расположено так, чтобы минимизировать необязательный доступ в рабочие зоны;
- b) средства обработки информации, обращающиеся с важными данными, должны располагаться так и иметь такой угол видимости, чтобы снизить риск того, что информацию увидят посторонние лица в ходе их использования, а средства хранения должны охраняться для того, чтобы избежать неразрешенного доступа;
- c) элементы, требующие особой защиты, должны быть изолированы для того, чтобы снизить общий уровень необходимой защиты;

- d) должны быть созданы средства управления для того, чтобы минимизировать риск возможных физических угроз, например, кража, пожар, взрывоопасные вещества, дым, вода (или сбой в подаче воды), пыль, вибрации, химические воздействия, помехи электроснабжению, помехи связи, электромагнитное излучение и вандализм;
- e) должны быть определены руководящие указания по употреблению пищи, напитков и курению вблизи средств обработки информации;
- f) внешние условия, такие как температура и влажность, должны постоянно контролироваться на наличие условий, которые могли бы негативно повлиять на работу средств обработки информации;
- g) защита от молний должна быть применена ко всем зданиям, и молниезащитные фильтры должны быть установлены на все входящие линии электропередач и линии связи;
- h) для оборудования в промышленной среде должна быть рассмотрена возможность использования специальных методов защиты, таких как клавиатурные мембранны;
- i) оборудование, обрабатывающее важную информацию, должно быть защищено для того, чтобы минимизировать риски утечки информации по каналам побочных излучений.

9.2.2 Вспомогательные коммунальные службы

Средство управления

Оборудование должно быть защищено от отказов в системе электроснабжения и других нарушений, вызывались сбоями в работе коммунальных служб.

Руководство по реализации

Все вспомогательные коммунальные службы, такие как электроснабжение, водоснабжение, канализация, отопление/вентиляция и кондиционирование воздуха должны быть адекватны системам, которые они поддерживают. Вспомогательные коммунальные службы должны регулярно контролироваться и, по обстановке, испытываться, с целью обеспечить их правильную работу и снизить любой риск от их неправильного функционирования или сбоя в их работе. Должно быть обеспечено подходящее электроснабжение, которое соответствует спецификации оборудования, предоставленной изготовителем.

Для оборудования, поддерживающего критические деловые операции, рекомендуется использовать источники бесперебойного питания (ИБП) для того, чтобы поддерживать нормальное завершение работы или непрерывную работу. Планы действий на случай аварий в системе электроснабжения должны учитывать действие, которое предстоит предпринять в случае сбоя в работе ИБП. Должна быть рассмотрена возможность использования резервного генератора, если требуется продолжать обработку в случае длительного перерыва в подаче электроэнергии.

Должна быть доступна надлежащая поставка топлива для того, чтобы генератор мог работать длительный период. Оборудование ИБП и генераторы должны регулярно проверяться для того, чтобы гарантировать, что они обладают требуемой мощностью, и испытываться в соответствии с рекомендациями изготовителя. Кроме того, надо рассмотреть возможность использования нескольких источников питания или, если помещение большое, то отдельной электроподстанции.

Переключатели аварийного отключения питания должны быть расположены около запасных выходов в комнатах с оборудованием для того, чтобы облегчить быстрое отключение электропитания в случае аварийной ситуации. На случай сбоя в работе основной сети электропитания должно быть предусмотрено аварийное освещение.

Водоснабжение должно быть стабильным и адекватным, чтобы снабжать системы кондиционирования воздуха, увлажняющее оборудование и системы пожаротушения (там, где используются). Неправильная работа системы водоснабжения может повредить оборудование или помешать результативной работе системы пожаротушения. Если требуется, то должна быть оценена и установлена система оповещения для того, чтобы обнаруживать сбои во вспомогательных коммунальных службах.

Телекоммуникационное оборудование должно быть подключено к поставщику коммунальных услуг, по крайней мере, двумя разными маршрутами, чтобы помешать сбою в работе одного пути соединения прекратить предоставление услуг голосовой связи. Услуги голосовой связи должны быть адекватными для того, чтобы соответствовать местным требованиям закона о связи в чрезвычайных ситуациях.

Прочая информация

Возможности достижения непрерывности электроснабжения включают распределенное питание для того, чтобы избежать одной критической точки в электроснабжении.

9.2.3 Защита кабельных соединений

Средство управления

Силовые кабели и кабели дальней связи, по которым передаются данные или вспомогательные информационные услуги, должны быть защищены от перехвата или повреждения.

Руководство по реализации

Для обеспечения безопасности кабельных соединений должны быть рассмотрены следующие руководящие указания:

- a) силовые линии и линии дальней связи, входящие в средства обработки информации, должны быть подземными там, где это возможно, или должны подлежать адекватной альтернативной защите;

- b) сетевые кабели должны быть защищены от неразрешенного перехвата или повреждения, например, путем использования кабельного канала или избегания маршрутов, пролегающих через общедоступные зоны;
- c) силовые кабели должен быть отделены от кабелей дальней связи для того, чтобы предотвратить помехи;
- d) легко различимые маркировки кабелей и оборудования должны использоваться для того, чтобы минимизировать ошибки из-за неправильного обращения, такие как случайная коммутация неправильных сетевых кабелей;
- e) для того, чтобы снизить возможность ошибок, должен использоваться документированный список коммутаций;
- f) для важных или критических систем, дополнительные средства управления, которые надо рассмотреть, включают в себя следующее:
 - 1) установка бронированного кабельного канала и запертых комнат или блоков в контрольных точках и точках прерывания;
 - 2) использование альтернативных маршрутизаций и/или средств передачи данных, обеспечивающих подходящую защиту;
 - 3) использование оптоволоконного кабеля;
 - 4) использование электромагнитного экранирования для защиты кабеля;
 - 5) инициация технических зачисток⁵ и физического контроля на предмет наличия неразрешенных устройств, присоединенных к кабелю;
 - 6) контролируемый доступ к коммутационным панелям и кабельным комнатам;

9.2.4 Обслуживание оборудования

Средство управления

Оборудование должно правильно обслуживаться для обеспечения непрерывной доступности и целостности.

Руководство по реализации

Для обслуживания оборудования должны быть рассмотрены следующие руководящие указания:

- a) оборудование должно обслуживаться в соответствии с рекомендуемыми поставщиком периодичностью и спецификациями технического обслуживания;

⁵ «зачистка» [sweep] – обследование помещений и объектов с целью обнаружения скрыто установленных устройств негласного съема информации (Прим. переводчика)

- b) только полномочный обслуживающий персонал должен выполнять ремонт и обслуживать оборудование;
- c) должны храниться записи обо всех предполагаемых или фактических дефектах, а также обо всем предупреждающем и корректирующем обслуживании;
- d) если оборудование включено в график обслуживания, то должны быть реализованы подходящие средства управления, учитывающие, выполняется ли это обслуживание местным персоналом или персоналом, внешним по отношению к организации; если это необходимо, то оборудование должно быть очищено от важной информации, или обслуживающий персонал должен иметь достаточный допуск к конфиденциальной работе;
- e) все требования, наложенные страховыми полисами, должны быть выполнены.

9.2.5 Защита оборудования, находящегося за пределами рабочего места

Средство управления

Защита должна применяться для оборудования, находящегося за пределами рабочего места, с учетом различных рисков работы за пределами организационных помещений.

Руководство по реализации

Независимо от собственности, использование любых средств обработки информации за пределами организационных помещений должно быть разрешено руководством.

Для защиты оборудования, находящегося за пределами рабочего места, должны быть рассмотрены следующие руководящие указания:

- a) оборудование и носители информации, выносимые из помещений, не должны оставляться без присмотра в общедоступных местах; портативные компьютеры при путешествии должны перевозиться в качестве ручной клади и должны быть замаскированы, если возможно;
- b) все время должны соблюдаться инструкции изготовителя для защиты оборудования, например, защита от сильных электромагнитных полей;
- c) средства управления домашней работой должны быть определены оценкой риска, и подходящие средства управления должны быть применены, по остановке, например, запирающийся картотечный блок, политика чистого стола, средства управления доступом для компьютеров и безопасная связь с офисом (см. также ISO/IEC 18028. Защита сети);
- d) для защиты оборудования, находящегося за пределами рабочего места, должен быть принят адекватный объем страховой ответственности.

Риски нарушения системы безопасности, например, риск ущерба, кражи или подслушивания, могут значительно различаться в зависимости от местоположения и должны быть учтены при определении наиболее подходящих средств управления.

Прочая информация

Оборудование, используемое для хранения и обработки информации, включает все формы персональных компьютеров, организеров, мобильных телефонов, смарт-карт, бумаг или другую форму, которая держится для домашней работы или уносится с места обычной работы.

Дополнительную информацию о других аспектах защиты мобильного оборудования можно найти в 11.7.1.

9.2.6 Безопасная ликвидация или повторное использование оборудования

Средство управления

Все элементы оборудования, содержащие носители информации, должны быть проверены для обеспечения того, что любые важные данные и лицензионное программное обеспечение были удалены или надежно затерты перед ликвидацией.

Руководство по реализации

Устройства, содержащие конфиденциальную информацию, должны быть физически уничтожены, или информация должна быть уничтожена, удалена или затерта, используя [соответствующие] методы с целью сделать оригинальную информацию невосстановимой, вместо того, чтобы использовать стандартную функцию удаления или форматирования.

Прочая информация

Поврежденные устройства, содержащие важные данные, могут потребовать оценки рисков для того, чтобы определить, должны ли элементы быть уничтожены физически, отправлены для ремонта или забракованы.

Информация может быть разглашена посредством небрежной ликвидации или повторного использования оборудования (см. также 10.7.2).

9.2.7 Вынос имущества

Средство управления

Оборудование, информация или программное обеспечение не должны выноситься за пределы рабочего места без предварительного разрешения.

Руководство по реализации

Должны быть рассмотрены следующие руководящие указания:

- a) оборудование, информация или программное обеспечение не должны выноситься за пределы рабочего места без предварительного разрешения;
- b) служащие, подрядчики и пользователи третьей стороны, которые имеют полномочие разрешать вынос активов за пределы рабочего места, должны быть четко определены;
- c) должны быть установлены ограничения на время выноса оборудования, и возвраты должны быть проверены на соответствие;
- d) если это необходимо и уместно, то оборудование должно быть записано как вынесенное с рабочего места и записано по возвращении.

Прочая информация

Внезапные проверки, предпринимаемые с целью обнаружить неразрешенный вынос имущества, также могут проводиться для того, чтобы обнаружить неразрешенные записывающие устройства, оружие и т.п., и предотвратить их внос на рабочее место. Такие внезапные проверки должны выполняться согласно соответствующим законам и нормам. Люди должны быть осведомлены о том, проводятся ли внезапные проверки, и проверки должны выполняться только с разрешением, соответствующим требованиям закона и юридическим требованиям.

10 Менеджмент средств связи и операций

10.1 Процедуры эксплуатации и рабочие обязанности

Цель: Обеспечить правильную и безопасную работу средств обработки информации.

Должны быть установлены обязанности и процедуры для менеджмента и работы всех средств обработки информации. Это включает в себя разработку подходящих процедур эксплуатации.

Там, где это уместно, должно быть реализовано разделение обязанностей, с целью снизить риск нечаянного или намеренного неправильного использования системы.

10.1.1 Документированные процедуры эксплуатации

Средство управления

Процедуры эксплуатации должны быть документированы, должны поддерживаться в рабочем состоянии и должны быть сделаны доступными для всех пользователей, которым они нужны.

Руководство по реализации

Должны быть подготовлены документированные процедуры для видов системной деятельности, связанной со средствами обработки информации и средствами обмена информацией, такими как процедуры запуска и прекращения работы компьютера, резервное копирование, обслуживание оборудования, обращение с носителями информации, менеджмент компьютерной комнаты и обработки корреспонденции, а также безопасность.

Процедуры эксплуатации должны определять инструкции по подробному исполнению каждой работы, включая следующее:

- a) обработка информации и обращение с информацией;
- b) резервное копирование (см. 10.5);
- c) планирование требований, включая взаимозависимости с другими системами, время начала самой ранней работы и время завершения самой поздней работы;
- d) инструкции по обращению с ошибками или другими исключительными условиями, которые могут возникнуть в ходе выполнения работы, включая ограничения на использование системных утилит (см. 11.5.4);
- e) служебные контакты на случай неожиданных эксплуатационных или технических трудностей;

- f) специальные инструкции по выводу информации и по обращению с носителями информации, например, использование специальных канцтоваров или управление выводом конфиденциальной информации, включая процедуры безопасной ликвидации вывода информации неудавшихся работ (см. 10.7.2 и 10.7.3);
- g) повторный пуск системы и процедуры восстановления для использования в случае сбоя в работе системы;
- h) менеджмент информации контрольного и системного журналов (см. 10.10).

С процедурами эксплуатации, а также с документированными процедурами для видов системной деятельности надо обращаться как с официальными документами, и изменения должны санкционироваться руководством. Там, где это технически выполнимо, информационные системы должны управляться последовательно, используя одни и те же процедуры, инструментальные средства и утилиты.

10.1.2 Менеджмент изменений

Средство управления

Изменения в средствах обработки информации и системах должны управляться.

Руководство по реализации

Операционные системы и прикладное программное обеспечение должны быть предметом строгого контроля менеджмента изменений.

В частности, должны быть рассмотрены следующие пункты:

- a) определение и запись значительных изменений;
- b) планирование и испытание изменений;
- c) оценка возможного влияния таких изменений, включая влияние на систему безопасности;
- d) официальная процедура утверждения предлагаемых изменений;
- e) сообщение подробностей изменений всем лицам, имеющим отношение к делу;
- f) процедуры нейтрализации неисправности, включая процедуры и обязанности по прерыванию и восстановлению после неудачных изменений и непредвиденных событий.

Должны быть приняты официальные обязанности руководства и процедуры для обеспечения удовлетворительного контроля всех изменений в оборудовании, программном обеспечении или процедурах. Если делаются изменения, то должен сохраняться контрольный журнал, содержащий всю значимую информацию.

Прочая информация

Неадекватное управление изменениями в средствах обработки информации и системах является общей причиной сбоев системы или защиты. Изменения в операционной среде, особенно при передаче системы со стадии разработки на стадию эксплуатации, могут повлиять на надежность приложений (см. также 12.5.1).

Изменения в операционных системах должны производиться только тогда, когда есть веская деловая причина это сделать, такая как увеличение риска для системы. Обновление систем самыми последними версиями операционной системы или приложений – не всегда в интересах бизнеса, поскольку это может привнести больше уязвимости и нестабильности, чем текущая версия. Также может иметься потребность в дополнительной подготовке, затратах на лицензии, поддержке, обслуживании и административных накладных расходах, а также в новых аппаратных средствах, особенно во время миграции.

10.1.3 Разделение обязанностей

Средство управления

Обязанности и зоны ответственности должны быть отделены для того, чтобы уменьшить возможность неразрешенной или непреднамеренной модификации или неправильного использования активов организации.

Руководство по реализации

Разделение обязанностей является методом для уменьшения рисков случайного или преднамеренного неправильного использования системы. Надо позаботиться о том, чтобы ни один человек не мог иметь доступ к активам, модифицировать активы или использовать активы без разрешения или обнаружения. Инициация события должна быть отделена из разрешения на него. При проектировании средств управления должна быть рассмотрена возможность сговора.

Для небольших организаций разделение обязанностей может показаться труднодостижимым, но принцип должен быть применен настолько, насколько это возможно и практически осуществимо. Всякий раз, когда трудно осуществить разделение, должны рассматриваться другие средства управления, такие как постоянный контроль деятельности, контрольные журналы и надзор руководства. Важно, чтобы контроль системы безопасности оставался независимым.

10.1.4 Разделение средств разработки, испытания и эксплуатации

Средство управления

Средства разработки, испытания и эксплуатации должны быть разделены для того, чтобы снизить риски неразрешенного доступа к операционной системе или изменений в ней.

Руководство по реализации

Должен быть определен уровень разделения между эксплуатационными средами, испытательными средами и средами разработки, который необходим для предотвращения эксплуатационных проблем, и должны быть реализованы соответствующие средства управления.

Должны быть рассмотрены следующие пункты:

- a) правила перевода программного обеспечения из статуса разработки в статус системного должны быть определены и документально подтверждены;
- b) инструментальное и системное программное обеспечение должны работать в разных системах или на разных компьютерных процессорах и в разных доменах или директориях;
- c) компиляторы, редакторы и другие инструментальные средства разработки или системные утилиты не должны быть доступны из операционных систем, если они не требуются;
- d) среда испытательной системы должна эмулировать среду операционной системы настолько близко, насколько это возможно;
- e) пользователи должны использовать разные учетные записи пользователей для операционных и испытательных систем, а в меню должны отображаться подходящие идентификационные сообщения, чтобы снизить риски ошибки;
- f) важные данные не должны копироваться в испытательную среду системы (см. 12.4.2).

Прочая информация

Деятельность по разработке и испытаниям может вызвать серьезные проблемы, например, нежелательную модификацию файлов или системной среды, или системный сбой. В этом случае, есть необходимость поддерживать в рабочем состоянии известную и стабильную среду для выполнения значащих испытаний и для предотвращения ненадлежащего доступа разработчика.

Если персонал, принимающий участие в разработке и испытаниях, имеет доступ к операционной системе и ее информации, то он может ввести неразрешенный и неиспытанный код или изменить эксплуатационные данные. В некоторых системах, этой возможностью можно злоупотребить для совершения мошенничества или введения неиспытанного или злонамеренного кода, который может вызвать серьезные эксплуатационные проблемы.

Разработчики и испытатели также представляют угрозу конфиденциальности эксплуатационной информации. Виды деятельности по разработке и испытанию могут вызвать неумышленные изменения программного обеспечения или информации, если они используют одну и ту же вычислительную среду. Следовательно, разделение средства разработки, испытания и эксплуатации,

желательно для того, чтобы снизить риск случайного изменения системного программного обеспечения и деловой информации или неразрешенного доступа к ним (см. также 12.4.2 для защиты данных испытания).

10.2 Менеджмент предоставления услуг третьей стороны

Цель: Реализовать и поддерживать надлежащей уровень защиты информации и обслуживания в соответствии с соглашениями о предоставлении услуг третьей стороны.

Организация должна проверять реализацию соглашений, постоянно контролировать соответствие соглашениям и управлять изменениями для того, чтобы обеспечить, что предоставленные услуги соответствуют всем требованиям, согласованным с третьей стороной.

10.2.1 Предоставление услуг

Средство управления

Должно быть гарантировано, что средства управления защитой, определения услуг и уровни обслуживания, включенные в соглашение о предоставлении услуги третьей стороны, реализованы, эксплуатируются и поддерживаются третьей стороной.

Руководство по реализации

Предоставление услуг третьей стороной должно включать согласованные мероприятия по обеспечению безопасности, определения услуг и вопросы менеджмента услуг. В случае аутсорсинга мероприятий, организация должна спланировать необходимые перемещения (информации, средств обработки информации и чего-либо еще, что должно быть перемещено) и должна обеспечить поддержание защиты в рабочем состоянии в течение всего периода перемещения.

Организация должна гарантировать, что третья сторона поддерживает достаточную работоспособность вместе с выполнимыми планами, предназначенными для обеспечения того, чтобы согласованные уровни непрерывности поддерживались после серьезных перебоев в обслуживании или бедствий (см. 14.1).

10.2.2 Постоянный контроль и анализ услуг третьей стороны

Средство управления

Услуги, отчеты и записи, предоставленные третьей стороной, должны постоянно контролироваться и регулярно анализироваться, а аудиты должны проводиться регулярно.

Руководство по реализации

Постоянный контроль и анализ услуг третьей стороны должны обеспечивать соблюдение условий соглашения по защите информации и правильный менеджмент

инцидентов и проблем в системе защиты информации. Это должно включать взаимоотношение менеджмента услуг и процесс между организацией и третьей стороной для того, чтобы:

- a) постоянно контролировать уровни обслуживания, с целью проверять соблюдение соглашений;
- b) анализировать отчеты об услугах, созданные третьей стороной, и проводить регулярные совещания по вопросу хода работ, как требуется соглашениями;
- c) обеспечивать информацию об инцидентах в системе защиты информации и анализ этой информации третьей стороной и организацией, как требуется соглашениями и любыми дополнительными руководящими указаниями и процедурами;
- d) анализировать контрольные журналы и записи третьей стороны о событиях в системе защиты информации, эксплуатационных проблемах, сбоях, прослеживании неисправностей и поломок, связанных с предоставляемой услугой;
- e) разрешать любые выявленные проблемы и управлять ими.

Ответственность за менеджмент взаимоотношений с третьей стороной должна быть назначена определенному лицу или группе по менеджменту услуг. Кроме того, организация должна обеспечивать, чтобы третья сторона назначала обязанности по осуществлению проверки соответствия и соблюдению требований соглашений. Достаточные технические навыки и ресурсы должны быть сделаны доступными для того, чтобы постоянно контролировать выполнение этих требований соглашения (см. 6.2.3), в частности, требований защиты информации. При обнаружении недостатков в обслуживании должно быть предпринято подходящее действие.

Организация должна поддерживать достаточную степень полного контроля и наблюдения во всех аспектах защиты для важной или критической информации или средств обработки информации, доступных третьей стороне, обрабатываемых или управляемых третьей стороной. Организация должна обеспечивать сохранение своего наблюдения видов деятельности по защите, например, управление изменениями, выявление слабых мест, предоставление отчетов об инцидентах/откликах на инциденты в системе защиты информации посредством четко определенного процесса, формата и структуры предоставления отчетов.

Прочая информация

В случае аутсорсинга, организации необходимо быть осведомленной о том, что окончательная ответственность за информацию, обрабатываемую привлеченной стороной, остается на организации.

10.2.3 Менеджмент изменений в услугах третьей стороны

Средство управления

Изменения в предоставлении услуг, включая поддержание и улучшение существующей политики, процедур и средств управления в области защиты информации, должны управляться, учитывая критичность вовлеченных деловых систем и процессов и переоценку рисков.

Руководство по реализации

Процесс менеджмента изменений в услугах третьей стороны должен учитывать следующее:

- a) изменения, сделанные организацией для реализации следующего:
 - 1) совершенствование текущих предлагаемых услуг;
 - 2) разработка каких-либо новых приложений и систем;
 - 3) модификация или обновление политики и процедур организации;
 - 4) новые средства управления для разрешения инцидентов в системе защиты информации и улучшения защиты;
- b) изменения в услугах третьей стороны для реализации следующего:
 - 1) изменения и совершенствования сетей;
 - 2) использование новых технологий;
 - 3) принятие новых продуктов или более новых версий/выпусков;
 - 4) новые инструментальные средства и среды разработки;
 - 5) изменения в физическом местоположении средств обслуживания;
 - 6) изменение организаций-поставщиков.

10.3 Планирование реализации и приемка системы

Цель: Минимизировать риск системных сбоев.

Долгосрочное планирование и подготовка требуются для того, чтобы обеспечить доступность требуемой производительности и ресурсов для предоставления необходимых показателей работы системы.

Прогнозы будущих требований к производительности должны быть сделаны для того, чтобы снизить риски перегрузки системы.

Эксплуатационные требования новых систем должны быть установлены, документально подтверждены и испытаны до их принятия и использования.

10.3.1 Менеджмент производительности

Средство управления

Использование ресурсов должно постоянно контролироваться, настраиваться, и должны делаться прогнозы будущих требований к производительности, с целью обеспечить необходимые показатели работы системы.

Руководство по реализации

Для каждой новой и продолжающейся деятельности должны быть определены требования к производительности. Настройка и постоянный контроль системы должны применяться для обеспечения и, если это необходимо, для улучшения доступности и эффективности систем. Должны быть введены в действие средства обнаружения для того, чтобы указывать на проблемы своевременно. Прогнозы будущих требований к производительности должны учитывать новые деловые и системные требования, а также текущие и прогнозируемые тенденции в способностях организации по обработке информации.

Особое внимание необходимо уделить любым ресурсам, приобретение которых требует длительного времени или больших затрат; следовательно менеджеры должны постоянно контролировать использование ключевых системных ресурсов. Они должны выявлять тенденции в использовании, особенно в том, что касается деловых приложений или инструментальных средств информационной системы менеджмента.

Менеджеры должны использовать эту информацию для того, чтобы выявлять и избегать возможных узких мест и зависимости от ключевого персонала, которые могут представлять угрозу системной защиты или услугам, и должны планировать подходящее действие.

10.3.2 Приемка системы

Средство управления

Должны быть определены критерии приемки новых информационных систем, модернизированных версий и новых версий, и должны быть выполнены подходящие испытания системы (систем) в ходе разработки и до приемки.

Руководство по реализации

Менеджеры должны обеспечивать, чтобы требования и критерии для приемки новых систем были четко определены, согласованы, документально подтверждены и испытаны. Новые информационные системы, модернизации и новые версии должны перемещаться в производство после только после получения официальной приемки. Перед тем, как будет выполнена официальная приемка, должны быть рассмотрены следующие пункты:

- a) требования к функционированию и требования к производительности компьютера;
- b) процедуры восстановления и повторного пуска после ошибок, а также чрезвычайные планы;
- c) подготовка и проведение испытаний рутинных процедур эксплуатации на соответствие определенным стандартам;
- d) согласованный набор средств управления защитой на месте;
- e) результативные ручные процедуры;
- f) мероприятия по обеспечению непрерывности бизнеса (см. 14.1);
- g) доказательство того, что установка новой системы не окажет негативного влияния на существующие системы, в особенности, во время наиболее интенсивной обработки, например, в конце месяца;
- h) доказательство того, что было рассмотрено влияние новой системы на общую защиту организации;
- i) подготовка в работе или использовании новых систем;
- j) удобство использования, поскольку это влияет на работу пользователя и предотвращает человеческую ошибку.

Для серьезных новых разработок, на всех стадиях процесса разработки должны производиться консультации с производственным отделом и пользователями для обеспечения эксплуатационной эффективности предлагаемого проектного решения для системы. Должны быть выполнены надлежащие испытания для того, чтобы подтвердить, что все критерии приемки были полностью выполнены.

