АКЦИОНЕРНОЕ ОБЩЕСТВО
«Гарнизон»

УТВЕРЖДАЮ
ВрИО Генерального директора
АО «Гарнизон»

_____ С.А.Штыкулин
«_31_» _07_____ 2015 г.

СТАНДАРТ ОРГАНИЗАЦИИ

СТО СМК.22-2015

Система менеджмента качества

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Экз. № _____

Москва
2015

Предисловие

Сведения о стандарте

1 РАЗРАБОТАН отделом лицензионно-разрешительной работы Главного управления производства и реализации государственного оборонного заказа АО «Гарнизон» совместно с сектором администрирования компьютерных сетей и технической поддержки отдела общего обеспечения Управления делами АО «Гарнизон».

2 ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ приказом Генерального директора АО «Гарнизон» от «31» 07 2015 года № 104

3 ВВЕДЕН ВПЕРВЫЕ

Настоящий Стандарт является интеллектуальной собственностью АО «Гарнизон» и не может быть передан сторонней организации, юридическому или физическому лицу без разрешения Генерального директора.

Содержание

1 Область применения....1
2 Нормативные ссылки....1
3 Термины, определения, обозначения и сокращения....2
4 Ответственность и контроль....3
5 Описание процедуры....3
6 Учет, хранение....8
7 Внесение изменений....8
8 Распределение....8
Приложение А (информационное)....10
Приложение Б (рекомендуемое)....57
Приложение В (рекомендуемое)....58
Приложение Г (рекомендуемое)....59
Библиография....60
Лист регистрации изменений....61

1 Область применения

1.1 Настоящий стандарт:

- определяет порядок организации и выполнения работ по защите информации об образцах военной продукции, учитывающий характер и условия выполнения оборонного заказа при несанкционированном воздействии на информацию, циркулирующую в технических каналах;
- определяет требования к управлению информационной безопасностью в организации.

1.2 АО «Гарнизон» не разрабатывает и не производит изделия информационных технологий в защищенном исполнении, предназначенные для применения в военной продукции, в связи с этим процедуры обеспечения и контроля безопасности технологий их разработки и производства в соответствии с требованиями п. 4.3.4 ГОСТ РВ 0015-002-2012 не разрабатывались.

1.3 Требования стандарта обязательны для всех структурных подразделений организации, участвующих в выполнении государственного оборонного заказа.

1.4 Настоящий стандарт разработан с учетом требований ГОСТ ISO 9001-2011 и ГОСТ РВ 0015-002-2012.

1.5 При разработке стандарта были использованы отдельные положения ГОСТ Р ИСО/МЭК 27001-2006.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

- ГОСТ РВ 0015-002-2012 Система разработки и постановки на производство военной техники. Системы менеджмента качества. Общие требования;
- ГОСТ ISO 9001-2011 Системы менеджмента качества. Требования;
- ГОСТ Р ИСО/МЭК 27001–2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
- ГОСТ РВ 50859-2010
- ГОСТ РВ 50934-2010
- СТО СМК.02-2015 Система менеджмента качества. Управление документацией;
- СТО СМК.01-2015 Система менеджмента качества. Стандарты организации. Порядок разработки, оформления, внесения изменений, хранения и актуализации;
- СТО СМК.03-2015 Система менеджмента качества. Управление записями.

3 Термины, определения, обозначения и сокращения

3.1 Термины и определения

3.1.1 **Требование**: потребность или ожидание, которое установлено, обычно предполагается или является обязательным.

3.1.2 **Доступность**: свойство объекта находиться в состоянии готовности и возможности использования по запросу авторизованного логического объекта.

3.1.3 **Несоответствие**: невыполнение требования.

3.1.4 **Коррекция**: действие, предпринятое для устранения обнаруженного несоответствия.

3.1.5 **Корректирующее действие**: действие, предпринятое для устранения причины обнаруженного несоответствия или другой нежелательной ситуации.

3.1.6 **Предупреждающее действие**: действие, предпринятое для устранения причины потенциального несоответствия или другой потенциально нежелательной ситуации

3.1.7 **Конфиденциальность**: свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса.

3.1.8 **Информационная безопасность (ИБ)**: свойство информации сохранять конфиденциальность, целостность и доступность.

3.1.9 **Событие информационной безопасности**: идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью.

3.1.10 **Инцидент информационной безопасности**: любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Примечание: инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций ИБ;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушения правил доступа.

3.1.11 **Активы**: все, что имеет ценность для организации.

3.2 Обозначения и сокращения

АО – акционерное общество;

АСУП – автоматизированная система управлением предприятия;

ВП – военное представительство;

ВТ – военная техника;

ГОСТ – государственный стандарт;
ДС – документы по стандартизации;
ИБ – информационная безопасность;
ИТР – иностранная техническая разведка;
НД – нормативная документация;
ОЛРР – отдел лицензионно-разрешительной работы;
ОПДИТР – отдел противодействия иностранным техническим разведкам;
Отд. ЗГТ – отдел защиты государственной тайны, режима и мобилизации;
РФ – Российская Федерация;
САКСиТП – сектор администрирования компьютерных сетей и технической поддержки;
СМК – система менеджмента качества;
СТО – стандарт организации;
ПДТК – постоянно действующая техническая комиссия;
ПЭМИН – побочные электромагнитные излучения наводки.

4 Ответственность и контроль

4.1 Ответственность за разработку данного стандарта возлагается на ОЛРР.

4.2 Ответственность за организацию работ по защите информации об образцах военной продукции возлагается на Генерального директора АО «Гарнизон».

4.3 Ответственность за обеспечение режима секретности в организации согласно Инструкции [1] возлагается на Генерального директора АО «Гарнизон».

4.4 Ответственность за организацию управления информационной безопасностью организации возлагается на заместителя Генерального директора (по вопросам управления и производственной деятельности).

4.5 Контроль выполнения требований стандарта возлагается на заместителя Генерального директора (по вопросам управления и производственной деятельности).

5 Описание процедуры

5.1 Общие положения

5.1.1 Порядок организации и осуществления работ по защите информации (относящейся к сведениям, составляющим государственную тайну) об образцах военной продукции, учитывающий характер и условия выполнения оборонного заказа при несанкционированном воздействии на информацию, циркулирующую в технических каналах излагается в специально разрабатываемой в соответствии с требованиями ГОСТ РВ 50859-2010, ГОСТ РВ 50934-2010 документации.

Обеспечение информационной безопасности в АО «Гарнизон» при обработке секретной информации техническими средствами регламентируется Инструкцией[2].

Порядок обеспечения внутриобъектового и пропускного режима изложен в Инструкции [3].

5.1.2 Процедура управления информационной безопасностью организации в отношении активов, не относящимся к сведениям, составляющим государственную тайну, изложена в настоящем стандарте.

5.1.3 Цель процедуры управления информационной безопасностью – обеспечить конфиденциальность, целостность и доступность информации, циркулирующей в организации с конечной целью защиты активов организации.

5.1.4 Основные задачи процедуры:

- обеспечение участия высшего руководства организации в решении вопросов, связанных с обеспечением информационной безопасности в соответствии с целями организации, законами и нормативными актами;
- предотвращение несанкционированного физического доступа, повреждений и воздействий на имущество и информацию организации, а также имущества, принадлежащего потребителю (заказчику);
- предотвращение потерь, повреждений, хищений или компрометации активов и прекращение деятельности организации;
- обеспечение надлежащего и безопасного функционирования средств обработки информации;
- защита целостности программного обеспечения и массивов информации;
- предотвращение несанкционированного разглашения, модификации, удаления или уничтожения активов и прерывание процессов СМК;
- обнаружение несанкционированных действий, связанных с обработкой информации;
- предотвращение несанкционированного доступа пользователей, а также компрометацию или кражу информации и средств обработки информации;
- обеспечение оперативного оповещения о событиях информационной безопасности и нарушениях, связанных с информационными системами, а также своевременное проведение коррекции и корректирующих действий.

5.1.5 Действия по управлению информационной безопасностью включает в себя:

- планирование;
- выявление событий и инцидентов ИБ;
- идентификацию и регистрацию событий и инцидентов ИБ;
- анализ событий и инцидентов ИБ;
- планирование и осуществление необходимых корректирующих и предупреждающих действий;
- оценка результативности принятых действий.

5.1.6 Осуществление действий по управлению информационной безопасностью производят должностные лица организации, указанные в Политике информационной безопасности АО «Гарнизон», приведенной в приложении А.

Указанные должностные лица назначаются на должность приказом Генерального директора, их обязанности изложены в соответствующих должностных инструкциях.

5.1.7 Организацией разработана и принята «Политика информационной безопасности» (далее – Политика), которая определяет цели, основные направления и принципы действий в сфере ИБ. Политика приведена в приложении А и утверждается Генеральным директором, либо в составе стандарта, либо отдельно (в случае необходимости издания отдельным документом).

Политика доводится под подпись до работников АО «Гарнизон» в части касающейся.

Пересмотр Политики с учетом появления новых рисков, производится не реже 1 раза в три года.

5.2 Планирование.

5.2.1 Планирование работ по обеспечению информационной безопасности осуществляется путем оформления ежегодных планов (Приложение Б).

План на последующий год составляет специалист по ИБ до 25 декабря текущего года.

5.2.2 Планирование внутренних аудитов обеспечения информационной безопасности также осуществляется путем оформления ежегодных планов (Приложение В).

План на последующий год составляет специалист по ИБ до 25 декабря текущего года.

5.3 Выявление событий и инцидентов ИБ производится:

- участниками обработки активов (в том числе информационных) в период осуществления деятельности;
- вневедомственной охраной (при наличии);
- работниками САКСиТП;
- во время проведения периодических и летучих контролей специалистов по ИБ;
- во время проведения внутренних и внешних аудитов ИБ.

События и инциденты ИБ может также выявлять ВП.

5.4 Идентификация и регистрация событий и инцидентов ИБ производится:

- докладными или служебными записками участников обработки активов, персонала отд. ЗГТ;
- оформлением записей в журналах периодических и летучих контролей;
- оформлением записей по результатам внутренних и внешних аудитов ИБ.

5.5 Анализ событий и инцидентов ИБ.

5.5.1 Анализ событий и инцидентов ИБ производится:

- специалистом по ИБ;
- начальником отд. ЗГТ;
- заместителем Генерального директора (по вопросам управления и производственной деятельности);
- Генеральным директором.
- на совещаниях и заседаниях ПДТК.

5.5.2 Состав ПДТК утверждается Генеральным директором не позднее первой декады января текущего года.

В состав ПДТК входят:

- заместитель Генерального директора (по вопросам управления и производственной деятельности);
- заместитель Генерального директора - представитель руководства по качеству;
- специалист по ИБ;
- начальник отд. ЗГТ;
- руководители основных подразделений организации, участвующих в обеспечении информационной безопасности.

Представители ВП включаются в состав комиссии по согласованию с начальником ВП.

Председатель ПДТК в зависимости от рассматриваемых вопросов имеет право:

- привлекать к участию в работе комиссии любых специалистов организации;
- поручать руководителям подразделений (должностным лицам) организации подготовку справочных материалов по вопросам, рассматриваемым на заседаниях ПДТК.

Проект приказа по объявлению состава ПДТК и ее задач ежегодно готовит специалист по ИБ.

5.5.3 Заседание ПДТК проводится не реже 1 раза в квартал. Оформление рассмотренных вопросов и назначенных действий производится решением согласно приложения Д. Решения оформляются секретарем ПДТК в течение трех рабочих дней после проведения заседания и при необходимости могут объявляться в приказах Генерального директора. Решение согласовывается с ВП при участии в заседании его представителя.

5.5.4 Ответственность за организацию проведения заседания ПДТК возлагается на председателя ПДТК.

Дату (с учетом п.5.5.3), время и место проведения заседания ПДТК определяет Генеральный директор по предложению его заместителя (по вопросам управления и производственной деятельности). Секретарь ПДТК доводит эту информацию до лиц, участвующих в заседании, за 5 дней до начала проведения.

5.5.5 Особо важные вопросы обеспечения информационной безопасности могут быть рассмотрены на внеочередных заседаниях ПДТК. Решение о созыве и сроках внеочередного заседания ПДТК принимает Генеральный директор. Секретарь ПДТК ставит в известность о внеочередном заседании все заинтересованные подразделения и ВП (по военной продукции) за 2 дня до заседания для подготовки и внесения предложений.

5.5.6 В состав задач ПДТК входят:

- координация вопросов обеспечения информационной безопасности;
- рассмотрение и одобрение «Политики информационной безопасности» и ее изменений;

- рассмотрение общих вопросов обеспечения информационной безопасности, в том числе результатов анализа событий и инцидентов ИБ;
- рассмотрение вопросов по совершенствованию форм и методов обеспечения информационной безопасности, в том числе вопросы подготовки (повышения квалификации) персонала и обновления технических средств;
- анализ мероприятий и их результативности по устранению причин событий и инцидентов ИБ;
- контроль исполнения плановых документов в области ИБ и «Политики информационной безопасности»;
- контроль разработки, корректировки и внедрения документов в области ИБ;
- рассмотрение и выработка рекомендаций по совершенствованию «Политики информационной безопасности», составу и содержанию документов в области ИБ;
- рассмотрение несоответствий обеспечения информационной безопасности, выявленных при внешних и внутренних аудитах;
- принятие необходимых корректирующих и предупреждающих действий;
- анализ рисков возникновения угроз информационной безопасности.

5.6 Планирование и осуществление необходимых корректирующих и предупреждающих действий осуществляются согласно:

- решений ПДТК;
- приказов Генерального директора;
- распоряжений заместителя Генерального директора (по вопросам управления и производственной деятельности);
- планов корректирующих действий подразделений по результатам внутренних аудитов.

Отчеты о выполнении запланированных мероприятий направляются руководителями подразделений служебными записками специалисту по ИБ, который докладывает обобщенные данные заместителю Генерального директора (по вопросам управления и производственной деятельности).

5.7 Управление документацией и записями в процессе выполнения работ по обеспечению информационной безопасности производится в соответствии с СТО СМК.02, СТО СМК.03 с назначением необходимых ограничений по праву доступа (гриф документа, записи).

5.8 Оценка результативности принятых действий.

5.8.1 Оценка результативности принятых действий проводится ежеквартально заместителем Генерального директора (по вопросам управления и производственной деятельности) на основании докладов специалиста по ИБ и докладывается на очередном заседании ПДТК.

5.9 Основные критерии результативности процедуры:

- отсутствие нарушений конфиденциальность, целостность и доступность информации, циркулирующей в организации.

5.9.1 Оценка результативности процедуры проводится ежеквартально заместителем Генерального директора (по вопросам управления и производственной деятельности) и докладывается на очередном заседании

ПДТК или других совещаниях, проводимых Генеральным директором. Также оценка результативности процедуры проводится во время внутренних и внешних аудитов.

6 Учет, хранение

6.1 Учет и хранение настоящего стандарта осуществляется в соответствии с требованиями СТО СМК.01.

7 Внесение изменений

7.1 Внесение изменений в настоящий стандарт осуществляется в соответствии с требованиями СТО СМК.01.

8 Распределение

8.1 Данный стандарт распределяется во все подразделения организации, ВП.

Разработал:
Главный специалист отдела лицензионно – разрешительной работы Главного управления производства и реализации государственного оборонного заказа — Д.Н.Картавцев

«09» 07 2015 г.

Согласовано:
Заместитель Генерального директора – представитель руководства по СМК — С.И.Тен

«__» _____ 2015 г.

Начальник Главного управления производства и реализации государственного оборонного заказа — С.А.Хрусталев

«09» 07 2015 г.

Начальник отдела лицензионно – разрешительной работы Главного управления производства и реализации государственного оборонного заказа — А.А.Анохин

«09» 07 2015 г.

Начальник отдела защиты государственной тайны, режима и мобилизации — О.А.Пищиков

«10» 07 2015 г.

Начальник Управления делами А.Г.Клюшкин

«09». 07. 2015 г.

Начальник отдела общего обеспечения
Управления делами С.А.Рудяк

«09» 07 2015 г.