Прочая информация

Приемка может включать в себя процесс официальной сертификации и аккредитации для того, чтобы верифицировать, что требования защиты были учтены правильно.

10.4 Защита от злонамеренного и мобильного кода

Цели: Защитить целостность программного обеспечения и информации.

Для того чтобы предотвратить и обнаружить введение злонамеренного кода и неразрешенного мобильного кода, требуются меры предосторожности.

Программное обеспечение и средства обработки информации уязвимы по отношению к введению злонамеренного кода, такого как компьютерные вирусы, сетевые черви, троянские кони и логические бомбы. Пользователи должны быть осведомлены об опасностях злонамеренного кода. Менеджеры должны, если это уместно, вводить средства управления для того, чтобы предотвращать, обнаруживать и удалять злонамеренный код и управлять мобильным кодом.

10.4.1 Средства управления против злонамеренного кода

Средство управления

Должны быть реализованы средства управления обнаружением, предотвращением и восстановлением для защиты против злонамеренного кода, а также процедуры ознакомления соответствующих пользователей.

Руководство по реализации

Защита против злонамеренного кода должна быть основана на программах обнаружения и удаления злонамеренного кода, осведомленности в области защиты, а также на надлежащих средствах управления доступом к системе и менеджментом изменений. Должны быть рассмотрены следующее руководящие указания:

- a) создание официальной политики, запрещающей использование неразрешенного программного обеспечения (см. 15.1.2);
- b) создание официальной политики для защиты от рисков, связанных с получением файлов и программного обеспечения из внешних сетей или через них, или же на любом другом носителе; указывающей, что какие защитные меры должны быть предприняты;
- c) проведение регулярного анализа программного обеспечения и содержания данных систем, поддерживающих критические деловые процессы; присутствие любых неутверждённых файлов или неразрешенных изменений должно быть официально расследовано;
- d) установка и регулярное обновление программы обнаружения и удаления злонамеренного кода для сканирования компьютеров и носителей информации как предупредительное средство, или в рабочем порядке; выполняемые проверки должны включать в себя следующее:
 - 1) проверка любых файлов на электронном или оптическом носителе, а также файлов, полученных по сетям, на наличие злонамеренного кода перед использованием;

- 2) проверка приложений к электронным письмам и загрузок на наличие злонамеренного кода перед использованием; эта проверка должна выполняться в разных местах, например, на серверах электронной почты, в персональных компьютерах и при поступлении в сеть организации;
 - 3) проверка web-страниц на наличие злонамеренного кода;
- e) определение управляющих процедур и обязанностей для работы с защитой систем от злонамеренного кода, подготовки по их использованию, предоставления отчетов и восстановления после атаки злонамеренного кода (см. 13.1 и 13.2);
 - f) подготовка подходящих планов обеспечения непрерывности бизнеса для восстановления после атаки злонамеренного кода, включая все необходимые резервные копии данных и программного обеспечения, а также мероприятия по восстановлению (см. раздел 14);
 - g) реализация процедур для регулярного сбора информации, например, подписка на почтовую рассылку и/или проверка web-сайтов, дающих информацию о новом злонамеренном коде;
 - h) реализация процедур с целью верифицировать информацию, связанную со злонамеренным кодом, и обеспечить точность и информативность предупреждающих бюллетеней; менеджеры должны обеспечивать использование компетентных источников, например, солидных журналов, надежных web-сайтов или поставщиков, производящих программы для защиты от злонамеренного кода, для того, чтобы делать различие между фантомами и реальным злонамеренным кодом; все пользователи должны быть осведомлены о проблеме фантомов и о том, что надо делать при их получении.

Прочая информация

Использование двух или более программных продуктов от разных поставщиков, защищающееся против злонамеренного кода по всей среде обработки информации, может улучшить результативность защиты от злонамеренного кода.

Программное обеспечение для защиты от злонамеренного кода может быть установлено так, чтобы обеспечивать автоматические обновления файлов определения и механизмов сканирования для обеспечения актуальности защиты. Кроме того, это программное обеспечение может быть установлено на каждом настольном компьютере для выполнения автоматических проверок.

Следует позаботиться о защите от введения злонамеренного кода в ходе процедур технического обслуживания и чрезвычайных процедур, которые могут обойти обычные средства управления защитой от злонамеренного кода.

10.4.2 Средства управления против мобильного кода

Средство управления

Если использование мобильного кода разрешено, то конфигурация должна обеспечивать, чтобы разрешенный мобильный код действовал согласно четко определенной политике в области защиты, а использование неразрешенного мобильного кода должно предотвращаться.

Руководство по реализации

Для защиты от мобильного кода, выполняющего неразрешенные действия, должны быть рассмотрены следующие действия:

- a) выполнение мобильного кода в логически изолированной среде;
- b) блокирование любого использования мобильного кода;
- c) блокирование получения мобильного кода;
- d) активизация технических мер, в зависимости от доступности для конкретной системы, для обеспечения того, чтобы мобильный код управлялся;
- e) управление ресурсами, подходящими для доступа мобильного кода;
- f) криптографические средства управления для однозначного установления мобильного кода.

Прочая информация

Мобильный код является программируемым кодом, который переноситься с одного компьютера на другой компьютер, а затем автоматически исполняется и выполняет конкретную функцию при небольшом участии пользователя или без такового. Мобильный код связан с рядом услуг промежуточного программного обеспечения.

Кроме обеспечения того, что мобильный код не содержит злонамеренного кода, управление мобильным кодом важно для того, чтобы избежать неразрешенного использования или нарушения системы, сети или прикладных ресурсов и других нарушений в системе защиты информации.

10.5 Резервное копирование

Цель: Поддерживать целостность и доступность информации и средств обработки информации.

Должны быть созданы стандартные процедуры для реализации согласованной политики и стратегии в области резервного копирования (см. также 14.1) для снятия резервных копий данных и репетиции их своевременного восстановления.

10.5.1 Резервное копирование информации

Средство управления

Резервные копии информации и программного обеспечения должны регулярно сниматься и испытываться в соответствии с согласованной политикой резервного копирования.

Руководство по реализации

Должны быть предусмотрены адекватные средства создания резервных копий для обеспечения того, чтобы вся существенная информация и программное обеспечение могли быть восстановлены после бедствия или сбоя в работе носителя информации.

Для резервного копирования информации должны быть рассмотрены следующие пункты:

- a) должен быть определен необходимый уровень резервного копирования информации;
- b) должны быть созданы точные и полные записи о резервных копиях и документированные процедуры восстановления;
- c) объем (например, полное или выборочное резервное копирование) и частота резервного копирования должны отражать деловые требования организации, требования защиты вовлеченной информации и критичность информации для непрерывного функционирования организации;
- d) резервные копии должны храниться в достаточном отдалении, чтобы избежать любого ущерба от бедствия на основном месте;
- e) резервной информации должен быть придан надлежащий уровень физической и экологической защиты (см. раздел 9), соответствующий стандартам, применяемым на основном месте; средства управления, применяемые к носителю на основном месте, должны быть расширены так, чтобы охватить местоположение резервной копии;
- f) носители резервной копии должны регулярно испытываться для обеспечения того, чтобы на них можно положиться в случае аварийного использования, если будет необходимо;
- g) процедуры восстановления должны регулярно проверяться и испытываться, с целью обеспечить, что они являются результативными и что они могут быть выполнены в течение времени, выделенного в процедурах эксплуатации на восстановление;
- h) в ситуациях, где важна конфиденциальность, резервные копии должны быть защищены посредством шифрования.

Мероприятия по резервному копированию для отдельных систем должны регулярно испытываться для обеспечения того, что они удовлетворяют требованиям планов обеспечения непрерывности бизнеса (см. раздел 14). Для критических систем, мероприятия по резервному копированию должны охватывать всю системную информацию, приложения и данные, необходимые для восстановления полной системы в случае бедствия.

Должен быть определен срок хранения для существенной деловой информации, а также любое требование по сохранению архивных копий (см. 15.1.3).

Прочая информация

Мероприятия по резервному копированию могут быть автоматизированы для того, чтобы облегчить процессы резервного копирования и восстановления. Такие автоматизированные решения должны в достаточной степени испытываться перед реализацией и периодически.

10.6 Менеджмент защиты сети

Цель: Обеспечить защиту информации в сетях и защиту опорной инфраструктуры.

Безопасный менеджмент сетей, который может простираться за пределы границ организации, требует тщательного рассмотрения потока данных, юридических последствий, постоянного контроля и защиты.

Также могут потребоваться дополнительные средства для защиты важной информации, проходящей через общедоступные сети.

10.6.1 Средства управления сетью

Средство управления

Сети должны управляться и контролироваться надлежащим образом для того, чтобы быть защищенными от угроз, и для того, чтобы поддерживать защиту для систем и приложений, использующих сеть, включая транзитную информацию.

Руководство по реализации

Сетевые менеджеры должны реализовывать средства управления для обеспечения защиты информации в сетях, а также защиты связанных с ней услуг от неразрешенного доступа. В частности, должны быть рассмотрены следующие пункты:

- a) ответственность за эксплуатацию сетей должна быть отделена от функционирования компьютеров, если это уместно (см. 10.1.3);
- b) должны быть определены обязанности и процедуры по менеджменту дистанционного оборудования, включая оборудование в пользовательских зонах;

- c) специальные средства управления должны быть установлены для охраны конфиденциальности и целостности данных, проходящих через общедоступные сети или по беспроводным сетям, а также для защиты связанных систем и приложений (см. 11.4 и 12.3); специальные средства управления также могут потребоваться для поддержания доступности сетевых услуг и подключенных компьютеров;
- d) для того чтобы сделать возможным ведение записей о действиях, значимых для обеспечения безопасности, должны применяться надлежащий сбор данных и постоянный контроль;
- e) деятельность по менеджменту должна быть тщательно скоординирована, как для того, чтобы оптимизировать обслуживание организации, так и для того, чтобы обеспечить, что средства управления последовательно применяются по всей инфраструктуре обработки информации.

Прочая информация

Дополнительную информацию по защите сети можно найти в ISO/IEC 18028, Информационные технологии. Методы защиты. Защита сети IT.

10.6.2 Защита сетевых услуг

Средство управления

Характеристики защиты, уровни обслуживания и требования к менеджменту всех сетевых услуг должны быть определены и должны включаться в любое соглашение о предоставлении сетевых услуг, независимо от того, внутри ли организации или посредством аутсорсинга предоставляются эти услуги.

Руководство по реализации

Способность поставщика сетевых услуг безопасно управлять согласованными услугами должна быть определена и должна постоянно контролироваться, также должно быть согласовано право на аудит.

Должны быть определены меры по обеспечению защиты, необходимые для конкретных услуг, такие как характеристики защиты, уровни обслуживания и требования к менеджменту. Организация должна обеспечивать, чтобы поставщики сетевых услуг реализовывали эти меры.

Прочая информация

Сетевые услуги включают в себя предоставление соединений, услуги частных сетей, а также сети с дополнительными услугами и управляемые решения по защите сетей, такие как брандмауэры и системы обнаружения вторжения. Эти услуги могут быть разными, от простой неуправляемой полосы пропускания до сложных предложений с дополнительными возможностями.

Признаками защиты сетевых услуг могут быть следующие элементы:

- a) технология, применяемая для защиты сетевых услуг, такая как аутентификация, шифрование и средства управления сетевым подключением;
- b) технические параметры, необходимые для защищенного соединения с сетевыми службами в соответствии с правилами защиты и сетевых подключений;
- c) процедуры использования сетевых услуг, с целью ограничить доступ к сетевым услугам или приложениям, если это необходимо.

10.7 Обращение с носителями информации

Цель: Предотвратить неразрешенное раскрытие, модификацию, удаление или разрушение активов и прерывание деловой деятельности фирмы.

Носители должны управляться и должны быть физически защищены.

Для защиты документов, компьютерных носителей информации (например, лент, дисков), входных/выходных данных и системной документации от неразрешенного раскрытия, модификации, удаления и разрушения должны быть определены надлежащие процедуры эксплуатации.

10.7.1 Менеджмент сменных носителей информации

Средство управления

На местах должны иметься процедуры менеджмента сменных носителей.

Руководство по реализации

Для менеджмента сменных носителей должны быть рассмотрены следующие руководящие указания:

- a) если больше не требуется, то содержание любого носителя многоразового использования, которое надлежит удалить из организации, должно быть сделано невосстановимым;
- b) если это необходимо и целесообразно, то для удаления носителя из организации должно требоваться разрешение, и должны храниться записи о таких удалениях для ведения контрольного журнала;
- c) все носители должны храниться в безопасной, защищенной среде, в соответствии со спецификациями изготовителями;
- d) информация, хранящаяся на носителе, которая должна быть доступна в течение срока, превышающего срок службы носителя (в соответствии со спецификациями изготовителя), должна также храниться где-нибудь еще, чтобы избежать потери информации из-за ухудшения состояния носителя;

- e) регистрация сменного носителя должна быть рассмотрена для того, чтобы ограничить возможность потери данных;
- f) накопители со сменным носителем должны быть разрешены только в том случае, если для этого есть деловая причина.

Все процедуры и уровни полномочий должны быть четко документированы.

Прочая информация

Сменные носители включают в себя ленты, флэш-диски, съемные жесткие диски, CD-, DVD-диски и печатные носители информации.

10.7.2 Ликвидация носителей информации

Средство управления

Когда носитель больше не нужен, он должен ликвидироваться надежно и безопасно, используя официальные процедуры.

Руководство по реализации

Официальные процедуры безопасной ликвидации носителя должны минимизировать риски утечки важной информации к неполномочным лицам. Процедуры для безопасной ликвидации носителя, содержащего важную информацию, должны быть соразмерны с конфиденциальностью этой информации. Должны быть рассмотрены следующие пункты:

- a) носитель, содержащий важную информацию должен храниться и ликвидироваться надежно и безопасно, например, путем сжигания или измельчения, или же данные с него должны быть стерты в целях использования носителя для других приложений в рамках организации;
- b) должны быть приняты процедуры для того, чтобы выявлять элементы, которые могут потребовать безопасной ликвидации;
- c) может быть легче организовать все единицы носителей информации, которые предстоит собрать и безопасно ликвидировать вместо того, чтобы разделять важные элементы;
- d) много организаций предлагают услуги по сбору и ликвидации бумаг, оборудования и носителей; следует проявлять осторожность в выборе подходящего подрядчика с адекватными средствами управления и опытом;
- e) ликвидация уязвимых элементов должна регистрироваться, если это возможно, в целях ведения контрольного журнала.

При накапливании носителей для ликвидации, внимание должно быть уделено эффекту агрегации, который может сделать так, что большое количество информации, не являющейся важной, станет важным.

Прочая информация

Важная информация может быть раскрыта через небрежную ликвидацию носителей (см. также 9.2.6 на предмет информации о ликвидации оборудования).

10.7.3 Процедуры обращения с информацией

Средство управления

Должны быть определены процедуры для обращения с информацией и хранения информации, с целью защитить эту информацию от неразрешенного раскрытия или неправильного использования.

Руководство по реализации

Должны быть составлены процедуры для обращения с информацией, обработки, хранения информации и обмена информацией, согласующиеся с ее классификацией (см. 7.2). Должны быть рассмотрены следующие пункты:

- a) обращение с носителями и наклейка ярлыков на все носители в соответствии с указанным уровнем их классификации;
- b) ограничения доступа в целях предотвращения доступа неполномочного персонала;
- c) ведение официальной записи уполномоченных получателей данных;
- d) обеспечение полноты входных данных, правильного выполнения обработки и применения валидации⁶ выходных данных;
- e) защита буферизованных данных, ожидающих вывода, на уровне, соответствующем их конфиденциальности;
- f) хранение носителей в соответствии со спецификациями изготовителя;
- g) сведение распространения данных до минимума;
- h) четкая маркировка всех копий носителя для привлечения внимания санкционированного получателя;
- i) регулярный анализ списков рассылки и списков уполномоченных.

Прочая информация

Эти процедуры относятся к информации в документах, компьютерных системах, сетях, мобильных компьютерных средах, мобильных системах связи, почте, голосовой почте, передаче речи в общем, мультимедиа, почтовых службах/средствах, к использованию факсимильных аппаратов и любых других уязвимых элементов, например, незаполненные чеки, счета-фактуры.

⁶ Валидация [validation] – проверка достоверности (прим. переводчика)

10.7.4 Защита системной документации

Средство управления

Системная документация должна быть защищена от неразрешенного доступа.

Руководство по реализации

Для того чтобы защитить системную документацию, должны быть рассмотрены следующие пункты:

- a) системная документация должна храниться в безопасности;
- b) список полномочий по доступу к системной документации должен быть сведен к минимуму и утвержден владельцем приложения;
- c) системная документация, сохраняемая в общедоступных сетях, или поставляемая через общедоступную сеть, должна быть надлежащим образом защищена.

Прочая информация

Системная документация может содержать спектр важной информации, например, описания приложений, процессов, процедур, структур данных, процессов выдачи разрешения.

10.8 Обмен информацией

Цель: Поддерживать защиту информации и программного обеспечения, обмен которыми происходит в рамках организации и с любым внешним объектом.

Обмены информацией и программным обеспечением между организациями должны быть основаны на официальной политике обмена, проводимой в соответствии с соглашениями об обмене, и должны соответствовать любым законам, имеющим к ним отношение (см. раздел 15).

Для защиты информации и физических носителей, содержащих переносимую информацию, должны быть установлены процедуры и стандарты.

10.8.1 Политика и процедуры обмена информацией

Средство управления

Должны быть приняты официальная политика, процедуры обмена и средства управления обменом информацией для защиты обмена информацией, осуществляющегося с помощью всех типов средств связи.

Руководство по реализации

Процедуры и средства управления, которым нужно следовать при использовании электронных средств связи для обмена информацией, должны учитывать следующие пункты:

- a) процедуры, разработанные для защиты обмениваемой информации от перехвата, копирования, модификации, неправильной маршрутизации и разрушения;
- b) процедуры обнаружения и защиты от злонамеренного кода, который может быть передан посредством электронных средств связи (см. раздел 10.4.1);
- c) процедуры для защиты передаваемой уязвимой электронной информации, которая имеет форму приложения;
- d) политика или руководящие указания, очерчивающие приемлемое использование электронных средств связи (см. 7.1.3);
- e) процедуры для использования беспроводных средств связи, учитывающие конкретные вовлеченные риски;
- f) обязательства служащего, подрядчика и любого другого пользователя не компрометировать организацию, например, посредством дискредитации, беспокойства, персонации⁷, пересылки «писем счастья», несанкционированных приобретений и т.п.;
- g) использование криптографических методов, например, для защиты конфиденциальности, целостности и достоверности информации (см. раздел 12.3);
- h) руководящие указания по сохранению и ликвидации всей деловой корреспонденции, включая сообщения, согласно соответствующим государственным и местным законам и нормам;
- i) не оставлять уязвимую или критическую информацию на средствах печати, например, в копировальных устройствах, принтерах и в факсимильных аппаратах, поскольку эти средства могут быть доступны неполномочному персоналу;
- j) средства управления и ограничения, связанные с пересылкой средств связи, например, автоматическая пересылка электронной почты по внешним почтовым адресам;

⁷ персонация [impearsonation] – выдача себя за другое лицо (Прим. переводчика)

- k) напоминание персоналу о том, что они должны предпринимать надлежащие меры предосторожности, например, чтобы не раскрыть важную информацию, чтобы при совершении звонков избежать подслушивания или перехватывания информации:
 - 1) людьми, находящимися в непосредственной близости, особенно при использовании мобильных телефонов;
 - 2) при помощи перехвата телефонных разговоров и других форм подслушивания посредством физического доступа к телефонной трубке или телефонной линии, или посредством использования сканирующих радиоприемников;
 - 3) люди на конце получателя;
- l) не оставлять сообщений, содержащих важную информацию, на автоответчиках, поскольку они могут быть воспроизведены неполномочными лицами, сохранены в общих системах или неправильно сохранены в результате неправильного набора номера;
- m) напоминание персоналу о проблемах использования факсимильных аппаратов, а именно:
 - 1) неразрешенный доступ к встроенным хранилищам сообщений с целью извлечения сообщений;
 - 2) преднамеренное или случайное программирование аппаратов для того, чтобы посыпать сообщения на конкретные номера;
 - 3) отправление документов и сообщений на неправильные номера или вследствие неправильного набора номера, или вследствие использования неправильно сохраненного номера;
- n) напоминание персоналу о том, чтобы он не регистрировал демографические данные, такие как адрес электронной почты или другая личная информация, в какой-либо программе, с целью избежать сбора информации для неразрешенного использования;
- o) напоминание персоналу о том, что современные факсимильные и фотокопировальные аппараты имеют кэш-память для страниц и в случае проблем с бумагой или сбоя передачи сохраняют страницы, которые будут напечатаны, как только дефект будет устранен.

Кроме того, персоналу надо напоминать о том, что они не должны вести конфиденциальные беседы в общественных местах или открытых офисах и местах для встреч, не имеющих звуконепроницаемых стен.

Средства обмена информацией должны соответствовать всем имеющим к ним отношение требованиям закона (см. раздел 15).

Прочая информация

Обмен информацией может происходить при помощи множества различных типов средств связи, включая электронную почту, устройства для передачи речи, факсимильные аппараты и видео.

Обмен программным обеспечением может происходить при помощи множества различных типов носителей, включая загрузку из Интернета и приобретение у поставщиков, продающих готовые продукты.

Должны быть учтены деловые, юридические последствия и последствия нарушения безопасности, связанные с обменом электронными данными, электронной торговлей и электронными средствами обмена информацией, а также требования к средствам управления.

Информация может быть раскрыта из-за недостатка осведомленности, политики или процедур использования средств обмена информацией, например, путем прослушивания мобильного телефона в общественном месте, неправильного направления сообщения электронной почты, подслушивания автоответчиков, неразрешенного доступа к вызываемым по телефону системам голосовой почты или случайной отправки факсов на неправильное факсимильное оборудование.

Деловые операции могут быть нарушены, а информация может быть раскрыта, если средства связи дают сбой, перегружаются или если их работа прерывается (см. 10.3 и раздел 14). Информация может быть раскрыта, если к ней осуществляется доступ неполномочными пользователями (см. раздел 11).

10.8.2 Соглашения об обмене

Средство управления

Должны быть установлены соглашения об обмене информацией и программным обеспечением между организацией и внешними сторонами.

Руководство по реализации

Соглашения об обмене должны учитывать следующие условия обеспечения безопасности:

- a) обязанности руководства по управлению передачей, отправкой и получением и по уведомлению об этом;
- b) процедуры для уведомления отправителя о передаче, отправке и получении;
- c) процедуры для обеспечения прослеживаемости и неотрекаемости;
- d) минимальные технические стандарты упаковки и передачи;
- e) договор об условном депозите;
- f) стандарты установления личности курьера;

- g) обязанности и обязательства в случае инцидентов в системе защиты информации, таких как потеря данных;
- h) использование согласованной системы маркировки для уязвимой или критической информации, обеспечивающее незамедлительно понимание значения этикеток и надлежащей защиты информации;
- i) собственность и обязанности в отношении защиты данных, авторского права, соответствия лицензии на использование программного обеспечения и подобные соображения (см. 15.1.2 и 15.1.4);
- j) технические стандарты записи и чтения информации и программного обеспечения;
- k) любые специальные средства управления, которые могут потребоваться для защиты уязвимых элементов, такие как криптографические ключи (см. 12.3).

Для защиты информации и физических носителей информации при транспортировке (см. также 10.8.3) политика, процедуры и стандарты должны быть определены, должны поддерживаться и должны быть указаны в таких соглашениях об обмене.

Содержание любого соглашения, касающееся обеспечения безопасности, должно отражать конфиденциальность вовлеченной деловой информации.

Прочая информация

Соглашения могут быть электронными или написанными от руки, и могут приобретать форму официальных договоров или условий работы по найму. Для важной информации, конкретные механизмы, используемые для обмена такой информацией, должны быть единообразными для всех организаций и типов соглашений.

10.8.3 Физические носители при транспортировке

Средство управления

Носитель, содержащий информацию, должен быть защищен от неразрешенного доступа, неправильного использования или повреждения в ходе транспортировки за пределы физических границ организации.

Руководство по реализации

Для защиты носителей информации, транспортируемых между местами расположения, должны быть рассмотрены следующие руководящие указания:

- a) должен использоваться надежный транспорт или;
- b) список уполномоченных курьеров должен быть согласован с руководством;
- c) должны быть разработаны процедуры для проверки удостоверения личности курьеров;

- d) упаковки должно быть достаточно для защиты содержимого от любого физического повреждения, которое может иметь место в ходе транспортировки и упаковка должна соответствовать любым спецификациям изготовителя (например, для программного обеспечения), в качестве примера можно привести защиту от каких-либо факторов влияния окружающей среды, которые могут снизить результативность восстановления носителя, например, воздействие тепла, влаги или электромагнитных полей;
- e) для защиты важной информации от неразрешенного раскрытия или модификации должны быть приняты, если это необходимо, средства управления; примеры включают следующее:
 - 1) использование запертых контейнеров;
 - 2) доставка под роспись;
 - 3) упаковка с индикацией признаков ее несанкционированного вскрытия (которая показывает любую попытку получить доступ к ее содержимому);
 - 4) в исключительных случаях, разбиение груза на более чем одну поставку и отправка разными маршрутами.

Прочая информация

Информация может быть уязвимой для неразрешенного доступа, неправильного обращения или повреждения в ходе физической транспортировки, например при отправке носителя по почте или курьером.

10.8.4 Электронный обмен сообщениями

Средство управления

Информация, включенная в электронный обмен сообщениями, должна быть надлежащим образом защищена.

Руководство по реализации

Соображения, связанные с обеспечением безопасности электронного обмена сообщениями, должны включить следующее:

- a) защита сообщений от неразрешенного доступа, модификации или отказа от обслуживания;
- b) обеспечение правильной адресации и транспортировки сообщения;
- c) общая надежность и доступность услуги;
- d) правовые соображения, например требования для электронных подписей;

- e) получение утверждения перед использованием внешних услуг связи, таких как система немедленной передачи сообщений или совместное использование файла;
- f) более высокие уровни аутентификации, управляющие доступом из сетей общественного пользования.

Прочая информация

Электронный обмен сообщениями, такой как электронная почта, электронный обмен данными (EDI) и система немедленной передачи сообщений играют чрезвычайно важную роль в деловом общении. Электронный обмен сообщениями имеет риски, отличные от рисков обмена напечатанной информацией.

10.8.5 Информационные системы для бизнеса

Средство управления

Для защиты информации, связанной с взаимосвязью информационных систем для бизнеса, должны быть разработаны и реализованы политика и процедуры.

Руководство по реализации

При рассмотрении последствий соединения таких средств для безопасности и для бизнеса, должно быть учтено следующее:

- a) известные слабые места в административной системе и системе учета, где информация используется совместно разными частями организации;
- b) уязвимость информации в системах передачи деловой информации, например, записывание телефонных звонков или конференций, конфиденциальность звонков, память факсимильных аппаратов, открытие сообщений, пришедших по почте, распространение почты;
- c) политика и надлежащие средства управления для менеджмента совместного использования информации;
- d) исключение категорий уязвимой деловой информации и закрытых документов, если система не обеспечивает подходящий уровень защиты (см. 7.2);
- e) ограничение доступа к информации регистрационного журнала, связанной с выбранными лицами, например, персоналом, работающим над уязвимыми проектами;
- f) категории персонала, подрядчиков или деловых партнеров, которым позволено использовать систему и места, из которых к ней может быть осуществлен доступ (см. 6.2 и 6.3);
- g) ограничение выбранных средств на конкретные категории пользователей;

- h) идентификация статуса пользователей, например, служащих организации или подрядчиков, в директориях ради других пользователей;
- i) сохранение и резервное копирование информации, содержащейся в системе (см. 10.5.1);
- j) требования и мероприятия в чрезвычайной ситуации (см. 14).

Прочая информация

Офисные информационные системы – это возможность для более быстрого распространения и совместного использования деловой информации, используя комбинацию следующего: документы, компьютеры, мобильные средства обработки, мобильные средства связи, почта, голосовая почта, голосовые средства связи в общем, мультимедиа, почтовые службы/средства и факсимильные аппараты.

10.9 Услуги электронной торговли

Цель: Обеспечить защиту услуг электронной торговли и их безопасное использование.

Должны быть рассмотрены последствия нарушения безопасности, связанного с использованием услуг электронной торговли, включая онлайневые сделки, а также требования для средств управления. Также должны быть рассмотрены целостность и доступность информации, опубликованной при помощи электронных средств через системы общего доступа.

10.9.1 Электронная торговля

Средство управления

Информация, вовлеченная в электронную торговлю, проходящая через общедоступные сети должна быть защищена от мошеннической деятельности, споров по договору, а также от неразрешенного раскрытия и модификации.

Руководство по реализации

Соображения, связанные с обеспечением безопасности электронной торговли, должны включать следующее:

- a) степень уверенности, который необходим каждой стороне в предъявляемой идентификационной информации друг друга, например, через аутентификацию;
- b) процессы выдачи разрешения, связанные с тем, кто может устанавливать цены, выпускать или подписывать ключевые торговые документы;
- c) обеспечение того, чтобы торговые партнеры были полностью проинформированы о своих полномочиях;

- d) определение и выполнение требований конфиденциальности, целостности, доказательства отправки и получения ключевых документов и неотрекаемости договоров, например, [требований] связанных с тендерными и договорными процессами;
- e) степень доверия, требуемого к целостности официального прайс-листа;
- f) конфиденциальность любых важных данных или информации;
- g) конфиденциальность и целостность любых сделок по заказам, информации об оплате, подробности об адресе доставки, а также подтверждение получения;
- h) степень верификации, достаточная для проверки информации об оплате, предоставленной потребителем;
- i) выбор наиболее подходящей расчетной формы оплаты для того, чтобы избежать мошенничества;
- j) уровень защиты, требуемый для поддержания конфиденциальности и целостности информации о заказе;
- k) исключение потери или дублирования информации о сделке;
- l) ответственность, связанная с любыми мошенническими сделками;
- m) страховые требования.

Многие из вышеуказанных соображений могут быть учтены применением криптографических средств управления (см. 12.3), принимая во внимание соответствие требованиям закона (см. 15.1, особенно 15.1.6 для законодательства в области криптографии).

Соглашение об электронной торговле между торговыми партнерами должно быть поддержано документированным соглашением, которое связывает обе стороны согласованными условиями торговли, включая детали выдачи разрешения (см. пункт b) выше). Могут понадобиться другие соглашения с информационными службами и поставщиками дополнительных сетевых услуг.

Прочая информация

Общедоступные системы торговли должны уведомить потребителей о своих условиях ведения дела.

Внимание должно быть уделено устойчивости по отношению к атакам хоста (хостов), используемых для электронной торговли, и последствиям нарушения защиты, связанными с любым межсетевым соединением, необходимым для реализации услуг электронной торговли (см. 11.4.6).

Прочая информация

Электронная торговля уязвима по отношению к ряду сетевых угроз, которые могут привести к мошеннической деятельности, спорам по договору, а также к раскрытию или модификации информации.

Электронная торговля может использовать безопасные методы аутентификации, например, используя криптографию с открытым ключом и цифровые подписи (см. также 12.3) для того, чтобы снизить риски. Также можно использовать надежные трети стороны там, где необходимы такие услуги.

10.9.2 Онлайновые сделки

Средство управления

Информация, вовлеченная в онлайновые сделки, должна быть защищена для того, чтобы предотвратить неполную передачу, неправильную маршрутизацию, неразрешенное изменение сообщения, неразрешенное раскрытие, неразрешенное дублирование или воспроизведение сообщения.

Руководство по реализации

Соображения, связанные с обеспечением безопасности для онлайновых сделок, должны включить следующее:

- a) использование электронных подписей каждой из сторон, вовлеченных в сделку;
- b) все аспекты сделки, т.е. обеспечение того, что:
 - 1) «верительные данные» пользователей всех сторон являются достоверными и верифицированными;
 - 2) сделка остается конфиденциальной; и
 - 3) сохраняется секретность, связанная со всеми вовлеченными сторонами;
- c) каналы связи между всеми вовлеченными сторонами зашифрованы;
- d) протоколы, используемые для обмена информацией между всеми вовлеченными сторонами, защищены;
- e) обеспечение того, чтобы место хранения подробностей сделки находилось вне общедоступных сред, например, на платформе для хранения, существующей в организационной внутренней сети, а не находилось незащищенным на носителе для хранения, непосредственно доступном из Интернета;
- f) если используется высоконадежная организация (например, для целей выпуска и поддержания цифровых подписей и/или цифровых сертификатов), то защита должна быть интегрирована и внедрена на всем протяжении процесса менеджмента.

Прочая информация

Объем принятых средств управления должен быть соразмерен уровню риска, связанного каждой формой онлайновой сделки.

Возможно, сделкам необходимо будет подчиняться законам, правилам и нормам в юрисдикции, где сделка создается, посредством которой обрабатывается, в которой она выполняется и/или где хранится.

Существует много форм сделок, которые могут выполняться в онлайновом режиме, например, договорные, финансовые и т.п.

10.9.3 Общедоступная информация

Средство управления

Целостность информации, сделанной доступной в общедоступной системе, должна быть защищена для того, чтобы предотвратить неразрешенную модификацию.

Руководство по реализации

Программное обеспечение, данные и другая информация, требующая высокого уровня целостности, сделанная доступной в общедоступной системе, должна быть защищена подходящими механизмами, например, цифровыми подписями (см. 12.3). Общедоступная система должна испытываться на слабые места и сбои до того, как информация будет сделана доступной.

Прежде чем информация будет сделан общедоступной, должен осуществляться официальный процесс утверждения. Кроме того, все вводимые данные, предоставляемые системе извне, должны быть верифицированы и утверждены.

Электронные издательские системы, особенно те, которые разрешают обратную связь и прямой ввод информации, должны тщательно контролироваться для того, чтобы:

- a) информация получалась в соответствии с законодательством в области защиты данных (см. 15.1.4);
- b) информация, вводимая в систему публикации и обрабатываемая ею, обрабатывалась полностью, аккуратно и своевременно;
- c) важная информация защищалась в ходе сбора, обработки и хранения;
- d) доступ к издательской системе не давал возможности непреднамеренного доступа к сетям, с которыми связана система.

Прочая информация

Может понадобиться, чтобы информация в общедоступной системе, например, информация на web-сервере, доступном через Интернет, соответствовала законам, правилам и нормам в юрисдикции, в которой находится система, где происходит

торговля или где находится (находятся) владелец (владельцы). Неразрешенная модификация опубликованной информации может повредить репутации публикующей организации.

10.10 Постоянный контроль

Цель: Обнаруживать неразрешенную деятельность по обработке информации.

Системы должны постоянно контролироваться, и должны записываться события в системе защиты информации. Журналы оператора и регистрация отказов должны использоваться для обеспечения выявления проблем в системе защиты информации.

Организация должна соответствовать всем юридическим требованиям, применимым к ее деятельности по постоянному контролю и регистрации.

Постоянный контроль системы должен использоваться для того, чтобы проверять результативность утвержденных средств управления и для того, чтобы верифицировать соответствие модели политики в области доступа.

10.10.1 Ведение контрольного журнала

Средство управления

Контрольные журналы, регистрирующие действия пользователей, исключения и события в системе защиты информации, должны быть созданы и должны храниться в течение согласованного периода для того, чтобы помогать в будущих расследованиях и постоянном контроле доступа.

Руководство по реализации

Контрольные журналы должны включать, если это относится к делу, следующее:

- a) идентификаторы пользователя [user IDs];
- b) даты, времена и подробности ключевых событий, например, вход в систему и выход из системы;
- c) идентификационная информация терминала или местоположение терминала, если возможно;
- d) записи успешных и отклоненных попыток доступа к системе;
- e) записи успешных и отклоненных попыток доступа к данным и другим ресурсам;
- f) изменения в системной конфигурации;
- g) использование привилегий;
- h) использование системных утилит и приложений;

- i) файлы, к которым осуществлялся доступ, и тип доступа;
- j) сетевые адреса и протоколы;
- k) тревоги, поднятые системой управления доступом;
- l) активизация и дезактивизация систем защиты, таких как анти-вирусные системы и системы обнаружения вторжения.

Прочая информация

Контрольные журналы могут содержать интрузивные и конфиденциальные личные данные. Должны быть предприняты надлежащие меры обеспечения секретности (см. также 15.1.4). Там, где это возможно, системные администраторы не должны иметь разрешение стирать или дезактивировать протоколы своей собственной деятельности (см. 10.1.3).

10.10.2 Постоянный контроль использования систем

Средство управления

Должны быть определены процедуры для постоянного контроля использования средств обработки информации, а результаты деятельности по постоянному контролю должны регулярно анализироваться.

Руководство по реализации

Уровень постоянного контроля, необходимый для отдельных средств, должен быть определен оценкой рисков. Организация должна соответствовать всем требованиям закона, применимым к ее деятельности по постоянному контролю. Области, которые должны быть учтены, включают следующее:

- a) разрешенный доступ, включая подробности, например, следующие:
 - 1) идентификатор пользователя;
 - 2) дата и время ключевых событий;
 - 3) типы событий;
 - 4) файлы, к которым осуществлялся доступ;
 - 5) используемые программа/утилиты;
- b) все привилегированные операции, например, следующие:
 - 1) использование привилегированных учетных записей, например, супервизор, корневой [супервизор], администратор;
 - 2) запуск и остановка системы;

- 3) присоединение/отсоединение устройства ввода/вывода;
- c) попытки неразрешенного доступа, например, следующие:
 - 1) давшие сбой или отклоненные действия пользователя;
 - 2) давшие сбой или отклоненные действия, включающие данные и другие ресурсы;
 - 3) нарушения политики в области доступа и уведомления для сетевых шлюзов и брандмауэров;
 - 4) предупреждения от специализированных систем обнаружения вторжения;
- d) системные предупреждения и сбои, например, следующие:
 - 1) предупреждения или сообщения на пульт;
 - 2) исключения из системного журнала;
 - 3) индикации аварии управления сетью;
 - 4) тревоги, поднятые системой управления доступом;
- e) изменения или попытки изменения настроек и средств управления защищкой системы.

То, как часто анализируются результаты деятельности по постоянному контролю, должно зависеть от вовлеченных рисков. Факторы рисков, которые должны быть учтены, включают следующее:

- a) критичность процессов приложения;
- b) ценность, уязвимость и критичность вовлеченной информации;
- c) прошлый опыт проникновения в систему и неправильного использования системы, а также частота использования слабых мест [в системе защиты];
- d) степень межсистемной связи (особенно с сетями общего доступа);
- e) дезактивация средства ведения журнала.

Прочая информация

Использование процедур постоянного контроля необходимо для обеспечения того, чтобы пользователи выполняли только ту деятельность, которая явно разрешена.

Анализ журнала включает понимание угроз, с которыми столкнулась система, и способов, которыми они могут возникнуть. Примеры событий, которые могут потребовать дальнейшего расследования в случае инцидентов в системе защиты информации, приведены в 13.1.1.

10.10.3 Защита данных журнала

Средство управления

Средства ведения журнала и информация, содержащаяся в журнале, должны быть защищены от тайного вмешательства и неразрешенного доступа.

Руководство по реализации

Средства управления должны стремиться защитить от неразрешенных изменений и эксплуатационных проблем средства ведения журнала, включая следующее:

- a) изменения в типах записываемых сообщений;
- b) редактирование или удаление файла системного журнала;
- c) превышение емкости носителя информации, используемого для сохранения файла системного журнала, приводящее или к тому, что событие не записывается, или к перезаписыванию ранее полномочных событий.

Некоторые контрольные журналы может потребоваться архивировать как часть политики хранения документации или из-за требований собирать и сохранять доказательства (см. также 13.2.3).

Прочая информация

Системные журналы часто содержат большой объем информации, большая часть которого не относится к постоянному контролю защиты. Для того чтобы помочь выявить значимые события для целей постоянного контроля, должно быть рассмотрено автоматическое копирование сообщений надлежащих типов во второй журнал, и/или использование подходящих системных утилит или средств ведения контрольного журнала, с целью выполнить контрольное считывание и рационализацию файла.

Системные журналы должны быть защищены, поскольку если данные в них могут быть модифицированы или стерты, то их существование может создавать обманчивое чувство безопасности.

10.10.4 Журналы оператора и администратора

Средство управления

Деятельность системного администратора и системного оператора должна заноситься в журнал.

Руководство по реализации

В журналы должно включаться следующее:

- a) время, когда произошло событие (благоприятный исход или сбой);

- b) информация о событии (например, файлы, с которыми работали) или сбои (например, случившаяся ошибка и предпринятое корректирующее действие);
- c) какая учетная запись, и какой администратор или оператор были вовлечены;
- d) какие процессы были вовлечены.

Журналы системного администратора и оператора должны регулярно анализироваться.

Прочая информация

Для постоянного контроля деятельности системных и сетевых администраторов может использоваться система обнаружения вторжения, управляемая за пределами сферы контроля системных и сетевых администраторов.

10.10.5 Регистрация отказов

Средство управления

Отказы должны быть зарегистрированы, проанализированы, и должно быть предпринято подходящее действие.

Руководство по реализации

Отказы, о которых сообщили пользователи или системные программы, и которые относятся к проблемам с системами обработки информации или с системами обмена информацией, должны быть зарегистрированы. Должны иметься четкие правила для обращения с сообщенными отказами, включая следующее:

- a) анализ журналов регистрации отказов с целью гарантировать, что проблемы с отказами были удовлетворительным образом разрешены;
- b) анализ корректирующих мер с целью гарантировать, что средства управления не были подвергнуты риску, и что предпринятое действие полностью разрешено.

Должно быть обеспечено, чтобы была включена регистрация ошибок, если эта системная функция доступна.

Прочая информация

Регистрация ошибок и отказов может повлиять на функционирование системы. Такая регистрация должна быть включена компетентным персоналом, а уровень регистрации, необходимый для отдельных систем должен определяться оценкой рисков, с учетом ухудшения функционирования.

10.10.6 Синхронизации часов

Средство управления

Часы всех значимых систем обработки информации в организации или доменов безопасности должны быть синхронизированы с согласованным источником точного времени.

Руководство по реализации

Если компьютер или устройство связи имеет возможность управлять часами реального времени, то эти часы должны быть установлены по согласованному эталону, например, универсальное глобальное время (по Гринвичу) (UTC) или местное декретное время. Поскольку известно, что некоторые часы со временем дрейфуют, то должна иметься процедура, которая проверяет, исправляет и корректирует любую значимую вариацию.

Правильная интерпретация формата даты/времени важна для обеспечения того, чтобы временная метка отражала реальную дату/время. Должны быть учтены местные особенности (например, переход на «летнее время»).

Прочая информация

Правильная установка компьютерных часов важна для обеспечения точности контрольных журналов, которая может быть необходима для расследований или в качестве доказательств в случае нарушений законы или дисциплинарных проступках. Неточные контрольные журналы могут воспрепятствовать таким расследованиям и повредить правдоподобности такого доказательства. Часы, связанные с передачей времени по радио от государственных атомных часов, могут использоваться как главные часы для регистрирующих систем. Для того чтобы поддерживать все серверы в синхронизации с главными часами, может использоваться сетевой протокол службы времени.

11 Управление доступом

11.1 Деловые требования к управлению доступом

Цель: Управлять доступом к информации.

Доступ к информации, средствам обработки информации и деловым процессам должен управляться на основе деловых требований и требований защиты.

Правила управления доступом должны учитывать политику по распространению информации и выдаче разрешений.

11.1.1 Политика управления доступом

Средство управления

Политика управления доступом должна быть определена, документально подтверждена и должна анализироваться на основе деловых требований и требований защиты для доступа.

Руководство по реализации

Правила управления доступом и права доступа для каждого пользователя или группы пользователей должны быть четко сформулированы в политике управления доступом. Средства управления доступом бывают как логические, так и физические (см. также раздел 9), и они должны рассматриваться вместе. Пользователям и поставщикам услуг должна быть предъявлена четкая формулировка деловых требований, которые нужно выполнить средствам управления доступом.

Политика должна учитывать следующее:

- a) требования защиты отдельных деловых приложений;
- b) выявление всей информации, связанной с деловыми приложениями, и рисков, с которыми сталкивается информация;
- c) политика распространения информации и выдачи разрешения, например, принцип необходимого знания, уровни защиты и классификация информации (см. 7.2);
- d) согласованность между управлением доступом и политикой в области классификации информации разных систем и сетей;
- e) соответствующее законодательство и любые договорные обязательства, касающиеся защиты доступа к данным или услугам (см. 15.1);
- f) стандартные полномочия доступа пользователя для обычных должностных обязанностей в организации;

- g) менеджмент прав доступа в распределенной и сетевой среде, которая признает все типы доступных соединений;
- h) разделение ролей в области управления доступом, например, запрос на получение доступа, разрешение доступа, администрирование доступа;
- i) требования к официальному разрешению запросов на доступ (см. 11.2.1);
- j) требования к периодическому анализу средств управления доступом (см. 11.2.4);
- k) удаление прав доступа (см. 8.3.3).

Прочая информация

Следует позаботиться о том, чтобы при определении правил управления доступом учесть следующее:

- a) провести различие между правилами, которые всегда должны выполняться, и руководящими указаниями, которые являются необязательными или условными;
- b) установление правил, основанных на предпосылке «Все в общем случае запрещено, если явно не разрешено», а не на более слабом правиле «Все в общем случае разрешено, если явно не запрещено»;
- c) изменения в информационных метках (см. 7.2), которые вводятся автоматически средствами обработки информации, и в метках, введенных на усмотрение пользователя;
- d) изменения в полномочиях пользователя, которые вводятся автоматически информационной системой и в полномочиях, введенных администратором;
- e) правила, которые требуют особого утверждения перед вступлением в силу, и правила, которые этого не требуют.

Правила управления доступом должны поддерживаться официальными процедурами и четко определенными обязанностями (см., например, 6.1.3, 11.3, 10.4.1, 11.6).

11.2 Менеджмент доступа пользователей

Цель: Обеспечивать доступ зарегистрированного пользователя и предотвращать неразрешенный доступ к информационным системам.

Должны быть приняты официальные процедуры для управления назначением прав доступа к информационным системам и услугам.

Процедуры должны охватывать все этапы времени существования доступа пользователя, от первоначальной регистрации новых пользователей до окончательной отмены регистрации пользователей, которым больше не требуется доступ к информационным системам и услугам. Особое внимание должно быть уделено, если это необходимо, потребности в управлении распределением привилегированных прав доступа, которые позволяют пользователям игнорировать средства управления системой.

11.2.1 Регистрация пользователя

Средство управления

Должна быть принята официальная процедура регистрации и отмены регистрации пользователя для предоставления и отмены доступа ко всем информационным системам и услугам.

Руководство по реализации

Процедура управления доступом для регистрации и отмены регистрации пользователя должна включать в себя следующее:

- a) использование уникальных идентификаторов пользователей для того, чтобы дать пользователям возможность быть связанными со своими действиями и нести за них ответственность; использование групповых идентификаторов должно быть разрешено только там, где они необходимы по деловым или практическим причинам, и оно должно быть утверждено и документировано;
- b) проверка того, что пользователь имеет разрешение владельца системы на использование информационной системы или услуги; отдельное утверждение прав доступа со стороны руководства также может быть уместным;
- c) проверка того, что уровень предоставленного доступа соответствует деловой цели (см. 11.1) и согласуется с организационной политикой в области защиты, например, он не подвергает риску разделение обязанностей (см. 10.1.3);
- d) предоставление пользователям письменных формулировок их прав доступа;
- e) требование того, чтобы пользователи подписывали заявления, указывающие, что они понимают условия доступа;
- f) обеспечение того, чтобы поставщики услуг не предоставляли доступ до тех пор, пока процедуры выдачи разрешения не будут завершены;
- g) поддержание официальной записи всех лиц, зарегистрировавшихся для того, чтобы использовать услугу;
- h) немедленное удаление или блокировка прав доступа пользователей, которые изменили роли или должности, или ушли из организации;

- i) периодическая проверка, а также удаление или блокировка, избыточных идентификаторов и учетных записей пользователей (см. 11.2.4);
- j) обеспечение того, что избыточные идентификаторы пользователей не были выданы другим пользователям.

Прочая информация

Внимание должно быть уделено определению ролей доступа пользователей, основанных на деловых требованиях, которые суммируют некоторое количество прав доступа в типичные полномочия доступа пользователя. Запросами на доступ и анализом доступа (см. 11.2.4) легче управлять на уровне таких ролей, чем на уровне конкретных прав.

Внимание должно быть уделено включению в договоры с персоналом и договоры на обслуживание разделов, которые определяют санкции в случае попытки неразрешенного доступа, осуществленной персоналом или агентами обслуживания (см. также 6.1.5, 8.1.3 и 8.2.3).

11.2.2 Менеджмент привилегий

Средство управления

Распределение и использование привилегий должно быть ограничено и управляемо.

Руководство по реализации

Многопользовательские системы, которые требуют защиты от неразрешенного доступа, должны иметь распределение привилегий, управляемое через официальный процесс выдачи разрешений. Должны быть рассмотрены следующие шаги:

- a) должны быть выявлены привилегии доступа, связанные с каждым системным продуктом, например, операционной системой, системой управления базами данных, и с каждым приложением, а также пользователи, которым их необходимо распределить;
- b) привилегии должны быть распределены пользователям на основе принципа необходимости использования и принципа «событие - за - событием» [event-by-event] в соответствии с политикой управления доступом (11.1.1), т.е. минимальное требование к их функциональной роли только когда нужно;
- c) процесс выдачи разрешений и запись всех распределенных привилегий должны поддерживаться в рабочем состоянии. Привилегии не должны предоставляться до тех пор, пока процесс выдачи разрешений не будет завершен;
- d) должны поощряться разработка и использование системных стандартных программ, с целью избежать необходимости предоставлять привилегии пользователям;

- e) должны поощряться разработка и использование программ, которые избегают необходимости работы с привилегиями;
- f) привилегии должны быть назначены другому идентификатору пользователя, отличному от тех, которые используются для обычного делового применения.

Прочая информация

Неподходящее использование привилегий системного администрирования (любая характеристика или средство информационной системы, которые дают пользователю возможность игнорировать средства управления системой или приложением), могут быть основным фактором, дающим вклад в сбои или нарушения в работе систем.

11.2.3 Менеджмент паролей пользователя

Средство управления

Распределение паролей должно управляться посредством официального процесса управления.

Руководство по реализации

Процесс должен включать следующие требования:

- a) от пользователя надо потребовать подписать заявление сохранять личные пароли в тайне и сохранять групповые пароли исключительно в пределах участников группы; это подписанное заявление может быть включено в условия работы по найму (см. 8.1.3);
- b) если от пользователей требуется поддерживать свои собственные пароли, то изначально им должен быть предоставлен безопасный временный пароль (см. 11.3.1), который они вынуждены изменить немедленно;
- c) установить процедуры для верификации личности пользователя перед предоставлением ему нового, заменяющего или временного пароля;
- d) временные пароли должны даваться пользователям безопасным способом; надо избегать использования третьей стороны или незащищенных (открытый текст) сообщений электронной почты;
- e) временные пароли должны быть уникальными для личности и не должны быть угадываемыми;
- f) пользователи должны подтвердить получение паролей;
- g) пароли никогда не должны храниться в компьютерных системах в незащищенной форме;
- h) пароли поставщика по умолчанию должны быть изменены после установки систем или программного обеспечения.