Заместитель начальника отдела - заведующий
сектором администрирования компьютерных
сетей и технической поддержки отдела
общего обеспечения Управления делами А.В.Бобровников

«09» 07 2015 г.

Приложение А
(информационное)

АКЦИОНЕРНОЕ ОБЩЕСТВО
«Гарнизон»

УТВЕРЖДАЮ

ВрИО Генерального директора
АО «Гарнизон»

_____ С.А.Штыкулин

«____»_____ 2015 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АО «Гарнизон»

Москва
2015

СОДЕРЖАНИЕ

1 Область применения.....12
2 Нормативные ссылки .....**Ошибка! Закладка не определена.**
3 Термины, определения, обозначения и сокращения.....12
4 Назначение и правовая основа документа 19
5 Объекты защиты 20
6 Цели и задачи обеспечения безопасности информации.....22
7 Основные угрозы безопасности информации 25
8 Основные принципы построения системы информационной безопасности ...32
9 Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов.....38
10 Порядок утверждения, внесения изменений и дополнений.....55

1 Область применения

1 Настоящая Политика определяет цели, основные направления и принципы действий в сфере информационной безопасности АО «Гарнизон».

2 Термины, определения, обозначения и сокращения

2.1 Термины и определения

2.1.1 Автоматизированная система обработки информации – организационно - техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов: технических средств обработки и передачи данных (средств вычислительной техники и связи), методов и алгоритмов обработки в виде соответствующего программного обеспечения, массивов (наборов, баз) данных на различных носителях, персонала и пользователей, объединенных по организационно - структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных с целью удовлетворения информационных потребностей потребителей информации.

2.1.2 Авторизованный субъект доступа - субъект, которому предоставлены соответствующие права доступа к объектам системы (полномочия).

2.1.3 Администратор безопасности - лицо или группа лиц, ответственных за обеспечение безопасности системы, за реализацию и непрерывность соблюдения установленных административных мер защиты и осуществляющих постоянную организационную поддержку функционирования применяемых физических и технических средств защиты.

2.1.4 Атака на информационную систему - любое действие, выполняемое нарушителем, которое приводит к реализации угрозы, путем использования уязвимостей системы.

2.1.5 Безопасность информации - защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

2.1.6 Безопасность любого ресурса информационной системы - складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности, кроме того также могут быть включены другие, такие как аутентичность, подотчетность, неотрекаемость, надежность.

2.1.7 Конфиденциальность компонента системы - заключается в том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.

2.1.8 Целостность компонента предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права. Целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени.

2.1.9 Доступность компонента означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

2.1.10 Внешний воздействующий фактор - воздействующий фактор, внешний по отношению к объекту информатизации.

2.1.11 Внутренний воздействующий фактор - воздействующий фактор, внутренний по отношению к объекту информатизации.

2.1.12 Вредоносные программы - программы или измененные программы объекта информатизации, приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации или нарушению работы.

2.1.13 Защищаемое помещение - помещение для размещения технических средств защищенного объекта информатизации, а также помещение, предназначенное для проведения семинаров, совещаний, бесед и других мероприятий, в котором циркулирует конфиденциальная речевая информация.

2.1.14 Доступ к информации - ознакомление с информацией или получение возможности ее обработки. Доступ к информации регламентируется ее правовым режимом и должен сопровождаться строгим соблюдением его требований. Доступ к информации, осуществленный с нарушениями требований ее правового режима, рассматривается как несанкционированный доступ.

2.1.15 Доступ к ресурсу - получение субъектом доступа возможности манипулировать (использовать, управлять, изменять характеристики и т.п.) данным ресурсом.

2.1.16 Доступность информации - важнейшее свойство системы, в которой циркулирует информация (средств и технологии ее обработки), характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

2.1.17 Естественные угрозы - это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека.

2.1.18 Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на информацию.

2.1.19 Защита информации от несанкционированного доступа - деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

2.1.20 Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

2.1.21 Злоумышленник - нарушитель, действующий намеренно из корыстных, идейных или иных побуждений.

2.1.21 Информативный сигнал - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта информация ограниченного распространения, передаваемая, хранимая, обрабатываемая или обсуждаемая в выделенных помещениях.

2.1.22 Информация - сведения о предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

2.1.23 Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах.

2.1.24 Информационная среда - совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом отношений.

2.1.25 Информационная система - организационно упорядоченная совокупность документов (массивов документов), независимо от формы их представления, и информационных технологий, в том числе с использованием вычислительной техники и связи. Информационная система включает в себя множество всех документов, существующих в АО «Гарнизон».

2.1.26 Информационные способы нарушения безопасности информации включают:

- противозаконный сбор, распространение и использование информации; манипулирование информацией (дезинформация, сокрытие или искажение информации);
- незаконное копирование информации (данных и программ);
- незаконное уничтожение информации;
- хищение информации из баз и банков данных;
- нарушение адресности и оперативности информационного обмена;
- нарушение технологии обработки данных и информационного обмена.

2.1.27 Искусственные угрозы - это угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

- непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п.;
- преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников).

2.1.28 Компьютерная информация - информация в виде:

- записей в памяти компьютеров, электронных устройствах, на машинных носителях (элементы, файлы, блоки, базы данных, микропрограммы, прикладные и системные программы, пакеты и библиотеки программ, микросхемы, программно-информационные комплексы и др.), обеспечивающих функционирование объекта информатизации (сети);
- сообщений, передаваемых по сетям передачи данных;
- программно-информационного продукта, являющегося результатом генерации новой или обработки исходной документированной информации,

представляемого непосредственно на экранах дисплеев, на внешних носителях данных (магнитные диски, магнитные ленты, оптические диски, дискеты, бумага для распечатки и т.п.) или через сети передачи данных;

- электронных записей о субъектах прав.

2.1.29 Контролируемая зона - это пространство, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового пропуска, и посторонних транспортных средств.

Границей контролируемой зоны могут являться:

- периметр охраняемой территории;

- ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

В отдельных случаях на период обработки техническими средствами конфиденциальной информации (проведения закрытого мероприятия) контролируемая зона временно может устанавливаться большей, чем охраняемая территория предприятия. При этом должны приниматься организационно-режимные и технические меры, исключающие или существенно затрудняющие возможность ведения перехвата информации в этой зоне.

2.1.30 Конфиденциальность информации - характеристика (свойство) информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.

2.1.31 Корпоративная информационная система - автоматизированная система обработки информации АО «Гарнизон».

2.1.32 Лицензия в области защиты информации - разрешение на право проведения тех или иных работ в области защиты информации.

2.1.33 Морально-этические меры защиты информации - традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

2.1.34 Нарушитель - это лицо (субъект), которое предприняло (пыталось предпринять) попытку несанкционированного доступа к ресурсам системы (попытку выполнения запрещенных ему действий с данным ресурсом) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или с целью самоутверждения и т.п.) и использовавшее для этого различные возможности, методы и средства.

2.1.35 Несанкционированное действие - действие субъекта в нарушение установленных в системе правил обработки информации.

2.1.36 Несанкционированный доступ - доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа.

2.1.37 Объект - пассивный компонент системы, единица ресурса информационной системы, доступ к которому регламентируется правилами разграничения доступа.

2.1.38 Объект защиты - информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Организационно-правовые способы нарушения безопасности информации включают:

- закупку несовершенных, устаревших или неперспективных средств информатизации и информационных технологий;
- невыполнение требований законодательства или нормативных актов и задержки в разработке и принятии необходимых нормативных правовых и технических документов в области безопасности информации.

2.1.39 Организационные меры защиты - это меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации.

2.1.40 Организационный контроль эффективности защиты информации - проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

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

2.1.42 Пароль - слово (набор символов), которое считается известным узкому кругу лиц (одному лицу) и используется для ограничения доступа к информации, в помещение, на территорию;

2.1.43 Пользователь - субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации;

2.1.44 Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе.

2.1.45 Правовые меры защиты информации - действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей.

2.1.46 Программно-математические способы нарушения безопасности информации включают:

- внедрение программ-вирусов;
- внедрение программных закладок как на стадии проектирования системы (в том числе путем заимствования «зараженного» закладками программного продукта), так и на стадии ее эксплуатации, позволяющих осуществить несанкционированный доступ или действия по отношению к информации и системам ее защиты (блокирование, обход и модификация

систем защиты, извлечение, подмена идентификаторов и т.д.) и приводящих к компрометации системы защиты информации.

2.1.47 Радиоэлектронные способы нарушения безопасности информации включают:

- перехват информации в технических каналах ее утечки (побочных электромагнитных излучений, создаваемых техническими средствами обработки и передачи информации, наводок в коммуникациях (сети электропитания, заземления, радиотрансляции, пожарной и охранной сигнализации и т.д.) и линиях связи, путем прослушивания конфиденциальных разговоров с помощью акустических, виброакустических, оптических и лазерных технических средств разведки, прослушивания конфиденциальных телефонных разговоров, визуального наблюдения за работой средств отображения информации);
- перехват и дешифрование информации в сетях передачи данных и линиях связи; внедрение электронных устройств перехвата информации в технические средства и помещения;
- навязывание ложной информации по сетям передачи данных и линиям связи; радиоэлектронное подавление линий связи и систем управления.

2.1.48 Разграничение доступа к ресурсам - это такой порядок использования ресурсов системы, при котором субъекты получают доступ к объектам в строгом соответствии с установленными правилами.

2.1.49 Система информационной безопасности - совокупность (комплекс) специальных мер правового (законодательного) и административного характера, организационных мероприятий, физических и технических (программных и аппаратных) средств защиты, а также специального персонала, предназначенных для обеспечения информационной безопасности.

2.1.50 Средство защиты информации - техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

2.1.51 Субъект - активный компонент системы (пользователь, процесс, программа), действия которого регламентируются правилами разграничения доступа.

2.1.52 Субъекты информационных отношений - государство, государственные органы, государственные, общественные или коммерческие организации (объединения) и предприятия (юридические лица), отдельные граждане (физические лица) и иные субъекты, взаимодействующие с целью совместной обработки информации.

2.1.53 Технические (аппаратно-программные) средства защиты - различные электронные устройства и специальные программы, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

2.1.54 Технология обеспечения информационной безопасности - определенное распределение функций и регламентация порядка их исполнения,

а также порядка взаимодействия подразделений и сотрудников по обеспечению комплексной защиты информационных ресурсов.

2.1.55 Угроза - реально или потенциально возможные действия по реализации опасных воздействующих факторов с целью преднамеренного или случайного (неумышленного) нарушения режима функционирования объекта и нарушения свойств защищаемой информации или других ресурсов объекта.

2.1.56 Угроза безопасности информации - потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию, которое наносит ущерб собственнику, владельцу или пользователю информации.

2.1.57 Угроза интересам субъектов информационных отношений - потенциально возможное событие, действие, процесс или явление, которое посредством воздействия на информацию и другие информационной системы может привести к нанесению ущерба интересам данных субъектов.

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

2.1.59 Уровень защиты (класс и категория защищенности) - характеристика, описываемая в нормативных документах определенной группой требований к данному классу и категории защищенности;

2.1.60 Уязвимость автоматизированной системы - любая характеристика автоматизированной системы, использование которой может привести к реализации угрозы;

2.1.61 Уязвимость информации - подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению ее конфиденциальности, целостности, доступности, или неправомерному ее тиражированию.

2.1.62 Уязвимость субъекта информационных отношений - потенциальная подверженность субъекта нанесению ущерба его жизненно важным интересам посредством воздействия на критичную для него информацию, ее носители и процессы обработки.

2.1.63 Физические меры защиты - это разного рода механические, электро- или электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к защищаемой информации и другим ресурсам информационной системы, а также технические средства визуального наблюдения, связи и охранной сигнализации.

2.1.64 Физические способы нарушения безопасности информации - включают:

- уничтожение, хищение и разрушение средств обработки и защиты информации, средств связи, целенаправленное внесение в них неисправностей;
- уничтожение, хищение и разрушение машинных или других оригиналов носителей информации;

- хищение ключей (ключевых документов) средств криптографической защиты информации, программных или аппаратных ключей средств защиты информации от несанкционированного доступа;

- воздействие на обслуживающий персонал и пользователей системы с целью создания благоприятных условий для реализации угроз безопасности информации;

- диверсионные действия по отношению к объектам безопасности информации (взрывы, поджоги, технические аварии и т.д.).

2.1.65 Физический канал утечки информации - неконтролируемый физический путь от источника информации за пределы организации или круга лиц, обладающих охраняемыми сведениями, посредством которого возможно неправомерное (несанкционированное) овладение нарушителем защищаемой информацией.

2.1.66 Целостность информации - свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

2.1.67 Цель защиты информации - предотвращение или минимизация наносимого ущерба (прямого или косвенного, материального, морального или иного) субъектам информационных отношений посредством нежелательного воздействия на компоненты информационной системы, а также разглашения (утечки), искажения (модификации), утраты (снижения степени доступности) или незаконного тиражирования информации.

2.2 Обозначения и сокращения

АО - акционерное общество;

ВТСС – вспомогательные технические средства связи;

ИБ – информационная безопасность;

ПДТК – постоянно действующая техническая комиссия;

ПЭМИН – побочное электромагнитное излучение и наводки электронных средства обработки информации;

РФ – Российская Федерация.

3 Назначение и правовая основа документа

Политика информационной безопасности АО «Гарнизон» (далее - Политика) определяет систему взглядов на проблему обеспечения безопасности информации и представляет собой систематизированное изложение целей и задач защиты, как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми необходимо руководствуется в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации в АО «Гарнизон».

Политика учитывает современное состояние и ближайшие перспективы развития информационных технологий в АО «Гарнизон», цели, задачи и правовые основы их эксплуатации, режимы функционирования, а также

содержит анализ угроз безопасности для объектов и субъектов информационных отношений АО «Гарнизон».

Основные положения и требования данного документа распространяются на все структурные подразделения, включая территориально удаленные. Политика также распространяются на другие организации и учреждения, взаимодействующие с АО «Гарнизон» в качестве потребителей информационных ресурсов в том или ином качестве.

Законодательной основой настоящей Политики являются Конституция Российской Федерации, Гражданский и Уголовный кодексы, законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации, документы по стандартизации, документы Федеральной службы по таможенному и экспортному контролю, Федеральной службы безопасности и Министерства обороны Российской Федерации.

Политика является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности информации в АО «Гарнизон»;
- принятия управленческих решений и разработке практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;
- координации деятельности структурных подразделений АО «Гарнизон» при проведении работ по созданию, развитию и эксплуатации информационных технологий с соблюдением требований по обеспечению безопасности информации;
- разработки предложений по совершенствованию правового, нормативного, технического и организационного обеспечения безопасности информации в АО «Гарнизон».

Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности позволит оптимизировать затраты на ее построение.

При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

Основные положения Политики базируются на качественном осмыслении вопросов безопасности информации и не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защиту информации.

4 Объекты защиты

4.1 Объектами системы информационной безопасности в АО «Гарнизон» являются:

- информационные ресурсы с ограниченным доступом, составляющие служебную, коммерческую тайну, персональные данные работников или иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы;

- процессы обработки информации в информационной системе АО «Гарнизон» регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;

- информационная инфраструктура, включающая системы обработки, хранения и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные элементы информационной среды.

4.2 Структура, состав и размещение основных объектов защиты, информационные связи

Информационная среда является сосредоточенной структурой, которая имеет подключения к телекоммуникационно-информационным сетям международного информационного обмена.

К основным особенностям информационной среды АО «Гарнизон», относятся:

- объединение в единую систему большого количества разнообразных технических средств обработки и передачи информации;

- значительное расширение сферы использования автоматизированных систем обработки информации, широкое многообразие информационно-управляющих систем;

- большое разнообразие решаемых задач и типов обрабатываемых данных, сложные режимы автоматизированной обработки информации;

- значительная важность и ответственность решений, принимаемых на основе автоматизированной обработки данных;

- объединение в единых базах данных информации различного назначения, принадлежности и уровней конфиденциальности;

- высокая значимость информационных потоков;

- разнообразие категорий пользователей и обслуживающего персонала системы.