Прочая информация

Пароли являются обычным средством верификации личности пользователя до того, как будет предоставлен доступ к информационной системе или услуге в соответствии с полномочиями пользователя. Имеются и должны быть рассмотрены другие технологии идентификации и аутентификации пользователя, такие как биометрические характеристики, например, верификация отпечатков пальцев, проверка подписи, а также использование аппаратных маркеров [tokens], например, смарт-карт.

11.2.4 Анализ прав доступа пользователя

Средство управления

Руководство должно регулярно анализировать права доступа пользователей, используя официальный процесс.

Руководство по реализации

Анализ прав доступа должен учитывать следующие руководящие указания:

- a) права доступа пользователей должны анализироваться регулярно, например, через каждые 6 месяцев, и после любых изменений, например, повышение в должности, понижение в должности или прекращение работы по найму (см. 11.2.1);
- b) права доступа пользователей должны анализироваться и перераспределяться при смене одного места работы на другое в рамках одной организации;
- c) разрешения на особые привилегированные права доступа (см. 11.2.2), должны анализироваться более часто, например, каждые 3 месяца;
- d) распределения привилегий должно проверяться регулярно для того, чтобы обеспечить, что не были получены неразрешенные привилегии;
- e) изменения в привилегированных учетных записях должны быть зарегистрированы для целей периодического анализа.

Прочая информация

Необходимо регулярно анализировать права доступа пользователей для того, чтобы поддерживать результативный контроль над доступом к данным и информационным услугам.

11.3 Обязанности пользователя

Цель: предотвратить неразрешенный доступ пользователей, а также раскрытие или кражу информации и средств обработки информации.

Для результативной защиты важно сотрудничество полномочных пользователей.

Пользователей надо уведомить об их обязанностях по поддержанию результативных средств управления доступом, особенно в том, что касается использования паролей и защиты оборудования пользователя.

Должна реализовываться политика чистого стола и чистого экрана для того, чтобы снизить риски неразрешенного доступа или повреждения бумаг, носителей и средств обработки информации.

11.3.1 Использование пароля

Средство управления

От пользователей надо требовать следовать хорошим методам защиты при выборе и использовании паролей.

Руководство по реализации

Всем пользователям надо посоветовать следующее:

- a) сохранять пароли в тайне;
- b) избегать вести запись (например, на бумаге, в программном файле или в карманном устройстве) паролей, за исключением тех случаев, когда запись может храниться безопасно, а метод хранения был утвержден;
- c) менять пароли всякий раз, когда есть любое указание на возможное раскрытие системы или пароля;
- d) выбирать качественные пароли с достаточной минимальной длиной, которые:
 - 1) легко запоминаются;
 - 2) не основаны на чем-нибудь, о чем кто-либо другой мог бы легко догадаться или получить, используя информацию, связанную с личностью человека, например, имена, номера телефонов, даты рождения и т.п.;
 - 3) не являются уязвимыми для словарных атак (т.е. не состоят из слов, включенных в словари);
 - 4) не содержат последовательных идентичных, всех цифровых или всех буквенных, символов;
- e) менять пароли регулярно или на основе количества доступов (пароли для привилегированных учетных записей должны меняться чаще, чем обычные пароли) и избегать повторного использования или циклического повторения старых паролей;
- f) менять временные пароли при первом входе в систему;
- g) не включать пароли в какой-либо автоматизированный процесс входа в систему, например, сохраненный в макросе или в функциональном ключе;

- h) не использовать совместно личные пароли пользователя;
- i) не использовать один и тот же пароль для деловых и неделевых целей.

Если пользователям необходимо иметь доступ нескольким службам, системам или платформам, и от них требуется поддерживать несколько отдельных паролей, то им надо посоветовать использовать один, качественный пароль (см. d) выше) для всех служб, где пользователю гарантируется, что для хранения пароля в каждой службе, системе или платформе была установлена достаточная степень защиты.

Прочая информация

Менеджмент системы справочной службы, работающей с потерянным или забытыми паролями, требует особого внимания, как она также может быть средством атаки на систему паролей.

11.3.2 Оборудование пользователя, находящееся без присмотра

Средство управления

Пользователи должны гарантировать, что оборудование, находящееся без присмотра, имеет подходящую защиту.

Руководство по реализации

Все пользователи должны быть осведомлены о требованиях защиты и процедурах для защиты оборудования, находящегося без присмотра, а также о своих обязанностях по реализации такой защиты. Пользователям надо посоветовать следующее:

- a) закрывать активные сеансы по завершении работы, если только их нельзя защитить подходящим блокирующим механизмом, например, защищенным паролем хранитель экрана;
- b) выходить из системы универсальных ЭВМ, серверов и офисных ПК по завершении сеанса (т.е. не просто выключить экран ли терминал ПК);
- c) защитить ПК или терминалы от неразрешенного использования блокировкой клавиатуры или эквивалентным средством управления, например, доступ по паролю, когда они не используются (см. также 11.3.3).

Прочая информация

Оборудование, установленное в зонах пользователя, например, рабочие станции или файловые серверы, может потребовать особой защиты от неразрешенного доступа, когда оно остается работать без присмотра на длительный период.

11.3.3 Политика чистого стола и чистого экрана

Средство управления

Должны быть приняты политика чистого стола для бумаг и устройств хранения данных со съемным носителем и политика чистого экрана для средств обработки информации.

Руководство по реализации

Политика чистого стола и чистого экрана должны учитывать классификацию информации (см. 7.2), требования закона и договорные требования (см. 15.1), а также соответствующие риски и культурные аспекты организации. Должны быть рассмотрены следующие руководящие указания:

- a) уязвимая или критическая деловая информация, например, на бумаге или на электронном носителе, должна быть заперта (в идеале, в сейфе, в шкафу или в других формах надежной мебели), если она не требуется, особенно когда все ушли из офиса;
- b) компьютеры и терминалы должны быть оставлены в состоянии выполненного выхода из системы или с запирающим механизмом экрана или клавиатуры, управляемым паролем, маркером или подобным механизмом аутентификации пользователя, когда они находятся без присмотра, и должны быть защищены блокировкой клавиатуры, паролями или другими средствами управления, когда не используются;
- c) пункты работы с входящей и исходящей почтой и факсимильные аппараты, находящиеся без присмотра, должны быть защищены;
- d) неразрешенное использование фотокопировальных устройств и другой техники воспроизведения (например, сканеры, цифровые камеры), должно предотвращаться;
- e) документы, содержащие важную или секретную информацию, должны удаляться с принтеров немедленно.

Прочая информация

Политика чистого стола/чистого экрана снижает риски неразрешенного доступа, потери и повреждения информации в течение стандартного рабочего дня и в нерабочее время. Сейфы или другие формы безопасных средств хранения могут также защитить хранимую в них информацию от стихийных бедствий, таких как пожар, землетрясение, наводнение или взрыв.

Рассмотрите использование принтеров с функцией персонального идентификационного номера, чтобы создатель документа был единственным лицом, которое могло бы получить свою собственную распечатку, и только при нахождении около принтера.

11.4 Управления доступом в сеть

Цель: Предотвратить неразрешенный доступ к сетевым услугам.

Доступ как к внутренним, так и к внешним сетевым услугам должен управляться.

Доступ пользователя к сетям и сетевым услугам не должен подвергать риску безопасность сетевых услуг путем обеспечения следующего:

- a) между сетью организации, сетями, находящимися во владении других организаций, и общедоступными сетями установлены подходящие интерфейсы;
- b) подходящие механизмы аутентификации применяются к пользователям и оборудованию;
- c) приведено в исполнение управление доступом пользователей к информационным услугам.

11.4.1 Политика в отношении использования сетевых услуг

Средство управления

Пользователям должен быть предоставлен доступом только к тем услугам, которые им было конкретно разрешено использовать.

Руководство по реализации

Должна быть сформулирована политика, касающаяся использования сетей и сетевых услуг. Этот политика должен охватывать следующее:

- a) сети и сетевые услуги, к которым разрешен доступ;
- b) процедуры выдачи разрешения для определения того, кому и к каким сетям и сетевым услугам позволено иметь доступ;
- c) административные средства и процедуры для защиты доступа к сетевым соединениям и сетевым услугам;
- d) средства, используемые для доступа к сетям и сетевым услугам (например, условия разрешения наборного доступа к поставщику услуг Интернет или удаленной системе).

Политика в отношении использования сетевых услуг должна быть согласованной с деловой политикой управления доступом (см. 11.1).

Прочая информация

Неразрешенные и небезопасные подключения к сетевым услугам могут повлиять на целую организацию. Это средство управления особенно важно для сетевых подключений к уязвимым или критическим деловым приложениям или к

пользователям в зонах повышенного риска, например, общедоступные или внешние зоны, которые находятся за пределами управления защитой и контроля организации.

11.4.2 Аутентификация пользователя для внешних соединений

Средство управления

Для управления доступом удаленных пользователей должны использоваться подходящие методы аутентификации.

Руководство по реализации

Аутентификация удаленных пользователей может быть достигнута путем использования, например, методов, основанных на криптографии, аппаратных маркеров или протоколов с запросом и подтверждением. Возможные реализации таких методов можно найти в различных решениях на основе виртуальных частных сетей (VPN). Для обеспечения уверенности в источнике соединений также могут быть использованы специализированные частные линии связи.

Процедуры обратного соединения и средства управления обратным соединением, например, использующие модемы с посылкой обратного вызова, могут обеспечить защиту от неразрешенных и нежелательных подключений к средствам обработки информации организации. Этот тип управления аутентифицирует пользователей, пытающихся установить связь с сетью организации с удаленных мест. При использовании этого средства управления, организация не должна использовать сетевые услуги, которые включают в себя переадресацию вызовов, или, если сетевые услуги включают в себя переадресацию вызовов, они должны блокировать использование таких характеристик для того, чтобы избежать [возникновения] слабых мест, связанных с переадресаций вызова. Процесс обратного вызова должен гарантировать, что происходит фактическое разъединение на стороне организации. В противном случае, удаленный пользователь может держать линию открытой, притворяясь, что верификация обратного вызова произошла. Процедуры обратного вызова и средства управления обратным вызовом должны тщательно испытываться на наличие этой возможности.

Аутентификация узлов сети может послужить в качестве альтернативного средства аутентификации групп удаленных пользователей, если они подключены к безопасному, совместно используемому компьютерному комплексу. Для аутентификации узлов могут использоваться криптографические методы, например, основанные на машинных сертификатах. Они являются частью некоторых решений, основанных на VPN.

Дополнительные средства управления аутентификацией должны быть реализованы для управления доступом к беспроводным сетям. В частности, особая осторожность необходима при выборе средств управления для беспроводных сетей из-за большого количества возможностей для необнаруженного перехвата сетевого трафика и ввода в него.

Прочая информация

Внешние соединения дают возможность неразрешенного доступа к деловой информации, например, доступ при помощи методов вызова по номеру. Имеются различные типы методов аутентификации, некоторые из них обеспечивают больший уровень защиты, чем другие; например, криптографические методы могут обеспечить строгую аутентификацию. Важно определить, исходя из оценки рисков, необходимый уровень защиты. Это необходимо для подходящего выбора метода аутентификации.

Средство автоматического подключения к удаленному компьютеру может дать способ неразрешенного доступа к бизнес-приложению. Это особенно важно, если подключение использует сеть, которая находится за пределами действия организационной системы управления защитой.

11.4.3 Идентификация оборудования в сетях

Средство управления

Автоматическая идентификация оборудования должна быть рассмотрена как средство аутентификации подключений с конкретных мест и оборудования.

Руководство по реализации

Идентификация оборудования может использоваться, если важно, чтобы подключение могло быть инициировано только с определенного места или оборудования. Идентификатор внутри оборудования или прикрепленный к нему может использоваться для указания на то, разрешено ли этому оборудованию подключаться к сети. Эти идентификаторы должны четко указываться на то, к какой сети разрешено подключать оборудование, если существует больше одной сети, и особенно в том случае, если эти сети обладают различающейся важностью. Может быть необходимым рассмотреть физическую защиту оборудования для того, чтобы поддержать защиту идентификатора оборудования.

Прочая информация

Это средство управления может быть дополнено другими методами аутентификации оборудования пользователя (см. 11.4.2). Идентификация оборудования может применяться в дополнение к аутентификации пользователя.

11.4.4 Защита удаленных диагностических и конфигурационных портов

Средство управления

Физический и логический доступ к диагностическим и конфигурационным портам должен управляться.

Руководство по реализации

Возможные средства управления для доступа к диагностическим и конфигурационным портам включают использование блокировки клавиатуры и вспомогательные процедуры для того, чтобы управлять физическим доступом к порту. Примером такой вспомогательной процедуры является проверка того, что диагностические и конфигурационные порты доступны только путем размещения между менеджером компьютерной услуги и вспомогательным персоналом аппаратных средств/программного обеспечения, требующим доступа.

Порты, услуги и аналогичные средства, установленные на компьютерном или сетевом комплексе, которое не особо требуется для деловой функциональности, назначения, должны быть заблокированы или удалены.

Прочая информация

Множество компьютерных систем, сетевых систем и систем связи устанавливаются удаленным диагностическим или средством конфигурации для использования эксплуатационными инженерами. Будучи незащищены, эти диагностические порты обеспечивают средства неразрешенного доступа.

11.4.5 Разделение в сетях

Средство управления

Группы информационных услуг, пользователей и информационные системы должны быть разделены в сетях.

Руководство по реализации

Одним из методов управления защитой больших сетей является разделение их на отдельные логические сетевые домены, например, домены внутренней сети организации и домены внешней сети, каждый из которых защищен определенным периметром безопасности. Дифференциальный комплект средств управления может применяться в различных логических сетевых доменах для дополнительного разделения сред сетевой безопасности, например, систем общего доступа, внутренних сетей и критических активов. Домены должны определяться на основе оценки рисков и различных требований защиты в каждом домене.

Такой сетевой периметр может быть реализован путем установки безопасного шлюза между двумя сетями, которые предстоит соединить, для того чтобы управлять доступом и информационным потоком между двумя доменами. Этот шлюз должен быть сконфигурирован так, чтобы фильтровать трафик между этими доменами (см. 11.4.6 и 11.4.7) и блокировать неразрешенный доступ в соответствии с организационной политикой управления доступом (см. 11.1). Примером такого типа шлюза является то, что обычно называется «брандмауэр». Другой метод разделения отдельных логических доменов состоит в том, чтобы ограничить доступ к сети путем использования виртуальных частных сетей для групп пользователей в рамках организации.

Сети также могут быть разделены, используя функциональные возможности сетевого устройства, например, IP-коммутация. Отдельные домены могут, следовательно, быть реализованы путем управления потоком данных в сети, используя возможности маршрутизации/коммутации, такие как список контроля доступа.

Критерии для разделения сетей на домены должны быть основаны на политике управления доступом и требованиях к доступу (см. 10.1), а также учитывать относительную стоимость и эксплуатационного влияния внедрения подходящей сетевой маршрутизации или межсетевой технологии (см. 11.4.6 и 11.4.7).

Кроме того, разделение сетей должно быть основано на ценности и классификации информации, хранимой или обрабатываемой в сетях, степени доверия, или направлений деятельности для того, чтобы снизить общее влияние нарушения обслуживания.

Внимание должно быть уделено отделению беспроводных сетей от внутренних и частных сетей. Так как периметры беспроводных сетей хорошо не определены, то в таких случаях должна быть проведена оценка рисков для того, чтобы определить средства управления (например, строгая аутентификация, криптографические методы и частотная селекция) для поддержания сетевого разделения.

Прочая информация

Сети все больше и больше расширяются за традиционные организационные границы с образованием деловых партнерств, что может потребовать взаимозависимости или совместного использования средств обработки информации и обмена информацией. Такие расширения могут увеличить риск неразрешенного доступа к существующим информационным системам, которые используют сеть, некоторым из них может потребоваться защита от пользователей других сетей из-за их важности или критичности.

11.4.6 Управление сетевыми соединениями

Средство управления

Для совместно используемых сетей, особенно тех, которые расширяются за пределы границ организаций, возможность пользователей подключиться к сети должна быть ограничена, в соответствии с политикой управления доступом и требованиями деловых приложений (см. 11.1).

Руководство по реализации

Права пользователей по доступу в сеть должны поддерживаться и обновляться, как требуется политикой управления доступом (см. 11.1.1).

Возможности подключения пользователей могут быть ограничены посредством сетевых шлюзов, которые фильтруют трафик посредством предопределенных таблиц или правил. Примерами приложений, к которым должны быть применены ограничения, являются:

- a) обмен сообщениями, например, электронная почта;
- b) передача файлов;
- c) интерактивный доступ;
- d) доступ к прикладным программам.

Должно быть рассмотрено связывание прав доступа в сеть с определенным временем дня или датами.

Прочая информация

Внедрение средств управления для ограничения возможности подключения пользователей может требоваться политикой управления доступом для совместно используемых сетей, особенно тех, которые расширяются за границы организации.

11.4.7 Управление сетевой маршрутизацией

Средство управления

Средства управления маршрутизацией должны быть реализованы для сетей для того, чтобы обеспечить, что компьютерные соединения и информационные потоки не нарушают политику управления доступом деловых приложений.

Руководство по реализации

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

Шлюзы безопасности могут использоваться для валидации источника и адреса назначения в административных консолях внутренних и внешних сетей, если задействованы технологии трансляции сетевых адресов и/или адресов proxy-серверов. Те, кто осуществляет реализацию, должны отдать себе отчет о сильных сторонах и слабых сторонах любых используемых механизмов. Требования к управлению сетевой маршрутизацией должны основываться на политике управления доступом (см. 11.1).

Прочая информация

Совместно используемые сети, особенно те, которые расширяются за пределы границ организаций, могут потребовать дополнительных средств управления маршрутизацией. В особенности это относится к тем случаям, когда сети используются совместно с пользователями третьей стороны (не из организации).

11.5 Управление доступом к операционной системе

Цель: Предотвратить неразрешенный доступ к операционным системам.

Средства защиты должны использоваться для того, чтобы ограничить доступ к операционным системам полномочными пользователями. Средства должны быть способны делать следующее:

- a) аутентифицировать полномочных пользователей, в соответствии с определенной политикой управления доступом;
- b) записывать успешные и неудачные попытки аутентификации при входе в систему;
- c) записывать использование специальных системных привилегий;
- d) выдавать сигналы тревоги, когда нарушается политика в области защиты;
- e) обеспечивать подходящие средства для аутентификации;
- f) если это необходимо, ограничивать время соединения пользователей.

11.5.1 Безопасные процедуры входа в систему

Средство управления

Доступ к операционным системам должен управляться безопасной процедурой входа в систему.

Руководство по реализации

Процедура входа в операционную систему должна быть разработана так, чтобы минимизировать возможность неразрешенного доступа. Процедура входа в систему должна, следовательно, раскрывать минимум информации о системе для того, чтобы избежать предоставления неполномочному пользователю любой необязательной помощи. Хорошая процедура входа в систему должна делать следующее:

- a) не отображать идентификаторы системы или приложения до тех пор, пока процесс входа в систему не будет успешно завершен;
- b) отображать сообщение общего характера, предупреждающее, что доступ к компьютеру должен осуществляться только полномочными пользователями;
- c) не предоставлять сообщений-подсказок в ходе процедуры входа в систему, которые помогут неполномочному пользователю;
- d) осуществлять валидацию информации входа в систему только по окончании ввода всех входных данных. Если возникает состояние ошибки, то система не должна указывать, какая часть данных является правильной или неправильной;

- e) ограничивать число разрешенных неудачных попыток входа в систему, например, до трех попыток, и рассмотреть следующее:
 - 1) запись неудачных и удачных попыток;
 - 2) принудительная установка временной задержки до того, как будут разрешены новые попытки входа в систему, или отклонение дальнейших попыток без специального разрешения;
 - 3) разъединение каналов передачи данных;
 - 4) отправка сообщения об аварийной ситуации на пульт управления системой, если достигнуто максимальное число попыток входа в систему;
 - 5) установление числа повторных наборов пароля вместе с минимальной длиной пароля и ценностью защищаемой системы;
- f) ограничивать максимальное и минимальное время, допускаемое для процедуры входа в систему. Если оно превышено, то система должна прекратить осуществление процесса входа в систему;
- g) отображать следующую информацию по завершении успешного входа в систему:
 - 1) дата и время предыдущего успешного входа в систему;
 - 2) подробности любых неудачных попыток входа в систему с момента последнего успешного входа в систему;
- h) не отображать вводимый пароль или продумать скрывание знаков пароля символами;
- i) не передавать пароли открытым текстом по сети.

Прочая информация

Если пароли передаются открытым текстом во время входа в систему по сети, то они могут быть захвачены сетевой программой-разведчиком.

11.5.2 Идентификация и аутентификация пользователей

Средство управления

Все пользователи должны иметь уникальный идентификатор (идентификатор [ID] пользователя) исключительно для личного использования, и должна быть подходящая методика аутентификации для доказательства заявленной личности пользователя.

Руководство по реализации

Это средство управления должно применяться для всех типов пользователей (включая вспомогательный технический персонал, операторов, сетевых администраторов, системных программистов и администраторов баз данных).

Идентификаторы пользователей должны использоваться для того, чтобы прослеживать деятельность несущих ответственность лиц. Деятельность обычных пользователей не должна осуществляться с привилегированных учетных записей.

В исключительных обстоятельствах, когда имеется очевидная польза для дела, можно использовать совместно используемый идентификатор пользователя для группы пользователей или для конкретной работы. Для таких случаев должна иметься документально подтвержденная санкция руководства. Могут потребоваться дополнительные средства для того, чтобы поддержать возможность учета.

Общие идентификаторы для использования [отдельным] лицом допускаться только тогда, когда доступные идентификатору функции либо выполняемые идентификатором действия не должны быть прослеживаемы (например, доступ только для чтения), или имеются другие средства управления (например, пароль для общего идентификатора выдается только одному сотруднику в данный момент времени, и этот факт регистрируется).

Там где требуется строгая аутентификация и верификация идентичности, должны использоваться методы, альтернативные паролям, такие как криптографические средства, смарт-карты, маркеры или биометрические средства.

Прочая информация

Пароли (см. также 11.3.1 и 11.5.3) являются наиболее общим способом обеспечения идентификации и аутентификации на основании секрета, который знает только пользователь. Того же самого также можно достичь криптографическими средствами и протоколами аутентификации. Строгость идентификации и аутентификации пользователя должна соответствовать важности информации, к которой будет предоставлен доступ.

Объекты, такие как маркеры с памятью или смарт-карты, которыми обладают пользователи, также могут использоваться для идентификации и аутентификации. Для аутентификации личности человека также могут использоваться биометрические технологии аутентификации, которые используют уникальные характеристики или атрибуты человека. Надежно связанная комбинация технологий и механизмов даст в результате более строгую аутентификацию.

11.5.3 Система менеджмента паролей

Средство управления

Системы для осуществления менеджмента паролей должны быть интерактивными и должны обеспечивать качественные пароли.

Руководство по реализации

Система менеджмента паролей должна:

- a) обязывать к использованию личных идентификаторов и паролей пользователя для того, чтобы поддерживать ведение учета;
- b) позволять пользователям выбирать и изменять свои собственные пароли и включать процедуру подтверждения для того, чтобы учесть ошибки ввода;
- c) обязывать к выбору качественных паролей (см. 11.3.1);
- d) обязывать к изменениям пароля (см. 11.3.1);
- e) принуждать пользователей изменять временные пароли при первом входе в систему (см. 11.2.3);
- f) поддерживать запись предыдущих паролей пользователя и предотвращать повторное использование;
- g) не отображать пароли на экране при их вводе;
- h) хранить файлы с паролями отдельно от данных прикладной системы;
- i) хранить и передавать пароли в защищенной форме (например, зашифрованными или хешированными).

Прочая информация

Пароли являются одним из главных средств осуществления валидации полномочий пользователя иметь доступ к компьютерной услуге.

Некоторые приложения требуют, чтобы пароли пользователя были назначены независимым органом; в таких случаях, пункты b), d) и e) вышеприведенных руководящих указаний не применяются. В большинстве случаев пароли выбираются и поддерживаются пользователями. Руководящие указания по использованию паролей см. в разделе 11.3.1.

11.5.4 Использования системных утилит

Средство управления

Использование утилит, которые могут игнорировать средства управления системой и приложениями, должно быть ограничено и должно строго контролироваться.

Руководство по реализации

Должны быть рассмотрены следующие руководящие указания по использованию системных утилит:

- a) использование процедур идентификации, аутентификации и выдачи разрешения для системных утилит;
- b) отделение системных утилит от прикладных программ;
- c) ограничение использования системных утилит до минимального целесообразного числа надежных, полномочных пользователей (см. также 11.2.2);
- d) разрешение для специального использования системных утилит;
- e) ограничение доступности системных утилит, например, на срок действия разрешенного изменения;
- f) регистрация всех эпизодов использования системных утилит;
- g) определение и документальное подтверждение уровней полномочий для системных утилит;
- h) удаление или блокировка всех необязательных программно-реализованных утилит и системного программного обеспечения;
- i) обеспечение недоступности системных утилит для пользователей, которые имеют доступ к приложениям в системах, где требуется разделение обязанностей.

Прочая информация

Большинство компьютерных установок имеют одну или более системных утилит, которые могут быть способны игнорировать средства управления системой и приложениями.

11.5.5 Блокировка сеанса по превышению лимита времени [тайм-аут]

Средство управления

Неактивные сеансы должны быть закрыты по истечении определенного периода бездействия.

Руководство по реализации

Средство блокировки должно очищать экран сеанса, а также, возможно позже, закрывать как приложения, так и сеансы работы в сети по истечении определенного периода бездействия. Значение лимита времени должно отражать риски для защиты зоны, классификацию информации, с которой осуществляется работа, и

используемые приложения, а также риски, связанные с пользователями оборудования.

Для некоторых систем может быть предусмотрена ограниченная форма средства блокировки, которая очищает экран и предотвращает неразрешенный доступ, но не закрывает приложения или сеансы работы в сети.

Прочая информация

Это средство управления особенно важно в местах повышенного риска, которые включают общедоступные или внешние зоны за пределами управления защищкой организации. Сеансы должны закрываться для того, чтобы предотвратить доступ неполномочными лицами и воздействия, вызывающие отказ в обслуживании законных пользователей.

11.5.6 Ограничение времени соединения

Средство управления

Ограничения на время соединения должны использоваться для обеспечения дополнительной защиты для приложений с высокой степенью риска.

Руководство по реализации

Для важных компьютерных приложений должны быть продуманы средства управления временем соединения, особенно при подключении с мест с высокой степенью риска, например, общедоступные или внешние зоны, которые находятся за пределами управления защищкой организации. Примеры таких ограничений включают следующее:

- a) использование преопределенных отрезков времени, например, для передач командного файла, или кратковременных нормальных интерактивных сеансов;
- b) ограничение времени соединения обычным рабочим временем, если нет требования к работе в сверхурочное или в продленное время;
- c) предусмотреть повторную аутентификацию в рассчитанные по времени промежутки времени.

Прочая информация

Ограничение периода, в ходе которого разрешены подключения к компьютерным услугам, уменьшает «окно возможностей» неразрешенного доступа. Ограничение продолжительности активных сеансов оберегает пользователей от того, чтобы оставлять сеансы открытыми с целью избежать повторной аутентификации.

11.6 Управление доступом к приложениям и информации

Цель: Предотвратить неразрешенный доступ к информации, содержащейся в прикладных системах.

Средства защиты должны использоваться для того, чтобы ограничить доступ к прикладным системам и в пределах прикладных систем.

Логический доступ к прикладному программному обеспечению и информации должен ограничиваться полномочными пользователями.

Прикладные системы должны:

- a) управлять доступом пользователя к информационным и прикладным системным функциям, в соответствии с определенной политикой управления доступом;
- b) обеспечивать защиту от неразрешенного доступа, осуществляемого любой утилитой, программным обеспечением операционной системы и злонамеренным программным обеспечением, которые способны игнорировать или обойти средства управления системой или приложением;
- c) не подвергать риску другие системы, совместно с которыми используются информационные ресурсы.

11.6.1 Ограничение доступа к информации

Средство управления

Доступ к функциям информационной и прикладной системы, осуществляемый пользователями и вспомогательным персоналом, должен быть ограничен в соответствии с определенной политикой управления доступом.

Руководство по реализации

Ограничения на доступ должны быть основаны на требованиях отдельных бизнес-приложений. Политика управления доступом также должна быть согласованной с организационной политикой в области предоставления доступа (см. раздел 11.1).

Для того чтобы поддерживать требования ограничения доступа, должно быть предусмотрено применение следующих руководящих указаний:

- a) предоставление меню для того, чтобы управлять доступом к функциям прикладной системы;
- b) управление правами доступа пользователей, например, чтение, запись, удаление и исполнение;
- c) управление правами доступа других приложений;

- d) обеспечение того, чтобы выходные данные прикладных систем, работающих с важной информацией, содержали только ту информацию, которая значима для использования выходных данных, и посыпались только на разрешенные терминалы и места; сюда должен быть включен периодический анализ таких выходных данных с целью обеспечения удаления излишней информации.

11.6.2 Изоляция важных систем

Средство управления

Важные системы должны иметь выделенную (изолированную) компьютерную среду.

Руководство по реализации

Для изоляции важных систем должны быть рассмотрены следующие пункты:

- a) важность прикладной системы должна быть четко определена и документально подтверждена владельцем приложения (см. 7.1.2);
- b) если важное приложение должно работать в совместно используемой среде, то прикладные системы, совместно с которыми ему предстоит использовать ресурсы, и соответствующие риски должны быть выявлены и приняты владельцем важного приложения.

Прочая информация

Некоторые прикладные системы важны в том, что касается возможной потери настолько, что они требуют особого обращения. Важность может указывать на то, что прикладная система:

- a) должна работать на выделенном компьютере; или
- b) должно совместно использовать ресурсы только с надежными системами прикладными системами.

Изоляция может быть достигнута путем использования физических или логических методов (см. также 11.4.5).

11.7 Мобильная обработка и телеобработка

Цель: Обеспечить защиту информации при использовании средств мобильной обработки и телеобработки.

Требуемая защита должна быть соразмерна с рисками этих особых способов стиля работы. При использовании мобильной обработки, должны быть рассмотрены риски работы в незащищенной среде, и должна применяться надлежащая защита. В случае телеобработки организация должна применять защиту к месту телеобработки и обеспечивать наличие подходящих мероприятий для этого метода работы.

11.7.1 Мобильная обработка и связь

Средство управления

Должны быть приняты официальная политика и надлежащие меры безопасности для защиты от рисков использования средств мобильной обработки и связи.

Руководство по реализации

При использовании средств мобильной обработки и связи, например, ноутбуков, карманных компьютеров, смарт-карт и мобильных телефонов, особая забота должна быть проявлена для обеспечения того, чтобы деловая информация не была раскрыта. Политика в области мобильной обработки должна учитывать риски работы с оборудованием для мобильной обработки в незащищенных средах.

Политика в области мобильной обработки должна включать в себя требования к физической защите, средствам управления доступом, методам шифрования, резервному копированию и защите от вирусов. Эта политика также должна включать в себя правила и советы по подключению мобильных средств к сети и руководящие указания по использованию этих средств в общедоступных местах.

При использовании средств мобильной обработки в общественных местах, конференц-залах в других незащищенных зонах вне помещений организации должна быть проявлена особая осторожность. Должна иметься защита для того, чтобы избежать неразрешенного доступа к информации или раскрытия информации, хранящейся и обрабатываемой этими средствами, например, путем использования криптографических методов (см. 12.3).

Пользователи средств мобильной обработки в общедоступных местах должны проявлять осторожность для того, чтобы избежать риска подсматривания посторонними лицами. Процедуры, направленные против злонамеренного программного обеспечения, должны быть приняты и должны обновляться (см. 10.4).

Резервное копирование критической деловой информации должно осуществляться регулярно. Должно быть доступным оборудование для того, чтобы создать возможность для быстрого и легкого резервного копирования информации. Этим копиям должна быть обеспечена надлежащая защита, например, от кражи или потери информации.

Подходящая защита должна быть обеспечена для использования мобильных средств, подключенных к сетям. Удаленный доступ к деловой информации через общедоступную сеть, используя средства мобильной обработки, должен происходить только после успешной идентификации и аутентификации, и при наличии подходящих механизмов управления доступом (см. 11.4).

Средства мобильной обработки также должны быть физически защищены от кражи, особенно тогда, когда они оставляются, например, в автомобилях и других формах транспорта, комнатах отелей, конференц-центрах и местах для встреч. Для случаев кражи или утери средств мобильной обработки должна быть принята специальная процедура, учитывающая юридические, страховые и другие требования защиты организации. Оборудование, несущее в себе значимую, важную и/или критическую деловую информацию не должно оставаться без присмотра и, где возможно, должно физически запираться, или же должны быть использованы специальные замки для защиты оборудования (см. 9.2.5).

Для персонала, использующего мобильную обработку, должна быть организована подготовка, с целью улучшить их осведомленность о дополнительных рисках, проистекающих из этого метода работы, и о средствах управления, которые должны быть реализованы.

Прочая информация

Беспроводные соединения с мобильными сетями подобны другим типам сетевых соединений, но имеют важные различия, которые должны быть учтены при определении средств управления. Типичные отличия таковы:

- a) некоторые протоколы защиты беспроводных соединений являются незрелыми и имеют известные слабые места;
- b) резервная копия информации, хранящейся на мобильных компьютерах, может не создаться из-за ограниченной полосы пропускания и/или потому что мобильное оборудование может не быть подключенным во все моменты времени, на которые запланировано резервное копирование.

11.7.2 Телеобработка

Средство управления

Для деятельности по телеобработке должны быть разработаны и реализованы политика, эксплуатационные планы и процедуры.

Руководство по реализации

Организации должны разрешать деятельность по телеобработке только в том случае, если они убеждены в том, что имеются подходящие меры безопасности и средства управления, и что они соответствуют политике организации в области защиты.

Должна иметься подходящая защита места телеборотки, например, от кражи оборудования и информации, неразрешенного раскрытия информации, неразрешенного удаленного доступа к внутренним системам организации или от неправильного использования средств. Деятельность по телеборотке должна быть и разрешена, и управляема руководством, и должно быть обеспечено наличие подходящих мероприятий для этого способа работы.

Должны быть рассмотрены следующие вопросы:

- a) существующая физическая защита места телеборотки, принимая во внимание физическую защиту здания и местное окружение;
- b) предлагаемая физическая среда телеборотки;
- c) требования защиты связи, принимая во внимание потребность в удаленном доступе к внутренним системам организации, уязвимость информации, к которой будет осуществляться доступ, и которая будет проходить через каналы связи, а также уязвимость внутренней системы;
- d) угроза неразрешенного доступа к информации или ресурсам от других лиц, использующих жилье, например, семьи и друзей;
- e) использование домашних сетей и требования или ограничения на конфигурацию услуг беспроводной сети;
- f) политика и процедуры для предотвращения разногласий, касающихся прав на интеллектуальную собственность, разработанной на оборудовании, находящемся в частной собственности;
- g) доступ к оборудованию, находящемуся в частной собственности (для того чтобы проверить защиту машины или в ходе расследования), который может не допускаться законодательством;
- h) соглашения о лицензировании программного обеспечения, которые таковы, что организации могут стать ответственными за лицензирование клиентского программного обеспечения на рабочих станциях, находящихся в собственности служащих, подрядчиков или пользователей третьей стороны;
- i) требования к антивирусной защите и брандмаузеру.

Руководящие указания и меры, которые надо рассмотреть, должны включать следующее:

- a) предоставление подходящего оборудования и мебели для хранения для деятельности по телеборотке, если использование оборудования, находящегося в частной собственности, которое не находится под управлением организации, не допускается;

- b) определение позволенной работы, часов работы, классификации информации, которая может сохраняться, и внутренних систем и услуг, к которым надомнику⁸ разрешено иметь доступ;
- c) предоставление подходящего оборудования связи, включая методы защиты удаленного доступа;
- d) физическая защита;
- e) правила и руководящие указания по доступу членов семьи и посетителей к оборудованию и информации;
- f) предоставление аппаратной и программной поддержки и сопровождения;
- g) предоставление страховки;
- h) процедуры для резервного копирования и обеспечения непрерывности бизнеса;
- i) аудит и постоянный контроль защиты;
- j) отмена полномочий и прав доступа, и возврат оборудования при прекращении деятельности по телеобработке.

Прочая информация

Телеобработка использует технику связи для того, чтобы позволить персоналу работать на удалении с фиксированного местоположения за пределами их организации.

⁸ надомник [teleworker] — работник, получающий задания по телефону или электронной почте (Прим. переводчика)

12 Приобретение, разработка и обслуживание информационных систем

12.1 Требования защиты информационных систем

Цель: Гарантировать, что защита является неотъемлемой частью информационных систем.

Информационные системы включают операционные системы, инфраструктуру, бизнес-приложения, готовые продукты, услуги, а также приложения, разработанные пользователем. Проектирование и реализация информационных систем, поддерживающих деловой процесс, могут быть решающими для защиты. Перед разработкой и/или реализацией информационных систем должны быть определены и согласованы требования защиты.

Все требования защиты должны быть выявлены на стадии определения требований проекта и обоснованы, согласованы и документально подтверждены как часть общего экономического обоснования проекта для информационной системы.

12.1.1 Анализ и спецификация требований защиты

Средство управления

Формулировки деловых требований для новых информационных систем, или улучшения существующих информационных систем должны специфицировать требования для средств управления защитой.

Руководство по реализации

Спецификация требований для средств управления должна учитывать автоматизированные средства управления, которые предстоит внедрить в информационную систему, и потребности во вспомогательных ручных средствах управления. Аналогичные соображения должны учитываться при оценке пакетов программ, разрабатываемых или приобретаемых для бизнес-приложений.

Требования защиты и средств управления должны отражать деловую ценность вовлеченных информационных активов (см. также 7.2) и возможный ущерб для бизнеса, который может произойти в результате сбоя в защите или отсутствия защиты.

Системные требования для защиты информации и процессов реализации защиты должны быть интегрированы на ранних стадиях проектирования информационных систем. Средства управления, введенные на стадии проектирования, значительно дешевле для реализации и обслуживания, нежели те, которые включены в ходе реализации или после реализации.

Если продукты приобретаются, то необходимо следовать официальному процессу испытания и приобретения. В договорах с поставщиком должны быть оговорены определенные требования защиты. Если функциональность защиты в предлагаемом продукте не удовлетворяет установленным требованиям, тогда привносимый риск и связанные с ним средства управления должны быть пересмотрены до приобретения продукта. Если дополнительное функциональные возможности поставляются и являются причиной риска для системы защиты, то они должны быть блокированы, или предлагаемая схема управления должна быть просмотрена, с целью определить, может ли быть извлечено преимущество из имеющейся улучшенной функциональности.

Прочая информация

Если это будет сочтено уместным, например, по причине стоимости, руководство может захотеть использовать независимо оцененные и сертифицированные продукты. Дополнительную информацию о критериях оценки для средств защиты в области информационных технологий можно найти в ISO/IEC 15408 или в других стандартах по оценке или сертификации, по обстоятельствам.

В техническом отчете ISO/IEC TR 13335-3 даны руководящие указания по использованию процессов менеджмента рисков для определения требований для средств управления защитой.

12.2 Правильная обработка в приложениях

Цель: Предотвратить ошибки, потерю, неразрешенную модификацию или неправильное использование информации в приложениях.

Для обеспечения правильной обработки в приложениях, включая приложения, разработанные пользователем, должны быть спроектированы подходящие средства управления. Эти средства управления должны включать валидацию входных данных, внутренней обработки и выходных данных.

Дополнительные средства управления могут быть необходимы для систем, которые обрабатывают важную, ценную или критическую информацию, или имеют влияние на такую информацию. Такие средства управления должны быть определены на основе требований защиты и оценки рисков.

12.2.1 Валидация входных данных

Средство управления

Должна осуществляться валидация данных, вводимых в приложения, с целью гарантировать, что эти данные являются правильными и уместными.

Руководство по реализации

Проверки должны применяться к входным данным деловых сделок, неизменным данным (например, имена и адреса, кредитные лимиты, номера заказов

потребителей) и таблицы параметров (например, продажные цены, курсы пересчета валют, налоговые ставки). Должны быть рассмотрены следующие руководящие указания:

- a) двойной ввод или другие проверки входных данных, такие как граничные проверки или ограничение полей конкретными диапазонами входных данных для того, чтобы обнаруживать следующие ошибки:
 - 1) значения вне диапазона;
 - 2) неверные символы в полях данных;
 - 3) пропущенные или неполные данные;
 - 4) превышение верхних и нижних пределов объема данных;
 - 5) неразрешенные или противоречивые контрольные данные;
- b) периодический анализ содержимого ключевых областей или файлов данных для того, чтобы подтвердить их достоверность и целостность;
- c) контроль твердых копий входных документов на предмет каких-либо неразрешенных изменений (все изменения во входных документах должны быть разрешены);
- d) процедуры для реакции на ошибки, выявленные валидацией;
- e) процедуры для проверки правдоподобия входных данных;
- f) определение обязанностей всего персонала, вовлеченного в процесс ввода данных;
- g) создание журнала регистрации деятельности, связанной с процессом ввода данных (см. 10.10.1).

Прочая информация

Можно рассмотреть автоматическое обследование и валидацию входных данных, если это применимо, для того, чтобы снизить риски ошибок и предотвратить стандартные атаки, включая переполнение буфера и введение кода.

12.2.2 Управление внутренней обработкой

Средство управления

В приложения должны быть встроены валидационные проверки, с целью предотвратить любую порчу информации вследствие ошибок обработки или умышленных действий.

Руководство по реализации

Проектирование и реализация приложений должны обеспечивать, чтобы риски сбоев в обработке, приводящие к потере целостности, были минимизированы. Конкретные области, которые надо рассмотреть, включают следующее:

- a) использование функций добавления, модификации и удаления для того, чтобы осуществлять изменения в данных;
- b) процедуры для предотвращения работы программы в неправильном порядке или работы после сбоя предыдущей обработки (см. также 10.1.1);
- c) использование подходящих программ для того, чтобы восстанавливаться после сбоев, с целью обеспечить правильную обработку данных;
- d) защита от атак, использующих перегрузку/переполнение буфера.

Должны быть подготовлены подходящие контрольные листы, деятельность должна быть документально подтверждена, а результаты должны быть сохранены защищенными. Примеры проверок, которые можно встроить, включают следующее:

- a) средства управления соединениями или пакетами для того, чтобы согласовать сальдо файлов данных после обновления сделок;
- b) средства управления сальдо для того, чтобы проверять начальное сальдо по отношению к предыдущему конечному сальдо, а именно:
 - 1) средства управления от выполнения к выполнению [run-to-run];
 - 2) итоговые данные обновлений файла;
 - 3) средства управления от программы к программе [program-to-program];
- c) валидация входных данных, создаваемых системой (см. 12.2.1);
- d) проверки на целостность, аутентичность или какую-либо другую характеристику защиты данных или программного обеспечения, загружаемых или подкачиваемых между центральными и удаленными компьютерами;
- e) контрольные суммы записей и файлов;
- f) проверки для обеспечения того, чтобы прикладные программы выполнялись в правильное время;
- g) проверки для обеспечения того, чтобы программы выполнялись в правильном порядке, чтобы их выполнение прекращалось в случае сбоя, и чтобы дальнейшая обработка была остановлена до тех пор, пока проблема не будет решена;
- h) создание журнала регистрации действий, связанных с обработкой (см. 10.10.1).

Прочая информация

Данные, которые были введены правильно, могут быть повреждены аппаратными ошибками, ошибками обработки или вследствие преднамеренных действий. Необходимые валидационные проверки будут зависеть от характера приложения и делового влияния любого повреждения данных.

12.2.3 Целостность сообщений

Средство управления

Должны быть определены требования к обеспечению аутентичности и защите целостности сообщений в приложениях, и должны быть определены и реализованы соответствующие средства управления.

Руководство по реализации

Должна выполняться оценка рисков для защиты, с целью определить, требуется ли целостность сообщения, и выявить наиболее подходящие методы реализации.

Прочая информация

Криптографические методы (см. 12.3), могут использоваться как подходящие средства реализации аутентификации сообщений.

12.2.4 Валидация выходных данных

Средство управления

Должна осуществляться валидация вывода данных из приложения, с целью обеспечить, что обработка хранимой информации является правильной и соответствующей обстоятельствам.

Руководство по реализации

Валидация выходных данных может включать в себя следующее:

- a) проверки правдоподобности для того, чтобы выяснить, являются ли выходные данные корректными;
- b) согласование счетчика команд для обеспечения обработки всех данных;
- c) предоставление считывателю или последующей системе обработки достаточной информации для того, чтобы определить правильность, полноту, точность и классификацию информации;
- d) процедуры реагирования на валидационные испытания выходных данных;
- e) определение обязанностей всего персонала, вовлеченного в процесс вывода данных;

- f) создание протокола деятельности в процессе валидации вывода данных.

Прочая информация

Обычно, системы и приложения создаются на том предположении, что, пройдя надлежащую валидацию, верификацию и испытание, документально подтверждение, проверку и тестируя, выходные данные всегда будут правильными. Тем не менее, это предположение не всегда верно; т.е. системы, которые были испытаны, все еще могут при некоторых обстоятельствах выдать неправильные выходные данные.

12.3 Криптографические средства управления

Цель: Защищать конфиденциальность, аутентичность или целостность информации криптографическими средствами.

Должна быть разработана политика по использованию криптографических средств управления. Для того чтобы поддерживать использование криптографических методов, должно осуществляться распределение ключей.

12.3.1 Политика по использованию криптографических средств управления

Средство управления

Должна быть разработана и реализована политика по использованию криптографических средств управления для защиты информации.

Руководство по реализации

При разработке криптографической политики должно быть рассмотрено следующее:

- a) подход руководства к использованию криптографических средств управления по всей организации, включая общие принципы, в соответствии с которыми должна защищаться деловая информация (см. также 5.1.1);
- b) на основе оценки рисков должен быть определен необходимый уровень защиты, с учетом типа, строгости и качества требуемого шифровального алгоритма;
- c) использование шифрования для защиты важной информации, переносимой мобильными или сменными носителями, устройствами или через линии связи;
- d) подход к распределению ключей, включая методы для работы с защитой криптографических ключей и восстановление зашифрованной информации в случае потерянных, раскрытых или поврежденных ключей;
- e) роли и обязанности, например, кто отвечает за следующее:
 - 1) реализация политики;

- 2) распределение ключей, включая генерирование ключей (см. также 12.3.2);
 - f) стандарты, которые предстоит принять для результативной реализации по всей организации (для какого делового процесса какое решение используется);
 - g) влияние использования зашифрованной информации на средства управления, которые зависят от контроля содержимого (например, обнаружение вирусов).

При реализации организационной политики в области криптографии, внимание должно быть уделено нормам и государственным ограничениям, которые могут относиться к использованию криптографических методов в разных частях мира и к вопросам потока закодированной информации через границу (см. также 15.1.6).

Криптографические средства управления могут использоваться для достижения других целей защиты, например, следующих:

- a) конфиденциальность: использование шифрования информации для защиты важной или критической информации, как хранимой, так и передаваемой;
- b) целостность/аутентичность: использование цифровых подписей или кодов аутентификации сообщений для защиты аутентичности и целостности хранимой или передаваемой важной или критической информации;
- c) неотрекаемость: использование криптографических методов для того, чтобы получить доказательство того, имело место событие или действие, или нет.

Прочая информация

Принятие решения по вопросу того, уместно ли криптографическое решение, должно рассматриваться как часть более широкого процесса оценки рисков и выбора средств управления. Эта оценка может затем быть использована для определения того, уместно ли криптографическое средство управления, какой тип средства управления должен быть применен, для какой цели и для каких деловых процессов.

Политика по использованию криптографических средств управления необходима для того, чтобы извлечь максимум преимуществ и минимизировать риски использования криптографических методов, а также для того, чтобы избежать неуместного или неправильного использования. При использовании цифровых подписей, внимание должно быть уделено всем имеющим отношение к делу законам, в частности, законам, описывающим условия, при которых цифровая подпись юридически обязательна по закону (см. 15.1).

Надо прибегнуть к совету специалиста для того, чтобы определить подходящий уровень защиты и определить подходящие спецификации, которые обеспечат необходимую защиту и поддержат реализацию безопасной системы распределения ключей (см. также 12.3.2).

Подкомитет ISO/IEC JTC1 ПК27 разработал несколько стандартов, связанных с криптографическими средствами управления. Дополнительную информацию также можно найти в документах IEEE P1363 и в OECD *Guidelines on Cryptography*.

12.3.2 Распределение ключей

Средство управления

Для поддержки использования организацией криптографических методов должно иметься распределение ключей.

Руководство по реализации

Все криптографические ключи должны быть защищены от модификации, потери и разрушения. Кроме того, секретным и личным ключам нужна защита от неразрешенного раскрытия. Оборудование, используемое для того, чтобы генерировать, хранить и архивировать ключи, должно быть физически защищено.

Система распределения ключей должна быть основана на согласованном наборе стандартов, процедур и безопасных методов для следующего:

- a) генерирование ключей для различных криптографических систем и различных приложений;
- b) генерирование и получение сертификатов открытого ключа;
- c) раздача ключей предназначенным пользователям, включая то, как ключи должны быть активированы по получении;
- d) хранение ключей, включая то, как полномочные пользователи получают доступ к ключам;
- e) изменение или обновление ключей, включая правила касательно того, когда ключи должны меняться, и как это будет делаться;
- f) работа с раскрытыми ключами;
- g) аннулирование ключей, включая то, как ключи должны быть изъяты или дезактивированы, например, если ключи были раскрыты или если пользователь уходит из организации (в каком случае ключи также должны быть архивированы);
- h) восстановление ключей, которые потерялись или повредились, как часть менеджмента непрерывности бизнеса, например, для восстановления зашифрованной информации;
- i) архивирование ключей, например, для архивируемой информации или для информации, резервная копия которой создается;
- j) разрушение ключей;
- k) регистрация и аудит действий, связанных с распределением ключей.

Для того для того, чтобы снизить вероятность раскрытия, должны быть определены даты активизации и дезактивации для ключей, чтобы ключи можно было

использовать только в течение ограниченного периода времени. Этот период времени должен зависеть от обстоятельств, при которых используется криптографическое средство управления, и от воспринимаемого риска.

В дополнение к защищенному распределению секретных и частных ключей, также должна быть продумана аутентификация открытых ключей. Этот процесс аутентификации может быть осуществлен с использованием сертификатов открытого ключа, которые обычно выпускаются сертифицирующим органом, который должен быть признанной организацией с подходящими средствами управления и принятыми процедурами для того, чтобы обеспечить необходимую степень доверия.

Содержание соглашений об уровне обслуживания или договоров с внешними поставщиками криптографических услуг, например, сертификационным органом, должно охватывать вопросы ответственности, надежности услуг и времени реагирования для предоставления услуг (см. 6.2.3).

Прочая информация

Распределение криптографических ключей существенно для результативного использования криптографических методов. ISO/IEC 11770 дает дополнительную информацию о распределении ключей. Два типа криптографических методов таковы:

- a) методы секретных ключей, когда две стороны или более совместно используют один и тот же ключ, и этот ключ используется как для шифровки, так и для дешифровки информации; этот ключ должен храниться в секрете, поскольку каждый, имеющий доступ к ключу, имеет возможность декодировать всю информацию, зашифрованную с этим ключом, или ввести неразрешенную информацию, используя ключ;
- b) методы открытых ключей, когда каждый пользователь имеет пару ключей, открытый ключ (который может быть открыт любому) и личный ключ (который должен держаться в секрете); методы открытых ключей могут использоваться для шифрования и создания цифровых подписей (см. также ISO/IEC 9796 и ISO/IEC 14888).

Имеется угроза подделки цифровой подписи путем замены открытого ключа пользователя. Эта проблема решается использованием сертификата открытого ключа.