В этих условиях резко возрастает уязвимость информации и одним из важнейших элементов информационной среды становится корпоративная информационная система, в которой обрабатываются и накапливаются значительные объемы информации, совместно используемой различными категориями пользователей.

4.3 Категории информационных ресурсов, подлежащих защите.

В АО «Гарнизон» циркулирует информация конфиденциального характера, содержащая сведения ограниченного распространения (служебная тайна, коммерческая тайна, персональные данные), и открытые сведения.

Защите подлежит вся конфиденциальная информация и информационные ресурсы, независимо от ее представления и местонахождения в информационной среде АО «Гарнизон»:

- сведения, составляющие коммерческую тайну, доступ к которым ограничен собственником информации в соответствии с Федеральным законом «О коммерческой тайне»;
- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ;
- сведения о частной жизни граждан, позволяющие идентифицировать его личность (персональные данные), доступ к которым ограничен в соответствии с Федеральным законом «О персональных данных»;
- открытая информация, необходимая для обеспечения нормального функционирования АО «Гарнизон».

5 Цели и задачи обеспечения безопасности информации

5.1 Интересы затрагиваемых субъектов информационных отношений

Субъектами информационных отношений при обеспечении информационной безопасности АО «Гарнизон» являются:

- АО «Гарнизон», как собственник информационных ресурсов; подразделения АО «Гарнизон», участвующие в информационном обмене;
- руководство и сотрудники структурных подразделений, в соответствии с возложенными на них функциями;
- юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационной системе;
- другие юридические и физические лица, задействованные в обеспечении выполнения АО «Гарнизон» своих функций (разработчики, обслуживающий персонал, организации, привлекаемые для оказания услуг и пр.).

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- своевременного доступа к необходимой им информации (ее доступности); достоверности (полноты, точности, адекватности, целостности) информации; конфиденциальности (сохранения в тайне) определенной части информации;
- защиты от навязывания им ложной (недостоверной, искаженной) информации; разграничения ответственности за нарушения их прав (интересов) и установленных;
- правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;
- защиты части информации от незаконного тиражирования (защиты авторских прав, прав собственника информации и т.п.).

5.2 Цели защиты

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных

отношений от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а также минимизация рисков.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих основных свойств информации:

- доступности информации для легальных пользователей (устойчивого функционирования информационной системы, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время);
- целостности и аутентичности (подтверждение авторства) информации, хранимой и обрабатываемой в информационной системе и передаваемой по каналам связи;
- конфиденциальности - сохранения в тайне определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи;

Необходимый уровень доступности, целостности и конфиденциальности информации обеспечивается соответствующими множеству значимых угроз методами и средствами.

5.3 Основные задачи обеспечения информационной безопасности

Для достижения основной цели защиты и обеспечения указанных свойств информации система обеспечения информационной безопасности должна обеспечивать эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационной системы;
- создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- защиту от вмешательства в процесс функционирования информационной системы посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;
- обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

- защиту от несанкционированной модификации используемых в корпоративной информационной системе программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;
- защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
- обеспечение живучести криптографических средств защиты информации.

5.4 Основные пути решения задач системы защиты

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

- учетом всех подлежащих защите ресурсов информационной системы (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);
- регистрацией действий персонала, осуществляющего обслуживание и модификацию программных и технических средств корпоративной информационной системы;
- полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности;
- подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению информационной безопасности и процессов ее обработки;
- наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам;
- четким знанием и строгим соблюдением всеми пользователями информационной системы требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности;
- персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам;
- непрерывным поддержанием необходимого уровня защищенности элементов информационной среды;
- применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;
- эффективным контролем за соблюдением пользователями информационных ресурсов, требований по обеспечению информационной безопасности;
- юридической защитой интересов при взаимодействии его подразделений с внешними организациями (связанном с обменом информацией) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

6 Основные угрозы безопасности информации

6.1 Угрозы безопасности информации и их источники

Основными источниками угроз безопасности информации являются:

- непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей информационной системы (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы;

- преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия легально допущенных к информационным ресурсам пользователей (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), которые приводят к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы;

- деятельность преступных групп и формирований, политических и экономических структур, разведок иностранных государств, а также отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности информационной системы в целом и ее отдельных компонентов;

- удаленное несанкционированное вмешательство посторонних лиц из территориально удаленных сегментов корпоративной информационной системы и внешних информационно-телекоммуникационных сетей общего пользования (прежде всего сеть Интернет) через легальные и несанкционированные каналы подключения к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к ресурсам;

- ошибки, допущенные при разработке компонентов информационной системы и их систем защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации и контроля эффективности защиты);

- аварии, стихийные бедствия.

Наиболее значимыми угрозами безопасности информации для АО «Гарнизон» (способами нанесения ущерба субъектам информационных отношений) являются:

- нарушение конфиденциальности (разглашение, утечка) сведений, составляющих служебную или коммерческую тайну, а также персональных данных;

- нарушение функциональности компонентов информационной системы, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;

- нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов, а также фальсификация (подделка) документов.

6.2 Пути реализации непреднамеренных искусственных (субъективных) угроз информационной безопасности.

Работники АО «Гарнизон», зарегистрированные как легальные пользователи информационной системы или обслуживающие ее компоненты, являются внутренними источниками случайных воздействий, т.к. имеют непосредственный доступ к процессам обработки информации и могут совершать непреднамеренные ошибки и нарушения действующих правил, инструкций и регламентов.

Основные пути реализации непреднамеренных искусственных (субъективных) угроз безопасности информации (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

- неумышленные действия, приводящие к частичному или полному нарушению функциональности компонентов информационной системы или разрушению информационных или программно-технических ресурсов;

- неосторожные действия, приводящие к разглашению информации ограниченного распространения или делающие ее общедоступной;

- разглашение, передача или утрата атрибутов разграничения доступа (пропусков, идентификационных карточек, ключей, паролей, ключей шифрования и т. п.);

- игнорирование организационных ограничений (установленных правил) при работе с информационными ресурсами;

- пересылка данных и документов по ошибочному адресу (устройства); ввод ошибочных данных;

- неумышленная порча носителей информации; неумышленное повреждение линий связи;

- неправомерное отключение оборудования или изменение режимов работы устройств или программ;

- заражение компьютеров вирусами;

- несанкционированный запуск технологических программ, способных вызвать потерю работоспособности компонентов информационной системы или осуществляющих необратимые в них изменения (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

- некомпетентное использование, настройка или неправомерное отключение средств защиты.

6.3 Пути реализации преднамеренных искусственных (субъективных) угроз информационной безопасности

Основные возможные пути умышленной дезорганизации работы, вывода компонентов информационной системы АО «Гарнизон», из строя, проникновения в систему и несанкционированного доступа к информации (с корыстными целями, по принуждению, из желания отомстить и т.п.):

- умышленные действия, приводящие к частичному или полному нарушению функциональности компонентов информационной системы или разрушению информационных или программно-технических ресурсов;
- действия по дезорганизации функционирования информационной системы; хищение документов и носителей информации;
- несанкционированное копирование документов и носителей информации; умышленное искажение информации, ввод неверных данных;
- отключение или вывод из строя подсистем обеспечения функционирования информационных систем (электропитания, охлаждения и вентиляции, линий и аппаратуры связи и т.п.);
- перехват данных, передаваемых по каналам связи и их анализ;
- хищение производственных отходов (распечаток документов, записей, носителей информации и т.п.);
- незаконное получение атрибутов разграничения доступа (агентурным путем, используя халатность пользователей, путем подделки, подбора и т.п.);
- несанкционированный доступ к ресурсам информационной системы с рабочих станций легальных пользователей;
- хищение или вскрытие шифров криптозащиты информации;
- внедрение аппаратных и программных закладок с целью скрытно осуществлять доступ к информационным ресурсам или дезорганизации функционирования компонентов корпоративной информационной системы;
- незаконное использование оборудования, программных средств или информационных ресурсов, нарушающее права третьих лиц;
- применение технических средств для несанкционированного съема информации.

6.4 Пути реализации основных естественных угроз информационной безопасности:

- выход из строя оборудования информационных систем и оборудования обеспечения его функционирования;
- выход из строя или невозможность использования линий связи; пожары, наводнения и другие стихийные бедствия.