Криптографические методы также могут использоваться для защиты криптографических ключей. Может понадобиться предусмотреть процедуры для обработки юридических запросов на доступ к криптографическим ключам, например, может понадобиться сделать зашифрованную информацию доступной в незашифрованном виде как доказательство в судебном деле.

12.4 Защита системных файлов

Цель: Обеспечить защиту системных файлов.

Доступ к системным файлам и исходному тексту программы должен управляться, а проектирование и вспомогательная деятельность в области информационных технологий должны осуществляться защищенным способом. Необходимо позаботиться о том, чтобы избежать раскрытия важных данных в испытательной среде.

12.4.1 Управление системным программным обеспечением

Средство управления

Должны быть приняты процедуры для управления установкой программного обеспечения в операционных системах.

Руководство по реализации

С целью минимизировать риски порчи для операционных систем, для управления изменениями должны быть рассмотрены следующие руководящие указания:

- a) обновление операционного программного обеспечения, приложений и библиотек программ должно выполняться только подготовленными администраторами с соответствующего разрешения руководства (см. 12.4.3);
- b) операционные системы должны сохранять только утвержденные выполняемые программы и не должны сохранять программы, находящиеся в разработке, или компиляторы;
- c) приложения и системное программное обеспечение должны реализовываться только после проведения всесторонних и успешных испытаний; испытания должны включать испытания на практичность, безопасность, влияние на другие системы и удобность для пользователя, и должны выполняться в отдельных системах (см. также 10.1.4); должно быть проведено обновление всех соответствующих библиотек исходных программ;
- d) система управления конфигурацией должна использоваться для того, чтобы сохранять контроль над всем реализованным программным обеспечением, а также системной документацией;
- e) должна быть принята стратегия отката⁹ прежде, чем будут реализовываться изменения;
- f) должен вестись контрольный журнал всех обновлений в библиотеках системных программ;

⁹ откат [rollback] – восстановление предыдущего состояния

- g) предыдущие версии прикладного программного обеспечения должны сохраняться на случай чрезвычайно ситуации;
- h) старые версии программного обеспечения должны сохраняться в архиве вместе со всей необходимой информацией и параметрами, процедурами, деталями конфигурации и вспомогательным программным обеспечением столько, сколько данные сохраняются в архиве.

Поставляемое поставщиком программное обеспечение, используемое в операционных системах, должно поддерживаться на уровне, поддерживаемом поставщиком. Со временем, программные поставщики перестанут поддерживать более старые версии программного обеспечения. Организация должна учесть риски, связанные с расчетом на неподдерживаемое программное обеспечение.

Любое решение о переходе к новой версии должно учитывать деловые требования к изменениям, а также защиту версии, т.е. введение новых функциональных возможностей в области защиты или серьезность проблем в области защиты, влияющих на эту версию. Должны применяться заплаты к программному обеспечению, если они могут помочь устранить или уменьшить слабые места защиты (см. также 12.6.1).

Физический или логический доступ должен предоставляться поставщикам только в целях поддержки, когда это необходимо, и с одобрения руководства. Деятельность поставщика должна постоянно контролироваться.

Компьютерное программное обеспечение может полагаться на программное обеспечение и модули, поставляемые извне, которые должны постоянно контролироваться и управляться для того, чтобы избежать неразрешенных изменений, которые могут привнести слабые места в защиту.

Прочая информация

Версия операционных систем должна меняться только тогда, когда есть требование сделать так, например, если текущая версия операционной системы больше не поддерживает деловые требования. Смена версий не должна происходить только потому, что стала доступной новая версия операционной системы. Новые версии операционных систем могут быть менее безопасными, менее стабильными и хуже понимаемыми, чем текущие системы.

12.4.2 Защита испытательных данных системы

Средство управления

Испытательные данные должны выбираться тщательно, и должны быть защищены и управляемы.

Руководство по реализации

Надо избегать использования рабочих баз данных, содержащих личную информационную или любую другую важную информацию, в целях испытания. Если

личная информация или информация, важная в другом отношении, используется в целях испытания, то все важные подробности и содержание должны быть удалены или модифицированы до неузнаваемости перед использованием. Следующие руководящие указания должны применяться для защиты рабочих данных, когда те используются в целях испытания:

- a) процедуры управления доступом, которые применяются к рабочим прикладным системам, должны также применяться к испытательным прикладным системам;
- b) должно быть отдельное разрешение всякий раз, когда рабочая информация копируется в испытательную прикладную систему;
- c) рабочая информация должна быть стерта с испытательной прикладной системы немедленно после того, как испытание будет завершено;
- d) копирование и использование рабочей информации должны быть зарегистрированы для того, чтобы обеспечить ведение контрольного журнала.

Прочая информация

Системное и приемочное испытание обычно требуют солидных объемов испытательных данных, которые близки к рабочим данным настолько, насколько это возможно.

12.4.3 Управления доступом к исходному коду программы

Средство управления

Доступ к исходному коду программы должен быть ограничен.

Руководство по реализации

Доступ к исходному коду программы и связанным элементам (таким как проекты, спецификации, планы верификации и планы валидации) должен строго управляться для того, чтобы предотвратить введение неразрешенных выполняемых функций и для того, чтобы избежать непреднамеренных изменений. Для исходного кода программы этого можно достичь путем управляемого центрального хранения такого кода, предпочтительно в библиотеках исходных программ. Затем должны быть рассмотрены следующие руководящие указания (см. также 11) для управления доступом к таким библиотекам исходных программ, с целью снизить возможность порчи компьютерных программ:

- a) где возможно, библиотеки исходных программ не должны содержаться в операционных системах;
- b) менеджмент исходного кода программ и библиотек исходных программ должен осуществляться согласно установленным процедурам;
- c) вспомогательный персонал не должен иметь неограниченный доступ к библиотекам исходных программ;

- d) обновление библиотек исходных программ и связанных элементов, а также выпуск программных источников программистам должен осуществляться только после того, как будет получено соответствующее разрешение;
- e) распечатки программ должны находиться в безопасной среде (см. 10.7.4);
- f) должен вестись контрольный журнал всех доступов к библиотекам исходных программ;
- g) сопровождение и копирование библиотек исходных программ должно подчиняться строгим процедурам управления изменениями (см. 12.5.1).

Прочая информация

Исходный код программы – это код, написанный программистами, который компилируется (и связывается) для того, чтобы создавать модули. Определенные языки программирования не проводят формального различия между исходным кодом и модулями, так как модули создаются в то время, когда они активируются.

Стандарты ИСО 10007 и ISO/IEC 12207 предоставляют дополнительную информацию о менеджменте конфигурации и процессе жизненного цикла программного обеспечения.

12.5 Защита в процессах разработки и вспомогательных процессах

Цель: Поддерживать защиту прикладного системного программного обеспечения и информации.

Среды проектирования и вспомогательные среды должно строго управляться.

Менеджеры, ответственные за прикладные системы, должны также быть ответственными за защиту среды проектирования или вспомогательной среды. Они должны обеспечивать, чтобы все предлагаемые изменения системы были проанализированы для того, чтобы обеспечить, что они не подвергают риску защиту или системы, или операционной среды.

12.5.1 Процедуры управления изменениями

Средство управления

Реализация изменений должна управляться путем использования официальных процедур управления изменениями.

Руководство по реализации

Официальные процедуры управления изменениями должны быть документально подтверждены и приведены в исполнение для того, чтобы минимизировать порчу информационных систем. Введение новых систем и существенных изменений в существующих системах должно подчиняться официальному процессу

документирования, спецификации, испытания, управления качеством и управляемой реализации.

Этот процесс должен включать оценку рисков, анализ влияний изменений, а также спецификации необходимых средств защиты. Этот процесс также должен обеспечивать, чтобы существующая защита и процедуры управления не подвергались риску, чтобы вспомогательным программистам был предоставлен доступ только в те части системы, которые необходимы для их работы, и чтобы официальное соглашение и утверждение для любого изменения были получены.

Если только это практически выполнимо, то прикладные и операционные процедуры управления изменениями должны быть интегрированы (см. также 10.1.2). Процедуры изменения должны включать в себя следующее:

- a) ведение записи согласованных уровней разрешения;
- b) обеспечение того, что изменения подаются полномочными пользователями;
- c) анализ средств управления и процедур [обеспечения] целостности с целью гарантировать, что изменения не подвергнут их риску;
- d) выявление всего программного обеспечения, информации, объектов баз данных и аппаратных средств, которые требуют поправок;
- e) получение официального утверждения для подробных предложений до того как работа начнется;
- f) обеспечение того, чтобы полномочные пользователи приняли изменения до реализации;
- g) обеспечение того, чтобы набор системной документации обновлялся по выполнении каждого изменения, и чтобы старая документация архивировалась или ликвидировалась;
- h) поддержание управления версиями для всех обновлений программного обеспечения;
- i) ведение контрольного журнала всех запросов на изменения;
- j) обеспечение того, чтобы операционная документация (см. 10.1.1) и процедуры, определяемые пользователем, были изменены, как необходимо, чтобы оставаться соответствующими;
- k) обеспечение того, чтобы реализация изменений происходила в правильное время и не мешала вовлеченным деловым процессам.

Прочая информация

Изменение программного обеспечения может повлиять на операционную среду.

Хорошая практика включает испытание нового программного обеспечения в среде, отделенной как от производственных сред, так и от сред разработки (см. также 10.1.4). Это обеспечивает контроль над новым программным обеспечением и дает возможность дополнительной защиты рабочей информации, которая используется в испытательных целях. Это должно включать в себя заплаты, служебные пакеты и другие обновления. Автоматизированные обновления не должны использоваться в критических системах, поскольку некоторые обновления могут вызвать сбой в критических приложениях (см. 12.6).

12.5.2 Технический анализ приложений после изменений операционной системы

Средство управления

Когда операционные системы меняются, деловые критические приложения должны анализироваться и испытываться, с целью гарантировать отсутствие неблагоприятного влияния на организационные операции или защиту.

Руководство по реализации

Этот процесс должен охватывать следующее:

- a) анализ процедур управления прикладными процессами и [обеспечения] целостности с целью гарантировать, что они не были подвергнуты риску изменениями операционной системы;
- b) обеспечение того, что годовой план поддержки и бюджет будут охватывать анализ и испытание системы, вытекающие из изменений операционной системы;
- c) обеспечение того, чтобы уведомление об изменениях операционной системы было предоставлено заблаговременно, с целью сделать возможным проведение надлежащих испытаний и анализа до реализации;
- d) обеспечение того, чтобы надлежащие изменения были сделаны в планах обеспечения непрерывности бизнеса (см. Раздел 14).

Специальная группа или лицо должны быть назначены ответственными за проверку слабых мест и выпусков заплат и исправлений (см. 12.6).

12.5.3 Ограничения на изменения в пакетах программ

Средство управления

Надо препятствовать модификациям в пакетах программ, эти модификации должны быть ограничены необходимыми изменениями, и все изменения должны строго контролироваться.

Руководство по реализации

На сколько возможно и практически выполнимо, пакеты программ, поставляемые поставщиками, должны использоваться без модификации. Если пакет программ необходимо модифицировать, то должны быть рассмотрены следующие пункты:

- a) риски встроенных средств управления и процессы обеспечения целостности, которые подвергаются риску;
- b) должно ли быть получено согласие поставщика;
- c) возможность получения необходимых изменений от поставщика в виде стандартных программных обновлений;
- d) влияние, если организация становится ответственной за будущее сопровождение программного обеспечения в результате изменений.

Если изменения необходимы, то оригинальное программное обеспечение должно быть сохранено, а изменения применены к четко обозначенной копии. Должен быть реализован процесс управления обновлением программного обеспечения для того, чтобы гарантировать установку наиболее обновленных утвержденных заплат и обновлений приложений для всего разрешенного программного обеспечения (см. 12.6). Все изменения должны быть полностью испытаны и документально подтверждены для того, чтобы они могли быть применены повторно, если необходимо, к будущим программным обновлениям. Если требуется, то модификации должны быть испытаны и валидированы независимым оценочным органом.

12.5.4 Утечка информации

Средство управления

Возможности для утечки информации должны предупреждаться.

Руководство по реализации

Следующее должно быть рассмотрено для того, чтобы ограничить риск утечки информации, например, через использование и эксплуатацию скрытых каналов:

- a) сканирование исходящих носителей информации и средств связи на наличие скрытой информации;
- b) маскировка и модулирование поведения систем и средств связи для того, чтобы снизить вероятность того, что третья сторона будет способна проследить информацию из такого поведения;
- c) использование систем и программного обеспечения, которые, как считается, обладают высокой целостностью, например, используют оцененные продукты (см. ISO/IEC 15408);

- d) регулярный постоянный контроль деятельности персонала и системы там, где это разрешено по существующему законодательству или нормам;
- e) постоянный контроль использования ресурсов в компьютерных системах.

Прочая информация

Скрытые Каналы – это пути, которые не предназначены для проведения информационных потоков, но которые могут, тем не менее, существовать в системе или сети. Например, манипулирование битами в протоколах обмена пакетами может использоваться как скрытый метод сигнализации. По их природе, предотвращение существования всех возможных скрытых каналов будет трудным, если не невозможным. Тем не менее, эксплуатация таких каналов часто осуществляется троянским кодом (см. также 10.4.1). Следовательно, принятие мер для защиты от троянского кода уменьшает риски эксплуатации скрытых каналов.

Предотвращение неразрешенного доступа к сети (11.4), а также политика и процедуры для того, чтобы препятствовать неправильному использованию информационных услуг персоналом (15.1.5) помогут защититься от скрытых каналов.

12.5.5 Аутсорсинговая разработка программного обеспечения

Средство управления

Аутсорсинговая разработка программного обеспечения должна быть под надзором организации и постоянно контролироваться организацией.

Руководство по реализации

Если осуществляется аутсорсинг разработки программного обеспечения, то должны быть рассмотрены следующие пункты:

- a) лицензионные соглашения, собственность на код и права на интеллектуальную собственность (см. 15.1.2);
- b) сертификация качества и точности выполненной работы;
- c) мероприятия по условному депонированию на случай отказа третьей стороны;
- d) права доступа для аудита качества и точности сделанной работы;
- e) договорные требования для качества и защитной функциональности кода;
- f) испытание перед установкой с целью обнаружить злонамеренный и троянский код.

12.6 Менеджмент технических слабых мест

Цель: снизить риски, проистекающие из эксплуатации опубликованных технических слабых мест.

Менеджмент технических слабых мест должен реализовываться действенным, систематическим и повторяемым способом с измерениями, выполняемыми для подтверждения его результативности. Эти соображения должны включать операционные системы, а также любые другие приложения, находящиеся в использовании.

12.6.1 Управление техническими слабыми местами

Средство управления

Должна быть получена своевременная информация о технических слабых местах используемых информационных систем, оценена подверженность организации влиянию таких слабых мест, и предприняты подходящие меры для того, чтобы учесть связанный с ними риск.

Руководство по реализации

Текущая и полная опись активов (см. 7.1) – это предварительное условие для результаративного управления техническими слабыми местами. Специфическая информация, необходимая для поддержки менеджмента технических слабых мест, включает поставщика программного обеспечения, номера версий, текущее состояние разработки (например, какое программное обеспечение в каких системах установлено) и человек (люди) в организации, ответственные за программное обеспечение.

Подходящее, своевременное действие должно быть предпринято в ответ на выявление возможных технических слабых мест. Надо выполнять следующее руководство для того, чтобы установить результативный процесс менеджмента для технических слабых мест:

- a) организация должна определить и установить роли и обязанности, связанные с менеджментом технических слабых мест, включая постоянный контроль слабого места, оценку рисков слабого места, наложение заплат, отслеживание активов и любые необходимые обязанности по координации;
- b) информационные ресурсы, которые будут использоваться для выявления значимых технических слабых мест и для поддержки осведомленности о них, должны быть определены для программного обеспечения и другой технологии (основанной на описи активов, см. 7.1.1); эти информационные ресурсы должны обновляться на основе изменений в описи, или когда обнаруживаются другие новые или полезные ресурсы;
- c) должна быть определена временная шкала для того, чтобы реагировать на уведомления о возможно значимых технических слабых местах;

- d) как только возможное техническое уязвимое место будет выявлено, организация должна определить связанные с ним риски и действия, которые нужно предпринять; такое действие может включать в себя наложение заплат на уязвимые системы и/или применение других средств управления;
- e) в зависимости от того, насколько срочно необходимо рассмотреть техническое слабое место, предпринимаемое действие должно быть выполнено в соответствии со средствами управления, связанными с управлением изменениями (см. 12.5.1), или путем выполнения процедур реагирования на событие в системе защиты информации (см. 13.2);
- f) если доступна заплата, то должны быть оценены риски, связанные с установкой заплаты (риски, налагаемые уязвимым местом, должны быть сравнены с рисками установки заплаты);
- g) заплаты должны испытываться и оцениваться до того, как они будут установлены, с целью обеспечить, что они результативны, и что они не приведут к недопустимым побочным эффектам; если никакой заплаты нет в распоряжении, то должны быть рассмотрены другие средства управления, такие как следующие:
 - 1) отключение услуг или возможностей, связанных с уязвимым местом;
 - 2) адаптация или добавление средств управления доступом, например, брандмауэров, на границах сетей (см. 11.4.5);
 - 3) повышенный постоянный контроль для того, чтобы обнаружить или предотвратить фактическую атаку;
 - 4) повышение осведомленности об слабом месте;
- h) контрольный журнал должен вестись для всех выполняемых процедур;
- i) процесс менеджмента техническими слабыми местами должен регулярно контролироваться и оцениваться для того, чтобы обеспечить его результативность и эффективность;
- j) системы с высокой степенью риска должны быть рассмотрены в первую очередь.

Прочая информация

Правильное функционирование организационного процесса менеджмента технических слабых мест критично для многих организаций и, следовательно, должно регулярно контролироваться. Точная опись существенна для обеспечения того, что возможные значимые технические слабые места выявлены.

Менеджмент техническими слабыми местами может рассматриваться как подфункция управления изменениями и в этом качестве может использовать в своих интересах процесс и процедуры менеджмента изменений (см. 10.1.2 и 12.5.1).

Поставщики часто находятся под значительным давлением в отношении того, чтобы выпускать заплаты как можно скорее. Следовательно, заплата может не обращаться к проблеме надлежащим образом и может иметь отрицательные побочные эффекты. Также, в некоторых случаях, удаление заплаты может не быть легко достижимым после того, как заплата будет наложена.

Если требуемое испытание заплат не возможно, например, из-за издержек или недостатка ресурсов, то может быть рассмотрена задержка в наложении заплаты, с целью оценить связанный риск, основываясь на опыте, о котором сообщили другие пользователи.

13 Менеджмент инцидентов в системе защиты информации

13.1 Составление отчетов о событиях и недостатках в системе защиты информации

Цель: Обеспечить, чтобы о событиях в системе защиты информации и недостатках, связанных с информационными системами, сообщалось таким образом, чтобы была возможность своевременно предпринять корректирующее действие.

Должны иметься официальные процедуры составления отчетов о событиях и официальные процедуры эскалации. Все служащие, подрядчики и пользователи третьей стороны должны быть осведомлены о процедурах для составления отчетов о различных типах событий и недостатков, которые могут иметь влияние на защиту организационных активов. От них надо требовать сообщать о любых событиях в системе защиты информации и недостатках как можно скорее назначенному контактному лицу.

13.1.1 Составление отчетов о событиях в системе защиты информации

Средство управления

О событиях в системе защиты информации надо сообщать по подходящим каналам как можно быстрее.

Руководство по реализации

Должна быть создана официальная процедура составления отчетов о событиях в системе защиты информации, вместе с процедурой реагирования на инцидент и процедурой эскалации, устанавливающими действие, которое нужно предпринять по получении сообщения о событии в системе защиты информации. Должно быть установлено контактное лицо для подачи отчета о событиях в системе защиты информации. Надо обеспечить, чтобы это контактное лицо было известно по всей организации, всегда доступно и способно обеспечить требуемый и своевременный ответ.

Все служащие, подрядчики и пользователи третьей стороны должны быть осведомлены о своей обязанности сообщать о любых событиях в системе защиты информации как можно быстрее. Они должны также быть осведомлены о процедуре составления отчетов о событиях в системе защиты информации и контактном лице. Процедуры составления отчетов должны включать в себя следующее:

- a) надлежащие процессы обратной связи для обеспечения того, чтобы те, кто сообщал о событиях в системе защиты информации, были извещены о результатах после того, как вопрос будет рассмотрен и закрыт;

- b) формы составления отчетов о событиях в системе защиты информации для того, чтобы поддержать действие по составлению отчетов и помочь сообщающему лицу вспомнить все необходимые действия в случае события в системе защиты информации;
- c) правильное поведение, которое нужно осуществлять в случае события в системе защиты информации, т.е.
 - 1) сразу отмечать все важные подробности (например, тип несоответствия или нарушения, возникающий сбой, сообщения на экране, странное поведение);
 - 2) не выполнять никаких действий, а немедленно доложить контактному лицу;
- d) ссылка на установленный официальный дисциплинарный процесс для работы со служащими, подрядчиками или пользователями третьей стороны, которые нарушают защиту.

В средах с высокой степенью риска может быть предусмотрен сигнал непосредственной опасности¹⁰, посредством чего человек под психологическим давлением может указать на такие проблемы. Процедуры реагирования на сигнал непосредственной опасности должны отражать ситуации с высокой степенью риска, на которые такие сигналы указывают.

Прочая информация

Примерами событий и инцидентов в системе защиты информации являются следующие:

- a) невыполненное обслуживание, срывы оборудования или средств,
- b) системные сбои или перегрузки,
- c) человеческие ошибки,
- d) несоответствия политике или руководящим принципам,
- e) нарушения мер физической защиты,
- f) неконтролируемые системные изменения,
- g) сбои программного обеспечения или аппаратных средств,
- h) нарушения прав доступа.

С должной заботой о вопросах конфиденциальности, инциденты в системе защиты информации могут использоваться при подготовке в целях осведомленности пользователей (см. 8.2.2) как примеры того, что может случиться, как реагировать на

¹⁰ Сигнал непосредственной опасности [duress alarm] является методом скрытно указать на то, что действие происходит «под давлением» [under duress].

такие инциденты и как избежать их в будущем. Чтобы быть способным рассмотреть события и инциденты в системе защиты информации надлежащим образом, может оказаться необходимым собирать доказательства как можно скорее после возникновения (см. 13.2.3).

Сбои или другое аномальное поведение системы могут быть показателем атаки на защиту или фактического нарушения защиты, и должны, следовательно, всегда докладываться как событие в системе защиты информации.

Дополнительную информацию о составлении отчетов о событиях в системе защиты информации и менеджменте инцидентов в системе защиты информации можно найти в ISO/IEC TR 18044.

13.1.2 Составление отчетов о недостатках защиты

Средство управления

От всех служащих, подрядчиков и пользователей третьей стороны информационных систем и услуг надо потребовать отмечать и сообщать любые наблюдаемые или подозреваемые недостатки защиты в системах или услугах.

Руководство по реализации

Все служащие, подрядчики и пользователи третьей стороны должны сообщать эти материалы или своему руководству, или непосредственно поставщику услуги как можно быстрее для того, чтобы предотвратить инциденты в системе защиты информации. Механизм составления отчетов должен быть как можно более легким, понятным и доступным. Они должны быть проинформированы о том, что они не должны, при любых обстоятельствах, пытаться доказать подозрительный недостаток.

Прочая информация

Служащим, подрядчикам и пользователям третьей стороны надо посоветовать не пытаться доказать подозрительные недостатки защиты. Испытание недостатков может быть интерпретировано как возможное неправильное использование системы и может также вызывать ущерб для информационной системы или услуги и привести к юридической ответственности для лица, выполняющего испытание.

13.2 Менеджмент инцидентов и улучшений в системе защиты информации

Цель: Обеспечить применение последовательного и результативного подхода к менеджменту инцидентов в системе защиты информации.

Должны иметься обязанности и процедуры для того, чтобы результативно справляться с событиями и недостатками в системе защиты информации, как только о них будет сообщено. Процесс непрерывного улучшения должен применяться к реагированию на инциденты в системе защиты информации, постоянный контроль, оценивание и общий менеджмент инцидентов в системе защиты информации.

Там где требуются доказательства, они должны быть собраны для обеспечения соответствия юридическим требованиям.

13.2.1 Обязанности и процедуры

Средство управления

должны быть установлены обязанности руководства и процедуры для обеспечения быстрого, результативного и организованного реагирования на инциденты в системе защиты информации.

Руководство по реализации

В дополнение к составлению отчетов о событиях и недостатках в системе защиты информации (см. также 13.1), должны использоваться постоянный контроль систем, предупреждений и слабых мест (10.10.2) для того, чтобы обнаруживать инциденты в системе защиты информации. Должны быть рассмотрены следующие руководящие указания для процедур менеджмента инцидентов в системе защиты информации:

- a) должны быть установлены процедуры для обращения с разными типами инцидентов в системе защиты информации, включая следующие:
 - 1) сбои информационных систем и невыполненное обслуживание;
 - 2) злонамеренный код (см. 10.4.1);
 - 3) отказ от обслуживания;
 - 4) ошибки, проистекающие из неполной или неточной деловой информации;
 - 5) нарушения конфиденциальности и целостности;
 - 6) неправильное использование информационных систем;
- b) в дополнение к обычным чрезвычайным планам (см. 14.1.3), процедуры должны также охватывать следующее (см. также 13.2.2):
 - 1) анализ и определение причины инцидента;

- 2) ограничение распространения последствий;
 - 3) планирование и реализация корректирующего действия для того, чтобы предотвратить повторение, если необходимо;
 - 4) обмен информации с теми, на кого повлияет восстановление после инцидента или с теми, кто задействован в этом восстановлении;
 - 5) подача отчета о действии соответствующему руководству;
- c) контрольные журналы и аналогичные доказательства должны быть собраны (см. 13.2.3) и защищены, по обстановке, для следующих целей:
- 1) анализ внутренних проблем;
 - 2) использование в качестве судебного доказательства в отношении возможного нарушения договорного или нормативного требования или в случае гражданского или уголовного преследования, например, по закону в области неправильного использования компьютеров или защиты данных;
 - 3) ведение переговоров о компенсации от поставщиков программного обеспечения и услуг;
- d) действие для восстановления после нарушений защиты и исправления системных сбоев должно тщательно и официально управляться; процедуры должны обеспечивать следующее:
- 1) только четко определенному и уполномоченному персоналу разрешен доступ к живым системам и данным (см. также 6.2 для внешнего доступа);
 - 2) все предпринимаемые экстренные действия подробно документируются;
 - 3) об экстренном действии докладывается руководству, и действие анализируется в организованном порядке;
 - 4) целостность деловых систем и средств управления подтверждается с минимальной задержкой.