6.5 Неформальная модель возможных нарушителей

Нарушитель - это лицо, которое предприняло попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Злоумышленник - нарушитель, действующий намеренно из корыстных, идейных или иных побуждений.

Система обеспечения информационной безопасности АО «Гарнизон» должна строиться исходя из предположений о следующих возможных типах нарушителей в системе (с учетом категории лиц, мотивации, квалификации, наличия специальных средств и др.):

- некомпетентный (невнимательный) пользователь - сотрудник АО «Гарнизон» (или подразделения другой организации, являющийся легальным пользователем информационной системы), который может предпринимать попытки выполнения запрещенных действий, доступа к защищаемым ресурсам информационной системы с превышением своих полномочий, ввода некорректных данных, нарушения правил и регламентов работы с информацией и т.п., действуя по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (предоставленные) средства;

Любитель - сотрудник АО «Гарнизон» (или подразделения другой организации, являющийся зарегистрированным пользователем информационной системы), пытающийся нарушить систему защиты без корыстных целей или злого умысла или для самоутверждения. Для преодоления системы защиты и совершения запрещенных действий он может использовать различные методы получения дополнительных полномочий доступа к ресурсам, недостатки в построении системы защиты и доступные ему штатные средства (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств). Помимо этого он может пытаться использовать дополнительно нештатные инструментальные и технологические программные средства, самостоятельно разработанные программы или стандартные дополнительные технические средства;

Внутренний злоумышленник - сотрудник АО «Гарнизон» (или подразделения другого ведомства, зарегистрированный как пользователь системы), действующий целенаправленно из корыстных интересов или мести за нанесенную обиду, возможно в сговоре с лицами, не являющимися сотрудниками. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне;

Внешний злоумышленник - постороннее лицо, действующее целенаправленно из корыстных интересов, мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование

специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне АО «Гарнизон».

Внутренним нарушителем может быть лицо из следующих категорий сотрудников:

- зарегистрированные пользователи информационной системы;
- сотрудники АО «Гарнизон», не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационной системы, но имеющие доступ в здания и помещения;
- персонал, обслуживающий технические средства корпоративной информационной системы АО «Гарнизон»;
- сотрудники подразделений АО «Гарнизон», задействованные в разработке и сопровождении программного обеспечения;
- сотрудники подразделений обеспечения безопасности АО «Гарнизон»;
- руководители различных уровней.

Категории лиц, которые могут быть внешними нарушителями:

- уволенные сотрудники АО «Гарнизон»;
- представители организаций, взаимодействующих по вопросам технического обеспечения;
- посетители (представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.);
- члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;
- представители конкурирующих организаций;
- лица, случайно или умышленно проникшие в корпоративную информационную систему из внешних телекоммуникационных сетей (хакеры).

Пользователи и обслуживающий персонал из числа сотрудников АО «Гарнизон» имеют наиболее широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определенных полномочий по доступу к информационным ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связано с нарушением действующих правил и инструкций.

Особую категорию составляют администраторы автоматизированных систем, имеющих практически неограниченный доступ к информационным ресурсам компонентов корпоративной информационной системы. Численность данной категории пользователей должна быть минимальной, а их действия должны находиться под обязательным контролем со стороны подразделений обеспечения информационной безопасности.

Уволенные сотрудники могут использовать для достижения целей свои знания о технологии работы, защитных мерах и правах доступа. Полученные во время работы в АО «Гарнизон» знания и опыт выделяют их среди других источников внешних угроз.

Представители иностранных разведок являются наиболее агрессивным источником внешних угроз. Для осуществления своих замыслов эти структуры могут идти на открытое нарушение закона и вовлекать в свою деятельность сотрудников АО «Гарнизон» всеми доступными им силами и средствами.

Профессиональные хакеры имеют наиболее высокую техническую квалификацию и знания о слабостях программных средств, используемых в автоматизированных системах обработки информации. Они представляют наибольшую угрозу при взаимодействии с работающими или уволенными сотрудниками и представителями иностранных разведок.

Организации, занимающиеся разработкой, поставкой, ремонтом и обслуживанием оборудования или информационных систем, представляют внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к информационным ресурсам.

Принимаются следующие ограничения и предположения о характере действий возможных нарушителей:

- нарушитель скрывает свои несанкционированные действия от других сотрудников АО «Гарнизон»;

- несанкционированные действия могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;

- в своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж и другие средства и методы для достижения стоящих перед ним целей.

6.6 Утечка информации по техническим каналам

Наибольшую опасность для объектов АО «Гарнизон» представляют средства наземной разведки, которые по физическим принципам построения аппаратуры и своему функциональному предназначению можно классифицировать на следующие виды:

- радиоразведку, обеспечивающую добывание информации, содержащейся непосредственно в перехватываемых сообщениях, передаваемых по каналам радиосвязи различного типа и назначения (в том числе, по каналам радиотелефонной и сотовой систем связи);

- разведку побочных электромагнитных излучений и наводок электронных средств обработки информации (далее - разведку ПЭМИН), обеспечивающую добывание информации, содержащейся непосредственно в формируемых передаваемых или отображаемых (телефонных, телеграфных и т.п.) сообщениях и документах (текстах, таблицах, рисунках, картах, снимках, схемах, телевизионных изображениях и т.п.), с использованием радиоэлектронной аппаратуры, регистрирующей непреднамеренные прямые электромагнитные излучения и электрические сигналы средств обработки информации, а также вторичные электромагнитные излучения и электрические сигналы, наводимые прямым электромагнитными излучениями в токопроводящих цепях различных технических устройств и токопроводящих элементах конструкции зданий и сооружений;

- телевизионную разведку, обеспечивающую добывание информации, содержащейся в изображениях объектов, получаемых в видимом диапазоне электромагнитных волн с использованием телевизионной аппаратуры;

- визуальную оптико-электронную разведку, обеспечивающую добывание информации, содержащейся в изображениях объектов, получаемых с использованием приборов ночного видения в оптическом диапазоне электромагнитных волн;

- фотографическую разведку, обеспечивающую добывание информации, содержащейся в изображениях объектов, получаемых в оптическом диапазоне электромагнитных волн с использованием различных типов фотоаппаратуры;

- визуальную оптическую разведку, обеспечивающую добывание информации, содержащейся в видовых признаках наблюдаемых объектов с использованием различных типов оптических приборов (биноклей, стереотруб, визиров, перископов, эндоскопов и т.д.).

- акустическую разведку, обеспечивающую добывание информации, содержащейся непосредственно в произносимой либо воспроизводимой речи (акустическая, речевая, разведка), а также в параметрах акустических сигналов, сопутствующих работе механических устройств оргтехники и других технических систем (акустическая сигнальная разведка), с использованием аппаратуры, регенерирующей акустические (в воздухе) и виброакустические (в упругих средах) волны, а электромагнитные излучения и электрические сигналы, возникающие за счет акустических преобразований в различных технических средствах;

Наиболее вероятными носителями аппаратуры разведки могут быть:

- посты разведки в иностранных представительствах и местах проживания иностранных граждан, из которых может вестись разведка с использованием портативной разведывательной аппаратуры возимого и носимого типа;

- отдельные физические лица, использующие портативную разведывательную аппаратуру возимого и носимого типа;

- различные виды импортного оборудования, которые могут быть использованы для ведения технической разведки (аппаратура двойного назначения).

В зависимости от условий технической разведки (условий применения технических средств) разновидностей объектов разведки, возможностей скрытого применения технических средств могут использоваться следующие виды аппаратуры разведки:

- стационарная;
- портативная возимая;
- портативная носимая;
- автономная автоматическая.

Кроме того, для осуществления технической разведки с помощью портативной аппаратуры могут использоваться:

- помещения фирм, расположенных в квартирах, гостиницах и другие места проживания, местах нахождения иностранных представительств на постоянной и временной основе и т.п.;

- здания и помещения совместных предприятий, организаций;
- транспортные средства.

Автономная автоматическая аппаратура разведки может использоваться, вблизи объектов АО «Гарнизон», при этом нельзя исключать ее непосредственное использование, путем скрытного установления при посещении (проведении работ) на объектах.