Задачи для менеджмента инцидентов в системе защиты информации должны быть согласованы с руководством, и должно быть обеспечено, чтобы те, кто ответственен за менеджмент инцидентов в системе защиты информации, понимали приоритеты организации в отношении обращения с инцидентами в системе защиты информации.

Прочая информация

Инциденты в системе защиты информации могут выйти за границы организации и государства. Чтобы реагировать на такие инциденты, имеется увеличивающаяся потребность координировать реагирование и совместно использовать информацию об этих инцидентах с внешними организациями, по обстановке.

13.2.2 Извлечение уроков из инцидентов в системе защиты информации

Средство управления

Должны иметься механизмы для того, чтобы дать возможность количественно определить и постоянно контролировать типы, объемы и затраты на инциденты в системе защиты информации.

Руководство по реализации

Информация, полученная из оценки инцидентов в системе защиты информации, должна использоваться для выявления повторно возникающих инцидентов и инцидентов с высокой степенью влияния.

Прочая информация

Оценка инцидентов в системе защиты информации может указывать на потребность в расширенных или дополнительных средствах управления для того, чтобы ограничить частоту, ущерб и затраты будущих случаев, или ее надо принять во внимание в процессе анализа политики в области защиты (см. 5.1.2).

13.2.3 Сбор доказательств

Средство управления

Если последующая акция против человека или организации после инцидента в системе защиты информации включает судебный иск (или гражданский, или уголовный), то должны быть собраны, сохранены и представлены доказательства для того, чтобы соответствовать правилам для доказательств, сформулированным в соответствующей юрисдикции (юрисдикциях).

Руководство по реализации

При сборе и представлении доказательств для целей дисциплинарного действия, осуществляемого в рамках в организации, должны быть разработаны и должны исполняться внутренние процедуры.

В общих чертах, правила для доказательств охватывают следующее:

- a) допустимость доказательства: может ли доказательство использоваться в суде;
- b) вескость доказательства: качество и комплектность доказательства.

Чтобы достичь допустимости доказательства, организации должны обеспечивать, чтобы их информационные системы соответствовали какому-либо опубликованному стандарту или процессуальным нормам для производства допустимого доказательства.

Вес предоставляемого доказательства должен соответствовать любым применимым требованиям. Для того чтобы достичь веса доказательства, качества и полнота средств управления, используемых для того, чтобы правильно и последовательно

защитить доказательство (т.е. доказательство управления процессом) для всего периода, в течение которого доказательство, которое предстоит извлечь, хранилось и обрабатывалось, должны быть продемонстрированы серьезным разбирательством доказательства. В общих чертах, такое серьезное разбирательство может быть создано при следующих условиях:

- a) для бумажных документов: подлинник хранится надежно с записью лица, обнаружившего документ, где документ был обнаружен, когда документ был обнаружен и кто засвидетельствовал обнаружение; любое расследование должно гарантировать, что подлинники не были сфальсифицированы;
- b) для информации на компьютерном носителе: зеркальные отображение или копии (в зависимости от применимых требований) любого смennого носителя, информации на жестких дисках или в памяти должны быть взяты для обеспечения доступности; должен сохраняться протокол всех действий в ходе процесса копирования, и процесс должен быть засвидетельствован; оригиналный носитель и протокол (если это невозможно, то, по крайней мере, одно зеркальное отображение или копия), должны храниться защищенными и нетронутыми.

Любая судебная работа должна осуществляться только на копиях доказательного материала. Целостность доказательного материала должна быть защищена. Копирование доказательного материала должно быть под надзором надежного персонала, а информация о том, когда и где был выполнен процесс копирования, кто осуществлял деятельность по копированию, и какие инструментальные средства и программы были использованы, должна быть зарегистрирована.

Прочая информация

Когда событие в системе защиты информации обнаруживается впервые, может не быть очевидным, закончится ли событие судебным преследованием. Следовательно, существует опасность того, что необходимые доказательства будут уничтожены преднамеренно или случайно прежде, чем будет осознана серьезность инцидента. Желательно привлечь юриста или полицию в начале любого обдумываемого юридического действия и советоваться по требуемым доказательствам.

Доказательство может выйти за границы организации и/или юрисдикции. В таких случаях надо обеспечить, чтобы организация имела право собирать необходимую информацию как доказательство. Также должны быть рассмотрены требования разных юрисдикций для того, чтобы максимально увеличить шансы доступа через соответствующие юрисдикции.

14 Менеджмент непрерывности бизнеса

14.1 Аспекты менеджмента непрерывности бизнеса, связанные с защитой информации

Цель: Противодействовать прерываниям деловых операций и защищать критические деловые процессы от эффектов существенных сбоев информационных систем или бедствий, а также обеспечивать их своевременное возобновление.

Процесс менеджмента непрерывности бизнеса должен быть реализован для минимизации влияния на организацию и восстановления от потери информационных активов (которая может явиться результатом, например, стихийного бедствия, аварии, сбоя оборудования и преднамеренных действий) до приемлемого уровня посредством комбинации предупреждающих и восстанавливающих средств управления. Этот процесс должен идентифицировать критические деловые процессы и интегрировать требования непрерывности бизнеса к управлению защитой информации с другими требованиями непрерывности, связанными с такими аспектами, как операции, кадровое обеспечение, материалы, транспорт и средства.

Последствия бедствий, сбоев в системе защиты, невыполненного обслуживания, а также доступность услуги должны быть предметом анализа влияния на бизнес. Планы обеспечения непрерывности бизнеса должны быть разработаны и реализованы для обеспечения своевременного возобновления существенных операций. Защита информации должна быть неотъемлемой частью общего процесса обеспечения непрерывности бизнеса, а также других процессов менеджмента в организации.

Менеджмент непрерывности бизнеса должен включать средства управления для того, чтобы выявлять и снижать риски, в дополнение к общим процессам оценки рисков, ограничивать последствия повреждающих инцидентов и обеспечивать, чтобы информация, необходимая для деловых процессов, была легко доступна.

14.1.1 Включение защиты информации в процесс менеджмента непрерывности бизнеса

Средство управления

Должен быть разработан и должен поддерживаться по всей организации управляемый процесс для обеспечения непрерывности бизнеса, который рассматривает требования защиты информации, необходимые для обеспечения непрерывности бизнеса организации.

Руководство по реализации

Процесс должен свести воедино следующие ключевые аспекты менеджмента непрерывности бизнеса:

- a) понимание рисков, с которыми сталкивается организация, с точки зрения вероятности и влияния со временем, включая выявление и присваивание приоритетов критическим деловым процессам (см. 14.1.2);
- b) выявление всех активов, вовлеченных в критические деловые процессы (см. 7.1.1);
- c) понимание влияния, которое прерывания, вызванные инцидентами в системе защиты информации, могут оказать на бизнес (важно, чтобы были найдены решения, которые справляются с инцидентами, вызывающими меньшее влияние, равно как и с серьезными инцидентами, которые могут угрожать жизнеспособности организации) и установление деловых целей средств обработки информации;
- d) рассмотрение приобретения подходящей страховки, которая может образовать часть общего процесса обеспечения непрерывности, также являясь частью менеджмента операционных рисков;
- e) выявление и рассмотрение реализации дополнительных предупреждающих и уменьшающих средств управления;
- f) выявление достаточных финансовых, организационных, технических ресурсов и ресурсов окружающей среды для того, чтобы учесть определенные требования защиты информации;
- g) обеспечение безопасности персонала и защиты средств обработки информации, а также организационной собственности;
- h) формулировка и документирование планов обеспечения непрерывности бизнеса, учитывающие требования защиты информации в соответствии с согласованной стратегией обеспечения непрерывности бизнеса (см. 14.1.3);
- i) регулярное испытание и обновление реализованных планов и процессов (см. 14.1.5);
- j) обеспечение того, чтобы менеджмент непрерывности бизнеса был включен в процессы и структуру организации; ответственность за процесс менеджмента непрерывности бизнеса должна быть назначена на подходящем уровне в организации (см. 6.1.1).

14.1.2 Непрерывность бизнеса и оценка рисков

Средство управления

События, которые могут вызвать прерывания деловых процессов, должны быть определены, вместе с вероятностью и влиянием таких прерываний и их последствий для защиты информации.

Руководство по реализации

Аспекты обеспечения непрерывности бизнеса, связанные с защитой информации, должны быть основаны на выявлении событий (или последовательности событий), которые могут вызвать прерывания в деловых процессах организаций, например, сбой оборудования, человеческие ошибки, кражи, пожар, стихийные бедствия и акты терроризма. За оценкой рисков должно последовать определение вероятности и влияния таких прерываний с точки зрения времени, масштаба ущерба и периода восстановления.

Оценки рисков для непрерывности бизнеса должны проводиться с полным вовлечением владельцев деловых ресурсов и процессов. Эта оценка должна рассматривать все деловые процессы и не должна быть ограниченной средствами обработки информации, но должна включить результаты, специфичные для защиты информации. Важно связать воедино различные аспекты рисков для того, чтобы получить полную картину требований непрерывности бизнеса организации. Оценка должна выявлять, количественно определять риски и назначать им приоритеты в соответствии с критериями и задачами, значимыми для организации, включая критические ресурсы, влияния нарушений, допустимые периоды простоя и приоритеты восстановления.

В зависимости от результатов оценки рисков, должна быть разработана стратегия обеспечения непрерывности бизнеса для определения общего подхода к непрерывности бизнеса. Как только эта стратегия будет создана, руководством должно быть предоставлено подтверждение, и должен быть создан и претворен в жизнь план для реализации этой стратегии.

14.1.3 Разработка и реализация планов обеспечения непрерывности, включающих защиту информации

Средство управления

Должны быть разработаны и реализованы планы для поддержания или восстановления операций и обеспечения доступности информации на необходимом уровне и в рамках необходимого времени, выполнение которых следует за прерыванием или сбоем критических деловых процессов.

Руководство по реализации

Процесс планирования обеспечения непрерывности бизнеса должен учитывать следующее:

- a) выявление и согласование всех обязанностей и процедур обеспечения непрерывности бизнеса;
- b) определение приемлемой потери информации и невыполнения обслуживания;
- c) реализация процедур с целью сделать возможным возвращение к исходному режиму и восстановление деловых операций и доступности информации в необходимое время; особое внимание должно быть уделено оценке внутренних и внешних зависимостей бизнеса и имеющихся договоров;
- d) эксплуатационные процедуры, которым надо следовать в ожидании завершения возвращения к исходному режиму и восстановления;
- e) документация согласованных процедур и процессов;
- f) соответствующее образование персонала в области согласованных процедур и процессов, включая антикризисное управление;
- g) испытание и обновление планов.

Процесс планирования должен сфокусироваться на необходимых деловых задачах, например, восстановление конкретных услуг связи потребителям в приемлемое время. Должны быть выявлены услуги и ресурсы, способствующие этому, включая кадровое обеспечение, неинформационные обрабатывающие ресурсы, а также мероприятия перехода средств обработки информации в аварийный режим. Такие мероприятия перехода в аварийный режим могут включать мероприятия, проводимые совместно с третьими сторонами в форме соглашений на основе взаимности, или коммерческие подписные услуги.

Планы обеспечения непрерывности бизнеса должны учитывать организационные слабые места и, следовательно, могут содержать важную информацию, которая должна быть защищена надлежащим образом. Копии планов обеспечения непрерывности бизнеса должны храниться в отдаленном местоположении, на достаточном расстоянии для того, чтобы избежать любого ущерба от бедствия на основном месте. Руководство должно обеспечивать, чтобы копии планов обеспечения непрерывности бизнеса были обновленными и защищенными на том же самом уровне защиты, который применяется на основном месте. Другой материал, необходимый для реализации планов обеспечения непрерывности, также должен храниться в отдаленном местоположении.

Если используются альтернативные временные местоположения, то уровень реализованных средств управления защитой на этих местах должен быть эквивалентен основному месту.

Прочая информация

Следует отметить, что планы и виды деятельности антикризисного управления (см. 14.1.3 f)), могут отличаться от менеджмента непрерывности бизнеса; т.е. может произойти кризис, который может быть уложен обычными процедурами менеджмента.

14.1.4 Структура планирования непрерывности бизнеса

Средство управления

Должна поддерживаться единая структура планов обеспечения непрерывности бизнеса для обеспечения того, чтобы все планы были последовательны, для последовательного учета требований защиты информации и для определения приоритетов для испытания и эксплуатации.

Руководство по реализации

Каждый план обеспечения непрерывности бизнеса должен описывать подход к обеспечению непрерывности, например подход для обеспечения доступности и защиты информации или информационной системы. Каждый план также должен определять план эскалации и условия для его активации, равно как и лиц, ответственных за выполнение каждого компонента плана. Когда новые требования выявлены, любые существующие чрезвычайные процедуры, например, планы эвакуации или мероприятия перехода в аварийный режим, должны быть исправлены, по обстановке. Процедуры должны быть включены в организационную программу менеджмента изменений для обеспечения того, чтобы вопросы непрерывности бизнеса всегда надлежащим образом учитывались.

Каждый план должен иметь конкретного владельца. Чрезвычайные процедуры, планы перехода в аварийный режим вручную и планы возобновления должны находиться под ответственностью владельцев соответствующих вовлеченных деловых ресурсов или процессов. Мероприятия перехода в аварийный режим для альтернативных технических услуг, таких как обработка информации и средства связи, обычно должны находиться под ответственностью поставщиков услуг.

Структура планирования непрерывности бизнеса должна учитывать выявленные требования защиты информации и рассмотреть следующее:

- a) условия для активации планов, описывающих процесс, который предстоит выполнить (например, как оценить ситуацию, кто должен быть задействован) прежде, чем каждый план будет активирован;
- b) чрезвычайные процедуры, описывающие действия, которые будут предприняты вслед за инцидентом, подвергающим опасности деловые операции;
- c) процедуры перехода в аварийный режим, которые описывают действия, которые надлежит предпринять для перемещения важных деловых операций или вспомогательных услуг в альтернативные временные местоположения и вернуть деловые процессы обратно в работу в течение необходимого времени;

- d) временные эксплуатационные процедуры, которым надлежит следовать в ожидании завершения восстановления и возврата в обычный режим;
- e) процедуры возобновления, описывающие действия, которые надлежит предпринять для возврата к нормальным деловым операциям;
- f) график обслуживания, который определяет, как и когда план будет испытан, и процесс для обслуживания плана;
- g) деятельность по повышению осведомленности, образованию и подготовке, которые предназначены для того, чтобы создать понимание процессов обеспечения непрерывности бизнеса и обеспечить, что процессы продолжают оставаться результативными;
- h) обязанности лиц, описывающие, кто за выполнение какой компоненты плана ответственен. Если требуется, то должны быть назначены альтернативы;
- i) критические активы и ресурсы, необходимые для того, чтобы быть способным выполнить чрезвычайные процедуры, процедуры перехода в аварийный режим и процедуры возобновления.

14.1.5 Испытание, обслуживание и повторная оценка планов обеспечения непрерывности бизнеса

Средство управления

Планы обеспечения непрерывности бизнеса должны регулярно испытываться и обновляться для обеспечения того, что они являются новейшими и результативными.

Руководство по реализации

Испытания плана обеспечения непрерывности бизнеса должны гарантировать, что все члены группы по восстановлению и другой имеющий отношение к делу персонал осведомлены о планах и о своей ответственности за непрерывность бизнеса и защиту информации, и знают о своей роли при осуществлении плана.

Программа испытаний для плана (планов) обеспечения деловой непрерывности должна указывать, как и когда должен быть испытан каждый элемент плана. Каждый элемент плана (планов) должен испытываться часто.

Ряд методик должен использоваться для обеспечения гарантии того, что план (планы) будут работать в реальной жизни. Они должны включать в себя следующее:

- a) настольное испытание различных сценариев (обсуждение мероприятий восстановления бизнеса, используя примерные прерывания);
- b) моделирования (особенно для подготовки людей в их ролях после инцидентов/ в антикризисном управлении);

- c) испытание технического восстановления (обеспечение того, что информационные системы могут быть результативно восстановлены);
- d) испытание восстановления в альтернативном месте (выполнение деловых процессов параллельно с операциями восстановления вдали от основного места);
- e) испытания средств и услуг поставщика (обеспечение того, услуги и продукты, поставленные извне, соответствовали договорным обязательствам);
- f) полные репетиции (испытание того, что организация, персонал, оборудование, средства и процессы могут справиться с прерываниями).

Эти методики могут использоваться любой организацией. Они должны применяться таким способом, который значим для конкретного плана восстановления. Результаты испытаний должны быть записаны, и должны быть предприняты действия для того, чтобы улучшить планы, если это необходимо.

Должна быть назначена ответственность за регулярное проведение анализов каждого плана обеспечения непрерывности бизнеса. За выявлением изменений в деловых мероприятиях, еще не отраженных в планах обеспечения непрерывности бизнеса, должно последовать соответствующее обновление плана. Этот официальный процесс управления изменениями должен обеспечивать, чтобы обновленные планы распространялись и улучшались посредством регулярного анализа полного плана.

Примеры изменений, где должно быть рассмотрено обновление планов обеспечения непрерывности бизнеса, являются приобретение нового оборудования, модернизация систем и изменения в следующем:

- a) персонал;
- b) адреса или номера телефонов;
- c) деловая стратегия;
- d) местоположение, средства и ресурсы;
- e) законодательство;
- f) подрядчики, поставщики и ключевые потребители;
- g) процессы, или новые, или отмененные;
- h) риск (операционный и финансовый).

15 Соответствие

15.1 Соответствие юридическим требованиям

Цель: избежать нарушений любых требований закона, уставных, нормативных или договорных обязательств, и любых требований защиты.

Проектирование, работа, использование информационных систем и управление информационными системами могут быть предметом уставных, нормативных и договорных требований защиты.

За советом по конкретным юридическим требованиям надо обращаться к юридическим консультантам в организации или должным образом квалифицированным практикующим юристам. Законодательные требования отличаются от страны к стране и могут различаться для информации, созданной в одной стране, которая передается в другую страну (т.е. поток данных через границу государства).

15.1.1 Идентификация применимых законов

Средство управления

Все имеющие отношение к делу уставные, нормативные и договорные требования и подход организации к выполнению этих требований должны быть четко определены, документально подтверждены и должны поддерживаться на современном уровне для каждой информационной системы и организации.

Руководство по реализации

Конкретные средства управления и отдельные обязанности для того, чтобы выполнить эти требования, должны быть аналогичным образом определены и документально подтверждены.

15.1.2 Права на интеллектуальную собственность (ПИС)

Средство управления

Должны быть реализованы подходящие процедуры для обеспечения соответствия законодательным, нормативным и договорным требованиям по использованию материала, в отношении которого могут иметься права на интеллектуальную собственность, и по использованию патентованных программных продуктов.

Руководство по реализации

Должны быть рассмотрены следующие руководящие указания для защиты любого материала, который может считаться интеллектуальной собственностью:

- a) публикация политики соответствия в области прав на интеллектуальную собственность, которая определяет законное использование программных и информационных продуктов;
- b) приобретение программного обеспечения только через известные и солидные источники, с целью гарантировать, что авторское право не нарушено;
- c) поддержание осведомленности о политике для того, чтобы защищать права на интеллектуальную собственность, и уведомление о намерении осуществлять дисциплинарное действие против персонала, нарушающего ее;
- d) поддержание подходящих реестров активов, и выявление всех активов с требованиями защищать права на интеллектуальную собственность;
- e) поддерживание доказательств и свидетельств собственности на лицензии, мастер-диски, руководства и т.п.;
- f) реализация средств управления для обеспечения того, чтобы не разрешалось превышать любое максимальное количество пользователей;
- g) выполнение проверок того, что установлены только разрешенное программное обеспечение и лицензионные продукты;
- h) обеспечение политики для поддержания надлежащих лицензионных условий;
- i) обеспечение политики для отдачи или передачи программного обеспечения другим;
- j) использование подходящих инструментальных средств аудита;
- k) соответствие постановлениям и условиям для программного обеспечения и информации, полученным из общественных сетей;
- l) не дублировать, не преобразовывать в другой формат или не извлекать из коммерческих записей (фильм, аудио) ничего, кроме того, что разрешено законом об авторском праве;
- m) не копировать полностью или частично книги, статьи, отчеты или другие документы, кроме тех, копирование которых разрешено законом об авторском праве.

Прочая информация

Права на интеллектуальную собственность включают авторское право на программное обеспечение или документы, права промышленной собственности, торговые марки, патенты и лицензии на исходный код.

Патентованные программные продукты обычно поставляются по лицензионному соглашению, которое точно определяет лицензионные положения и условия, например, ограничение использования продуктов на определенные машины или ограниченное копирование только для создания резервных копий. Ситуацию с ПИС для программного обеспечения, разработанного организацией, требуется разъяснить персоналу.

Законодательные, нормативные и договорные требования могут налагать ограничения на копирование патентованного материала. В частности, они могут потребовать, что может использоваться только материал, который разработан организацией, или который лицензирован или предоставлен разработчиком в организацию. Нарушение авторского права может привести к правовому действию, которое может включать в себя уголовное преследование.

15.1.3 Защита организационных записей

Средство управления

Важные записи должны быть защищены от потери, разрушения и фальсификации, в соответствии с уставными, нормативными, договорными и деловыми требованиями.

Руководство по реализации

Записи должны быть распределены по типам записей, например, учетная [бухгалтерская] записи, записи базы данных, журналы транзакций, контрольные журналы и эксплуатационные процедуры, каждый с деталями сроков хранения и типом носителя, например, бумаги, микрофиши, магнитные, оптические. Любой связанный материал по криптографическому шифрованию и программы, связанные с зашифрованными архивами или цифровыми подписями (см. 12.3), также должны храниться для того, чтобы сделать возможной расшифровку записей в течение того периода времени, когда записи удерживаются.

Внимание должно быть уделено возможности ухудшения состояния носителя, используемого для хранения записей. Процедуры хранения и обслуживания должны быть реализованы в соответствии с рекомендациями изготовителя. Для длительного хранения, должно быть рассмотрено использование бумаги и микрофильмов.

Если выбран электронный носитель, то должны быть включены процедуры для обеспечения возможности иметь доступ к данным (читаемость как носителя, так и формата) в течение всего срока хранения для защиты от потери из-за будущего изменения технологии.

Системы хранения данных должны выбираться так, чтобы необходимые данные могли быть извлечены в приемлемый период времени и в приемлемом формате, в зависимости от требований, которые нужно выполнить.

Система хранения и обслуживания должна обеспечивать четкое обозначение записей и их срока хранения, определенного государственными или местными законами или нормами, если необходимо. Эта система должна делать возможной

надлежащую ликвидацию записей по истечении этого периода, если они не нужны организации.

Для того чтобы выполнить эти задачи по защите записей, в организации должны быть предприняты следующие шаги:

- a) должны быть выпущены руководящие указания по удержанию, обслуживанию, обработке и ликвидации записей и информации;
- b) должен быть составлен график сроков хранения, определяющий записи и период времени, в течение которого они должны удерживаться;
- c) должна поддерживаться опись источников ключевой информации;
- d) должны быть реализованы надлежащие средства управления для защиты записи и информации от потери, разрушения и фальсификации.

Прочая информация

Может понадобиться надежно сохранить некоторые записи для того, чтобы выполнить уставные, нормативные или договорные требования, а также для того, чтобы поддержать важные деловые операции. Примеры включают записи, которые могут потребоваться в качестве доказательства того, что организация действует в рамках уставных или нормативных правил для обеспечения требуемой защиты от возможного гражданского или уголовного иска или для того, чтобы подтвердить финансовый статус организации по отношению к акционерам, внешним сторонам и аудиторам. Период времени и содержание данных для удержания информации могут быть установлены государственным законом или нормой.

Дополнительную информацию об управлении организационными записями можно найти в ИСО 15489-1.

15.1.4 Защита данных и секретность личной информации

Средство управления

Защита данных и секретность должны быть гарантированы, как требуется в соответствующем законодательстве, нормах, и, если применимо, условиях договора.

Руководство по реализации

Должны быть разработаны и реализованы политика защиты организационных данных и политика обеспечения секретности. Эта политика должна быть доведена до сведения всех лиц, вовлеченных в обработку личной информации.

Соответствие этой политике и всем имеющим отношение к делу законам и нормам в области защиты данных требует соответствующей структуры менеджмента и управления. Часто это наилучшим образом достигается назначением ответственного лица, например, ответственный за защиту данных, который должен обеспечивать руководство для менеджеров, пользователей и поставщиков услуг по их личным

обязанностям и конкретным процедурам, которым надлежит следовать. Ответственность за обращение с личной информацией и обеспечение осведомленности о принципах защиты данных должна рассматриваться в соответствии с имеющимися отношениями к делу законодательством и нормами. Должны быть реализованы надлежащие технические и организационные меры для защиты личной информации.

Прочая информация

Ряд стран ввел законы, устанавливающие средства управления на сбор, обработку и передачу личных данных (обычно информация о живых людях, которые могут быть определены из этой информации). В зависимости от соответствующего государственного законодательства, такие средства управления могут налагать обязанности по сбору, обработке и распространению личной информации, и могут ограничивать способность передавать эти данные в другие страны.