Портативная возимая аппаратура используется преимущественно для ведения:

- радиоразведки (например, для перехвата переговоров по радиотелефонам и телефонам сотовой связи);
- разведки ПЭМИН;
- оптико-электронной (с использованием видео- и телекамер видимого диапазона); фотографической (с использованием длиннофокусной аппаратуры);
- визуально-оптической (с использованием биноклей, приборов ночного видения и подобных устройств);
- акустической (например, для снятия информации с окон помещений с помощью направленных микрофонов различного типа) или лазерной аппаратуры дистанционного прослушивания речи. Разведывательная аппаратура устанавливается на транспортных средствах, а добывание разведданных происходит в движении транспортного средства вблизи объектов (при передвижении по прилагающим к объектам улицам (трассам)). В состав портативной возимой аппаратуры разведки может входить аппаратура сбора информации с автономных автоматических устройств разведки.

7 Основные принципы построения системы информационной безопасности

Построение системы обеспечения информационной безопасности, и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- разумная достаточность (экономическая целесообразность);
- персональная ответственность;
- минимизация полномочий;
- исключение конфликта интересов;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

7.1 Законность

Предполагает осуществление защитных мероприятий и разработку системы информационной безопасности АО «Гарнизон» в соответствии с действующим законодательством в области информации, информатизации и защиты информации, а также других нормативных актов по информационной безопасности, утвержденных органами государственной власти и управления в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией. Принятые меры информационной безопасности не должны препятствовать доступу контролирующих органов в предусмотренных законодательством случаях к информации конкретных подсистем.

Все пользователи информационной системы АО «Гарнизон» должны иметь представление об ответственности за правонарушения в области информации.

Реализация данного принципа необходима для защиты имени и репутации АО «Гарнизон».

7.2 Системность

Системный подход к построению системы защиты информации предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности информации.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационной системы АО «Гарнизон», а также характер, возможные объекты и направления атак на нее со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и несанкционированного доступа к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

7.3 Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

7.4 Непрерывность защиты

Обеспечение информационной безопасности - процесс, осуществляемый руководством АО «Гарнизон» и сотрудниками всех уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность средств защиты, сколько процесс, который должен постоянно идти на всех уровнях внутри АО «Гарнизон» и каждый

сотрудник должен принимать участие в этом процессе. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности АО «Гарнизон», ее эффективность зависит от участия руководства в обеспечении информационной безопасности.

Кроме того, большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления защиты.

7.5 Своевременность

Предполагает упреждающий характер мер обеспечения информационной безопасности, то есть постановку задач по комплексной защите информации и реализацию мер обеспечения информационной безопасности на ранних стадиях разработки информационных систем в целом и их систем защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой информационной системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) системы, обладающие достаточным уровнем защищенности.

7.6 Преемственность и совершенствование

Предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационной системы АО «Гарнизон» и системы ее защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

7.7 Разумная достаточность (экономическая целесообразность)

Предполагает соответствие уровня затрат на обеспечение информационной безопасности ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы компонентов информационной системы. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока информация находится в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать

некоторый приемлемый уровень обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

7.8 Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

7.9 Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

7.10 Исключение конфликта интересов (разделение функций)

Эффективная система обеспечения информационной безопасности предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться, и находится под строгим независимым контролем. Реализация данного принципа предполагает, что не один сотрудник не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Наделение сотрудников полномочиями, порождающими конфликт интересов, дает ему возможность подтасовывать информацию в корыстных целях или с тем, чтобы скрыть проблемы или понесенные убытки. Для снижения риска манипулирования информацией и риска хищения, такие полномочия должны в максимально возможной степени быть разделены между различными сотрудниками или подразделениями. Необходимо проводить периодические проверки обязанностей, функций и деятельности сотрудников, выполняющих ключевые функции, с тем, чтобы они не имели возможности скрывать совершение неправомерных действий. Кроме того, необходимо принимать специальные меры по недопущению сговора между сотрудниками.

7.11 Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективах структурных подразделений. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности подразделений защиты информации.

Важным элементом эффективной системы обеспечения безопасности информации является высокая культура работы с информацией, соблюдение этических норм и стандартов профессиональной деятельности, создание корпоративной культуры, подчеркивающей и демонстрирующей персоналу на

всех уровнях важность обеспечения информационной безопасности. Все сотрудники должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе. Несмотря на то, что высокая культура обеспечения информационной безопасности не гарантирует автоматического достижения целей, ее отсутствие создает больше возможностей для нарушения безопасности или не обнаружения фактов ее нарушения.

7.12 Гибкость системы защиты

Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления АО «Гарнизон» своей деятельности. В число таких изменений входят:

- изменения организационной и штатной структуры;
- корпоративная реструктуризация, слияния и поглощения;
- изменение существующих или внедрение принципиально новых информационных систем;
- новые технические средства;
- новые виды деятельности;
- новые услуги, продукты.

Свойство гибкости системы обеспечения информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

7.13 Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

7.14 Простота применения средств защиты

Механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

7.15 Обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня информационной безопасности и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по информационной безопасности.

7.16 Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами АО «Гарнизон» (специалистами по ИБ).

7.17 Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности информации, на основе используемых систем и средств защиты информации, при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

Кроме того, эффективная система обеспечения информационной безопасности требует наличия адекватной и всеобъемлющей информации о текущем состоянии процессов, связанных с движением информации и сведений о соблюдении установленных нормативных требований, а также дополнительной информации, имеющей отношение к принятию решений. Информация должна быть надежной, своевременной, доступной и правильно оформленной.

Недостатки системы обеспечения информационной безопасности, выявленные сотрудниками АО «Гарнизон» или подразделениями обеспечения безопасности должны немедленно доводиться до сведения руководителей соответствующего уровня лично и оперативно устраняться. О существенных недостатках необходимо сообщать руководству. Важно, чтобы после получения информации соответствующие руководители обеспечивали своевременное исправление недостатков. Руководство должно периодически получать отчеты, суммирующие все проблемы, выявленные системой обеспечения информационной безопасности. Вопросы, которые кажутся незначительными, когда отдельные процессы рассматриваются изолированно, при рассмотрении их наряду с другими аспектами могут указать на отрицательные тенденции, грозящие перерасти в крупные недостатки, если они не будут своевременно устранены.

8 Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов

8.1 Меры обеспечения информационной безопасности

Все меры обеспечения безопасности информационной системы подразделяются на:

- правовые (законодательные);
- морально-этические;
- технологические;
- организационные (административные);
- физические;
- технические (аппаратные и программные).

8.1.1 Правовые (законодательные) меры защиты

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационной системы.

8.1.2 Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или в целом. Морально-этические нормы бывают как неписаные, так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений.

8.1.3 Технологические меры защиты

К данному виду мер защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий. Примером таких мер является использование процедур двойного ввода ответственной информации, инициализации ответственных операций только при наличии согласования нескольких лиц, процедур проверки реквизитов исходящих и входящих сообщений и т.п.

8.1.4 Организационные (административные) меры защиты

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования

системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

8.2 Формирование политики безопасности

Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать политику в области обеспечения безопасности информации (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

С практической точки зрения политику в области обеспечения безопасности информации в АО «Гарнизон» целесообразно разбить на два уровня. К верхнему уровню относятся решения руководства, затрагивающие деятельность АО «Гарнизон» в целом. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности информации, определить какими ресурсами (материальные, структурные, организационные) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью.

Политика нижнего уровня, определяет процедуры, и правила достижения целей и решения задач безопасности информации и детализирует (регламентирует) эти правила:

- каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности информации;
- кто имеет права доступа к информации ограниченного распространения, кто и при каких условиях может читать и модифицировать информацию и т.д.

Политика нижнего уровня должна:

- предусматривать регламент информационных отношений, исключающих возможность произвольных, монопольных или несанкционированных действий в отношении информационных ресурсов;
- определять коалиционные и иерархические принципы и методы разделения конфиденциальной информации и разграничения доступа к информации ограниченного распространения;
- выбирать программно-технические (аппаратные) средства криптозащиты, противодействия несанкционированному доступу, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

8.3 Регламентация доступа в помещения

Чувствительные к воздействиям компоненты информационной системы должны размещаться в помещениях, оборудованных надежными замками, средствами сигнализации и находящимися под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, серверов, реквизитов доступа и

т.п.). Уборка таких помещений должна производиться в присутствии ответственного сотрудника, за которым закреплены данные компоненты, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым информационным ресурсам.