15.1.5 Предотвращение неправильного использования средств обработки информации

Средство управления

Пользователи должны удерживаться от использования средств обработки информации для неразрешенных целей.

Руководство по реализации

Руководство должно утвердить использование средств обработки информации. Любое использование этих средств для неделовых целей без утверждения руководства (см. 6.1.4) или для любых неразрешенных целей должно рассматриваться как неправильное использование средств. Если в ходе постоянного контроля или другими средствами выявлена неразрешенная деятельность, то на эту деятельность надо обратить внимание отдельного менеджера, ответственного за рассмотрение надлежащего дисциплинарного и/или правового действия.

Перед реализацией процедур постоянного контроля надо получить юридическую консультацию.

Все пользователи должны быть осведомлены о точной сфере их разрешенного доступа и о постоянном контроле на местах с целью обнаружения неразрешенного использования. Это может быть достигнуто путем выдачи пользователям письменного разрешения, копия которого должна быть подписана пользователем и должна надежно сохраняться организацией. Служащим организации, подрядчикам и пользователям третьей стороны надо сказать, что не будет разрешен никакой доступ, кроме того, который разрешен.

В начале входа в систему должно быть представлено предупреждающее сообщение с целью указать, что средство обработки информации, на которое осуществляется вход, принадлежит организации, и что неразрешенный доступ запрещен. Пользователь должен подтвердить и надлежащим образом отреагировать на сообщение на экране для продолжения процесса входа в систему (см. 11.5.1).

Прочая информация

Средства обработки информации организации предназначены изначально или исключительно для деловых целей.

Обнаружение вторжения, контроль содержимого и другие инструментальные средства постоянного контроля могут помочь предотвратить и обнаружить неправильное использование средств обработки информации.

Много стран имеют законодательство для защиты от неправильного использования компьютеров. Это может быть уголовным преступлением – использовать компьютер для неразрешенных целей.

Законность постоянного контроля использования отличается от страны к стране и может потребовать от руководства сообщить всем пользователям о таком постоянном контроле и/или получить их согласие. Если система, в которую осуществляется вход, используется для открытого доступа (например, общественный веб-сервер) и подвергается постоянному контролю защиты, то должно быть отображено сообщение, в котором об этом сказано.

15.1.6 Регулирование криптографических средств управления

Средство управления

Криптографические средства управления должны использоваться в соответствии со всеми имеющимися отношение к делу соглашениями, законами и нормами.

Руководство по реализации

Для соответствия с имеющимися отношение к делу соглашениями, законами и нормами должны быть рассмотрены следующие пункты:

- a) ограничения на импорт и/или экспорт аппаратных средств и программного обеспечения для выполнения криптографических функций;
- b) ограничения на импорт и/или экспорт аппаратных средств и программного обеспечения, которые предназначены для того, чтобы добавлять к ним криптографические функции;
- c) ограничения на использование шифрования;
- d) обязательные или предоставленные на усмотрение методы доступа органами страны к информации, зашифрованной аппаратными средствами или программным обеспечением для того, чтобы обеспечить конфиденциальность содержимого.

Надо обратиться за юридической консультацией для того, чтобы обеспечить соответствие государственным законам и нормам. Прежде, чем зашифрованная информация или криптографические средства управления будут перемещены в другую страну, надо также обратиться за юридической консультацией.

15.2 Соответствие политике и стандартам в области защиты и техническое соответствие

Цель: обеспечить соответствие систем с организационной политикой и стандартами в области защиты.

Защита информационных систем должна регулярно анализироваться.

Такой анализ должен выполняться по отношению к соответствующей политике в области защиты и техническим платформам, а информационные системы должны проверяться на соответствие применимым стандартам реализации защиты и документально подтвержденным средствам управления защитой.

15.2.1 Соответствие политике и стандартам в области защиты

Средство управления

Менеджеры должны обеспечивать, чтобы все процедуры защиты в их зоне ответственности выполнялись правильно, чтобы достичь соответствия политике и стандартам в области защиты.

Руководство по реализации

Менеджеры должны регулярно анализировать соответствие обработки информации в их зоне ответственности политике, стандартам в области защиты, а также любым другим требованиям защиты.

Если в результате анализа обнаружено какое-либо несоответствие, то менеджеры должны:

- a) определить причину несоответствия;
- b) оценить потребность в действиях для обеспечения того, чтобы несоответствие не возникло повторно;
- c) определить и реализовать подходящее корректирующее действие;
- d) проанализировать предпринятое корректирующее действие.

Результаты анализов и корректирующих действий, выполненных менеджерами, должны быть записаны, и эти записи должны сохраняться. Менеджеры должны сообщать результаты лицам, выполняющим независимый анализ (см. 6.1.8), когда независимый анализ происходит в зоне их ответственности.

Прочая информация

Оперативный постоянный контроль использования систем охвачен в 10.10.

15.2.2 Проверка технического соответствия

Средство управления

Информационные системы должны регулярно проверяться на соответствие стандартам реализации защиты.

Руководство по реализации

Проверка технического соответствия должна выполняться или вручную (поддерживаемая подходящими программными средствами, если необходимо) опытным системотехником, и/или с помощью автоматизированных инструментальных средств, которые генерируют технический отчет для последующей интерпретации техническим специалистом.

Если используется испытание на проникновение или оценки уязвимости, то должно быть использовано предупреждение, поскольку такая деятельность может привести к подверганию риску защиты системы. Такие испытания должны быть запланированы, документально подтверждены и повторяемы.

Любая проверка технического соответствия должна выполняться только компетентными, уполномоченными лицами, или под контролем таких лиц.

Прочая информация

Проверка технического соответствия включает в себя обследование операционных систем для обеспечения того, чтобы аппаратные средства и программные средства управления были правильно реализованы. Этот тип проверки соответствия требует технического опыта специалиста.

Проверка соответствия также охватывает, например, испытание на проникновение и оценку слабых мест, которые могут выполняться независимыми экспертами, нанятыми специально для этой цели. Это может быть полезным в обнаружении слабых мест в системе и для проверки того, насколько средства управления результативны в предотвращении неразрешенного доступа из-за этих слабых мест.

Испытание на проникновение и оценка слабых мест дает моментальный снимок системы в конкретном состоянии в конкретный момент времени. Моментальный снимок ограничен теми частями системы, которые реально испытываются во время попытки (попыток) проникновения. Испытание на проникновение и оценки слабых места не являются заменой для оценки рисков.

15.3 Соображения, касающиеся аудита информационных систем

Цель: Максимально увеличит результативность и максимально снизить помехи для/от процесса аудита информационных систем.

Должны иметься средства управления для охраны операционных систем и инструментальных средств аудита в ходе аудитов информационных систем.

Защита также требуется для того, чтобы охранять целостность и предотвращать неправильное использование инструментальных средств аудита.

15.3.1 Средства управления аудитом информационных систем

Средство управления

Требования к аудиту и деятельности, включающей в себя проверки в операционных системах, должны быть тщательно спланированы и согласованы для того, чтобы минимизировать риск срывов деловых процессов.

Руководство по реализации

Надо обратить внимание на следующие руководящие указания:

- a) требования к аудиту должны быть согласованы с соответствующим руководством;
- b) область проверок должна быть согласована и должна контролироваться;
- c) проверки должны быть ограничены доступом «только для чтения» к программному обеспечению и данным;
- d) доступ, отличающийся от доступа «только для чтения», должен быть разрешен только для изолированных копий системных файлов, которые должны быть стерты по завершении аудита, или наделены соответствующей защитой, если в соответствии с требованиями к документации аудита имеется обязательство сохранять такие файлы;
- e) ресурсы для выполнения проверок должны быть четко определены и сделаны доступными;
- f) требования для специальной или дополнительной обработки должны быть определены и согласованы;
- g) весь доступ должен постоянно контролироваться и протоколироваться в целях создания контрольного следа; для критических данных или систем должно быть рассмотрено использование контрольного следа с отметкой времени;
- h) все процедуры, требования и обязанности должны быть документально подтверждены;
- i) лицо (лица), выполняющие аудит, должны быть независимыми от проверяемой деятельности.

15.3.2 Защита инструментальных средств аудита информационных систем

Средство управления

Доступ к инструментальным средствам аудита информационных систем должен быть защищен для того, чтобы предотвратить любое возможное неправильное использование или подвергание риску.

Руководство по реализации

Инструментальные средства аудита информационных систем, например, программное обеспечение или файлы данных, должны быть отделены от систем разработки и операционных систем и не должны содержаться в библиотеках на лентах или областях пользователя, если только им не придан надлежащий уровень дополнительной защиты.

Прочая информация

Если в аудит вовлечены третьи стороны, то может иметься риск неправильного использования инструментальных средств аудита этими третьими сторонами, и информации, к которой осуществляется доступ этой организацией третьей стороны. Для того чтобы учесть этот риск, могут быть рассмотрены средства управления, такие как 6.2.1 (для оценки рисков) и 9.1.2 (для ограничения физического доступа), и должны быть предприняты какие-либо действия, такие как немедленное изменение паролей, раскрытий аудиторам.

Библиография

- ISO/IEC Guide 2:1996, Standardization and related activities – General vocabulary
- ISO/IEC Guide 73:2002, Risk management – Vocabulary – Guidelines for use in standards
- ISO/IEC 13335-1:2004, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management
- ISO/IEC TR 13335-3:1998, Information technology – Guidelines for the Management of IT Security – Part 3: Techniques for the management of IT Security
- ISO/IEC 13888-1: 1997, Information technology – Security techniques – Non-repudiation – Part 1: General
- ISO/IEC 11770-1:1996 Information technology – Security techniques – Key management – Part 1: Framework
- ISO/IEC 9796-2:2002 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms
- ISO/IEC 9796-3:2000 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms
- ISO/IEC 14888-1:1998 Information technology – Security techniques – Digital signatures with appendix – Part 1: General
- ISO/IEC 15408-1:1999 Information technology – Security techniques – Evaluation Criteria for IT security – Part 1: Introduction and general model
- ISO/IEC 14516:2002 Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services
- ISO 15489-1:2001 Information and documentation – Records management – Part 1: General
- ISO 10007:2003 Quality management systems – Guidelines for configuration management
- ISO/IEC 12207:1995 Information technology – Software life cycle processes
- ISO 19011:2002 Guidelines for quality and /or environmental management systems auditing
- OECD Guidelines for the Security of Information Systems and Networks: ‘Towards a Culture of Security’, 2002
- OECD Guidelines for Cryptography Policy, 1997
- IEEE P1363-2000: Standard Specifications for Public-Key Cryptography
- ISO/IEC 18028-4 Information technology – Security techniques – IT Network security – Part 4: Securing remote access
- ISO/IEC TR 18044 Information technology – Security techniques – Information security incident

Индекс

А

- авторизации, процесс 6.1.4
- авторское право
 - ПИС 15.1.2
 - на программное обеспечение 15.1.2
- актив 2.1
 - приемлемое использование активов 7.1.3
 - опись активов 7.1.1
 - менеджмент 7
 - собственность на активы 7.1.2
 - ответственность за активы 7.1
 - возврат активов 8.3.2
- анализ
 - защиты информации 6.1.8
 - политики в области защиты информации 5.1.2
 - и постоянный контроль услуг третьей стороны 11.2.4
- аудит
 - соображения, касающиеся информационных систем 15.3
 - средства управления аудитом информационных систем 15.3.1
 - ведение контрольного журнала 10.10.1
 - инструментальные средства защиты аудита, 12.3.2
- аутентификация
 - пользователей 11.5.2
 - пользователей, для внешних соединений 11.4.3
- аутентичность 2.5
- аутсорсинговая разработка программного обеспечения 12.5.5

Б

- безопасные зоны 9.1
 - работа в безопасных зонах 9.1.5
- безопасные процедуры входа в систему 11.5.1
- бизнес, информационные системы для бизнеса 10.8.5
- бизнеса, непрерывность 14
 - менеджмент непрерывности бизнеса 14
 - менеджмент аспектов непрерывности бизнеса, связанных с защитой информации 14.1
 - процесс менеджмента непрерывности бизнеса для включения информационной защиты 14.1.1
 - планирование непрерывности бизнеса, структура 14.1.4
 - планы, разработка и реализация непрерывности бизнеса, 14.1.3
 - непрерывность бизнеса и оценка рисков 14.1.2
 - испытание, обслуживание и повторная оценка планов непрерывности бизнеса 14.1.5
- блокировка сеанса по превышению лимита времени 11.5.5

В

- валидация
 - входных данных 12.2.1
 - выходных данных 12.2.4

внешние стороны 6.2
выявление рисков, связанных с внешними сторонами 6.2.1
внутренняя организация 6.1
во время работы по найму 8.2
возврат активов 8.3.2
вспомогательные коммунальные службы 9.2.2
вынос имущества 9.2.7
выявление рисков, связанных с внешними сторонами 6.2.1

Д

дисциплинарный процесс 8.2.3
доказательств, сбор 13.2.3
документированные процедуры эксплуатации 10.1.1
доступность 2.5

Ж

журналы оператора и администратора 10.10.4

З

защита
данных журнала 10.10.3
от злонамеренного и мобильного кода 10.4
организационных записей 14.1.3
защита инструментальных средств аудита информационных систем 15.3.2
испытательных данных системы 12.4.2
в процессах разработки и вспомогательных процессах 12.5
человеческих ресурсов 8
оборудования 9.2
оборудования, находящегося за пределами рабочего места 9.2.5
сетевых услуг 10.6.2
политика в области защиты 5
политика в области защиты, соответствие ей 15.2.1
анализ и спецификация требований защиты 12.1.1
системной документации 10.7.4
системных файлов 12.4
недостатки защиты, составление отчетов о них 13.1.2
защита организационных записей 15.1.3
от вирусов 10.4
от внешних и экологических угроз 9.1.4
офисов, комнат и средств 9.1.3
системной документации 10.7.4
удаленных диагностических портов 11.4.4
человеческих ресурсов 8

защита данных и секретность личной информации 15.1.4

защита информации 2.5
осведомленность, образование и подготовка в области защиты информации 8.2.2
координация защиты информации 6.1.2
событие в системе защиты информации 2.6, 13.1
составление отчетов о событиях в системе защиты информации 13.1.1
инцидент в системе защиты информации 2.7, 13.2
извлечение уроков из инцидентов в системе защиты информации 13.2.2
включение защиты информации в процесс менеджмента непрерывности бизнеса 14.1.1
разработка и реализация планов обеспечения непрерывности, включающих защиту
информации 14.1.3
организация защиты информации 6
политика в области защиты информации 5.1
программный документ в области защиты информации 5.1.1

злонамеренный код
средства управления против злонамеренного кода 10.4.1
защита от злонамеренного кода 10.4

зона погрузки 9.1.6
зона поставки 9.1.6

И

идентификация
оборудования в сетях 11.4.3
пользователей 11.5.2

идентификация применимых законов 15.1.1
извлечение уроков из инцидентов в системе защиты информации 13.2.2

изменение
процедуры управления для изменений 12.5.1
изменение места работы по найму 8.3
менеджмент изменений 10.2.1
анализ изменений операционных систем 12.5.2
ограничения на изменения в пакетах программ 12.5.3
в услугах третьей стороны, менеджмент 10.2.3

изоляция важных систем 11.6.2
имущество, вынос имущества 9.2.7

информация
ограничение доступа к информации 11.6.1
резервное копирование информации 10.5.1
классификация информации 7.2
обмен информацией 10.8
политика и процедуры обмена информацией 10.8.1
процедуры обращения с информацией 10.7.3
маркировка информации и обращение с информацией 7.2.2
утечка информации 12.5.4
информация, сделанная общедоступной 10.9.3
средства обработки информации 2.4
средства обработки информации их неправильное использование 15.1.5
приобретение, разработка и обслуживание информационных систем 12
средства управления аудитом информационных систем 15.1.3
защита инструментальных средств аудита информационных систем 15.3.2
информационные системы для бизнеса 10.8.5

испытание, обслуживание и повторная оценка планов обеспечения непрерывности бизнеса 14.1.5
испытательные данные системы, защита 12.4.2
исходный код программы, управление доступом к исходному коду программы 12.4.3

К

классификация

руководящие указания по классификации 7.2.1
классификация информации 7.2

контакт

с органами 6.1.6
со специальными группами 6.1.7

контрольные журналы

журналы оператора и администратора 10.10.4
ведение контрольного журнала 10.10.1
регистрация отказов 10.10.5
защита данных журнала 10.10.3

конфиденциальность 2.5

криптографические средства 12.3

политика по использованию криптографических средств управления 12.3.1
регулирование криптографических средств управления 15.1.6

Л

ликвидация

оборудования 9.2.6
носителей информации 10.7.2

личная информация, секретность личной информации 15.1.4

М

маркировка информации и обращение с информацией 7.2.2

менеджмент

активов 7
непрерывности бизнеса 14
производительности 10.3.1
изменений 10.1.2
изменений в услугах третьей стороны 10.2.3
обязательств по защите информации 6.1.1
средств связи и операций 10
криптографических ключей 12.3.2
аспекты менеджмента непрерывности бизнеса, связанные с защищкой информации 14.1
инцидентов в системе защиты информации 13, 13.2
защиты сетей 10.6
привилегий 11.2.2
сменных носителей информации 10.7.1
система менеджмента паролей 11.5.3
технических слабых мест 12.6
доступа пользователей 11.2
средств связи и операций 10

мобильная обработка 11.7

мобильная обработка и связь 11.7.1

мобильный код

средства управления против мобильного кода 10.4.2
защита от мобильного кода 10.4

Н

надежность 2.5

независимый анализ защиты информации 6.1.8

неотрекаемость 2.5

услуг 12.3.1

неправильное использование средств обработки информации, предотвращение 15.1.5

носитель информации

ликвидация носителей информации 10.7.2
обращение с носителями информации с 10.7
носители информации при транспортировке 10.8.3
сменные носители информации 10.7.1

О

обмен

соглашения об обмене 10.8.2
обмен информацией 10.8
политика и процедуры обмена информацией 10.8.1

обмен сообщениями, электронный 10.8.4

оборудование

идентификация оборудования в сетях 11.4.3
обслуживание 9.2.4
защита оборудования 9.2
защита оборудования, находящегося за пределами рабочего места 9.2.5
безопасная ликвидация или повторное использование оборудования 9.2.6
расположение и защита оборудования 9.2.1
оборудование, находящееся без присмотра 11.3.2

оборудование пользователя, находящееся без присмотра 11.3.2

обслуживание

оборудования 9.2.4
приобретение, разработка и обслуживание информационных систем 12

общедоступная информация 10.9.3

обязанности

распределение обязанностей по защите информации 6.1.3
и роли 8.1.1
руководства 8.2.1
рабочие 10.1
пользователя 11.3
разделение 10.1.3

обязательства, связанные с прекращением работы по
найму 8.3.1

ограничение времени соединения 11.5.6

ограничения на изменения в пакетах программ 12.5.3

онлайневые сделки 10.9.2

операционная система

управление доступом к операционной системе 11.5
технический анализ приложений после изменений операционной системы 12.5.3

опись активов 7.1.1

органы, контакт с органами 6.1.6

осведомленность, образование и подготовка в области защиты информации 8.2.2

отбор 8.1.2

открытый доступ, зоны открытого доступа, поставки и погрузки 9.1.6

П

пароли

менеджмент паролей пользователя 11.2.3
система менеджмента паролей 11.5.3
использование паролей 11.3.1

перед началом работы по найму 8.1

планы обеспечения непрерывности бизнеса
разработка и реализация планов обеспечения непрерывности 14.1.3
испытание, обслуживание и повторная оценка планов обеспечения непрерывности бизнеса 14.1.5

повторное использование оборудования 9.2.6

подотчетность 2.5

политика 2.8
управления доступом 11.1
чистого стола и чистого экрана 11.3.2
обмена информацией 10.8.1
в области защиты информации 5.1
по использованию криптографических средств управления 12.3.1
в отношении использования сетевых услуг 11.4.1
в области защиты 5

политика и стандарты в области, соответствие им 15.2, 15.2.1

политика чистого стола и чистого экрана, 11.3.3

пользователь
менеджмент доступа пользователей 11.2
анализ прав доступа пользователя 11.2.4
автентификация для внешних соединений 11.2.4
идентификация и автентификация 11.5.2
менеджмент паролей 11.2.3
регистрация 11.2.1
обязанности 11.3
оборудование пользователя, находящееся без присмотра 11.3.2

постоянный контроль
10.10
и анализ услуг третьей стороны 10.2.2
использования систем 10.10.2

потребители, рассмотрение защиты при работе с потребителями 6.2.2

права доступа
удаление прав доступа 8.3.3
анализ прав доступа 11.2.4

права на интеллектуальную собственность 15.1.2

правильная обработка в приложениях 12.2

предоставление услуг 10.2.1
менеджмент предоставления услуг третьей стороны 10.2.1

превращение неправильного использования средств обработки информации 15.1.5

прекращение работы по найму 8.3

приемлемое использование активов 7.1.3

применение
управление доступом к системе 11.6
правильная обработка в приложениях 12.2
анализ, после изменений в операционной системе 12.5.2

приобретение, разработка и обслуживание информационных систем 12

программное обеспечение
аутсорсинговая разработка программного обеспечения 12.5.5
управление системным программным обеспечением 12.4.1
ограничения на изменения в пакетах программ 12.5.3

процедуры
управления изменениями 12.5.1
обмена информацией 10.8.1
обращения с информацией 10.7.3
входа в систему 11.5.3
эксплуатационные 10.1, 10.1.1
и обязанности менеджмента инцидентов 13.2.1

процедуры эксплуатации и рабочие обязанности 10.1
процедуры эксплуатации, документированные 10.1.1
процессы разработки и вспомогательные процессы, защита в них 12.5
прочая информация 3.2

P

работка в безопасных зонах 9.1.5
работка на дому
защита оборудования 9.2.5
защита телеобработки 11.7.2
работка по найму
во время работы по найму 8.2
перед началом работы по найму 8.1
прекращение работы по найму 8.3
разделение обязанностей 10.1.3
в сетях 11.4.5
разделение средств разработки, испытания и эксплуатации 10.1.4
разработка
приобретение, разработка и обслуживание информационных систем 12
разделение средств разработки, испытания и эксплуатации 10.1.4
программного обеспечения, аутсорсинговая 12.5.5
защита в процессах разработки и вспомогательных процессах 12.5
расположение оборудования 9.2.1
распределение ключей 12.3.2
распределение обязанностей по защите информации 6.1.3
регистрация отказов 10.10.5
регулирование криптографических средств управления 15.1.6
резервное копирование 10.5
информации 10.5.1
риск 2.9
анализ 2.10
оценка 2.11, 4.1
оценка рисков и непрерывность бизнеса 14.1.2
оценка значительности 2.12
менеджмент 2.13
обработка 2.14, 4.2
роли и обязанности 8.1.1
руководство по реализации 3.2
руководящий принцип 2.3

C

сбор доказательств 13.2.3
сделки, онлайновые 10.9.2

сеть
управления доступом в сеть 11.4
управление сетевыми соединениями 11.4.6
средства управления сетью 10.6.1
идентификация оборудования в сетях 11.4.3
управление сетевой маршрутизацией 11.4.7
менеджмент защиты сети 10.6
разделение в сетях 11.4.5
сетевые услуги, политика в отношении их использования 11.4.1
защита сетевых услуг 10.6.2

синхронизация часов 10.10.6

система
приемка 10.3.2
приобретение, разработка и обслуживание 12
соображения, касающиеся аудита 15.3
средства управления аудитом 15.3.1
защита инструментальных средств аудита 15.3.2
защита системной документации 10.7.4
защита системных файлов 12.4
планирование и приемка 10.3
испытательные данные системы, защита 12.4.2
использование систем, постоянный контроль использования систем 10.10.2
системные утилиты, использование 11.5.4

системные утилиты 11.5.4

слабое место 2.17
менеджмент технических слабых мест 12.6
управление техническими слабыми местами 12.6.1

сменные носители информации, менеджмент сменных носителей информации 10.7.1

собственность на активы 7.1.2

соглашения
учитывающие защиту у третьей стороне 6.2.3
об обмене 10.8.2
о конфиденциальности 6.1.5

соответствие 15
юридическим требованиям 15.1
политике и стандартам в области защиты 15.2, 15.2.1
проверка технического соответствия 15.2.2

составление отчетов
о событиях в системе защиты информации 13.1, 13.1.1
о недостатках в системе защиты информации 13.1, 13.1.2

средства управления физическим доступом 9.1.2

структура планирования непрерывности бизнеса 14.1.4

T

тайм-аут 11.5.5

телеобработка 11.7, 11.7.2

технический
техническое соответствие 15.2.2
технический анализ приложений после изменений операционной системы 12.5.2
управление техническими слабыми местами 12.6.1
менеджмент технических слабых мест 12.6

третья сторона 2.15
учет защиты в соглашениях с третьими сторонами 6.2.3
менеджмент предоставления услуг третьей стороны 10.2
менеджмент изменений в услугах третьей стороны 10.2.3
постоянный контроль и анализ услуг третьей стороны 10.2.2

У

угроза 2.16

удаление прав доступа
8.3.3

управление 2.2, 3.2

средства управления против злонамеренного кода 10.4.1
средства управления против мобильного кода 10.4.2
внутренней обработкой 12.2.2
системным программным обеспечением 12.4.1
сетевой маршрутизацией 11.4.7
сетевыми соединениями 11.4.6

управление доступом 11

к прикладным системам 11.6
деловые требования к управлению доступом 11.1
к информации 11.6, 11.6.1
к сетям 11.4
к операционным системам 11.5
политика управления доступом 11.1.1
к исходному коду программы 12.4.3

условия работы по найму 8.1.3

услуги электронной торговли 10.9

утечка информации 12.5.4

Ф

физический

физическая и экологическая безопасность 9
средства управления физическим доступом 9.1.2
физические носители при транспортировке 10.8.3
физический периметр безопасности

Ц

целостность

сообщений 12.2.3

Э

электронная

торговля 10.9.1
услуги электронной торговли 10.9
обмен сообщениями 10.8.4