Во время обработки информации ограниченного распространения в таких помещениях должен присутствовать только персонал, допущенный к работе с данной информацией. Запрещается прием посетителей в помещениях, когда осуществляется обработка информации ограниченного распространения.

По окончании рабочего дня, помещения, в которых размещаются чувствительные компоненты информационной системы, должны, опечатываться сдаваться под охрану с включением сигнализации и с отметкой в книге приема и сдачи помещений.

Для хранения служебных документов и машинных носителей с защищаемой информацией помещения снабжаются сейфами, металлическими шкафами или шкафами оборудованные замком.

В случае оснащения помещений средствами охранной сигнализации, прием-сдача таких помещений под охрану осуществляется на основании специально разрабатываемой инструкции.

Помещения должны быть обеспечены средствами уничтожения документов.

8.4 Регламентация допуска сотрудников к использованию информационных ресурсов

В рамках разрешительной системы допуска устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.

Допуск пользователей к работе с информационной системой и доступ к ее ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком, согласно регламента предоставления доступа пользователей.

Основными пользователями информации в корпоративной информационной системе являются сотрудники структурных подразделений. Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

- каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, должно согласовываться с подразделением, ответственным за информационное сопровождение данного ресурса.

Все сотрудники АО «Гарнизон» или других организаций, зарегистрированные как легальные пользователи информационной системы и обслуживающий персонал, должны нести персональную ответственность за нарушения установленного порядка обработки информации, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы. Каждый сотрудник (при приеме на работу) должен

подписывать обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению служебной и коммерческой тайны, а также правил работы с информацией.

Обработка информации в компонентах информационной системы должна производиться в соответствии с утвержденными технологическими инструкциями.

8.5 Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов

Подлежащие защите ресурсы системы (документы, задачи, сервера, программы) подлежат учету (на основе использования соответствующих формуляров или специализированных баз данных).

В целях поддержания режима информационной безопасности аппаратно-программная конфигурация автоматизированных рабочих мест сотрудников, с которых возможен доступ к ресурсам корпоративной информационной системы, должна соответствовать кругу возложенных на данных пользователей функциональных обязанностей.

Все неиспользуемые в работе устройства ввода-вывода информации (Wi-Fi, COM, LPT, USB, IR порты, CD, DVD и т.п.) на рабочих местах сотрудников, работающих с конфиденциальной информацией, должны быть по возможности отключены, не нужные для работы программные средства и данные с дисков также должны быть удалены. Дополнительные устройства обмена информацией могут использоваться только в исключительных случаях и только в качестве временного средства. Установка подобных устройств должна согласовываться со специалистом по ИБ. Порядок их использования определяется отдельным документом.

В компонентах корпоративной информационной системы и на рабочих местах пользователей должны устанавливаться и использоваться программные средства, только полученные от отдела системного администрирования. Порядок использования программного обеспечения, в АО «Гарнизон» определяется отдельным документом.

Для решения специальных задач по оценке защищенности информационной сети и построении системы защиты информации в сети АО «Гарнизон» может применяться специальное программное обеспечение.

8.6 Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов

Оборудование корпоративной информационной системы, используемое для доступа к конфиденциальной информации, к которому доступ обслуживающего персонала в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к его компонентам должно закрываться и опечатываться (пломбироваться).

Повседневный контроль за целостностью и соответствием печатей (пломб) должен осуществляться пользователями оборудования. Периодический контроль – специалистом по ИБ.

8.7 Обучение сотрудников и повышение осведомленности в вопросах информационной безопасности.

Все пользователи информационной системы должны быть ознакомлены с организационно - распорядительными документами по обеспечению информационной безопасности, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности информации. Доведение требований указанных документов до лиц, допущенных к обработке защищаемой информации, должно осуществляться под роспись.

Пользователи информационной системы, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации в АО «Гарнизон».

Целью обучения сотрудников является, снижение потерь (материальных, финансовых, ущерб репутации и т.д.) от угроз, связанных с незнанием или непониманием основных положений нормативно-распорядительных документов в области ИБ и правил по защите информации.

Задачи обучения повышения осведомленности в вопросах ИБ:

- информирование сотрудников о существующих угрозах (опасностях) и проблемах ИБ, которые могут возникнуть при автоматизированной обработке информации, обновление (расширение) их теоретических и практических знаний в области ИБ;
- доведение до сотрудников основных положений, ограничений и требований существующих нормативно-распорядительных документов принятых в АО «Гарнизон»;
- мобилизация и мотивация конечных пользователей информационной системы на сознательное выполнение ими требований, ограничений и правил обеспечения ИБ;
- выработка у сотрудников умения здраво оценивать возможные последствия своих действий (адекватно оценивать связанные с ними риски ИБ);
- выработка у сотрудников привычек, способствующих поддержанию высокого уровня ИБ;
- выработка у сотрудников АО «Гарнизон» умений (навыков) правильно и оперативно действовать при возникновении инцидентов ИБ;
- доведение до сотрудников координат лиц, ответственных за обеспечение ИБ в АО «Гарнизон»;
- доведение до сотрудников их обязанностей в области обеспечения ИБ и степени их ответственности в случае утечки конфиденциальной информации;
- оценка эффективности, развитие и совершенствование проводимых мероприятий по ИБ в целом.

Формы и методы повышения осведомленности сотрудников в области информационной безопасности:

- инструктаж при приеме на работу; обучение (курсы, семинары, тренинги);
- дистанционное обучение;

- инструктажи и зачеты по положениям Политики безопасности;
- рассылки на электронную почту, разделы на внутреннем сайте АО «Гарнизон» (с примерами конкретных нарушений, статистикой, результатами контроля);
- распространение кратких памяток;
- средства наглядной агитации, экранные заставки с правилами ИБ.

8.8 Подразделение обеспечения информационной безопасности

Для непосредственной организации и эффективного функционирования системы обеспечения информационной безопасности, исключающей возможные конфликты интересов, в АО «Гарнизон» целесообразно создать единое подразделение обеспечения информационной безопасности. На это подразделение возложить решение следующих основных задач:

- проведение в жизнь политики обеспечения информационной безопасности, определение требований к системе защиты информации;
- анализ текущего состояния обеспечения информационной безопасности;
- организация мероприятий и координация работ всех подразделений по комплексной защите информации;
- контроль и оценка эффективности принятых мер и применяемых средств защиты информации.

Основные функции подразделения обеспечения информационной безопасности должны заключаться в следующем:

- формирование требований к системам защиты в процессе создания и дальнейшего развития существующих компонентов информационной системы;
- подготовка решений по обеспечению конфиденциальности, доступности, целостности данных;
- участие в проектировании систем защиты, их испытаниях и приемке в эксплуатацию;
- обеспечение функционирования установленных систем защиты информации, включая управление криптографическими системами;
- генерация и распределение между пользователями необходимых атрибутов доступа к ресурсам информационной системы;
- наблюдение за функционированием системы защиты и ее элементов; проверка надежности функционирования системы защиты; разработка мер нейтрализации моделей возможных атак;
- обучение пользователей и обслуживающего персонала правилам безопасной обработки информации;
- оказание методической помощи сотрудникам в вопросах обеспечения информационной безопасности;
- контроль за действиями администраторов баз данных, серверов и сетевых устройств;
- контроль за соблюдением пользователями и обслуживающим персоналом установленных правил обращения с информацией;
- организация по указанию руководства служебного расследования по фактам нарушения правил обращения с информацией и оборудованием;

- принятие мер при попытках несанкционированного доступа к информационным ресурсам и компонентам системы или при нарушениях правил функционирования системы защиты;

- сбор, накопление, систематизация и обработка информации по вопросам информационной безопасности.

Организационно - правовой статус подразделения обеспечения информационной безопасности должен определяться следующим образом:

- численность подразделения должна быть достаточной для выполнения всех перечисленных выше функций;

- сотрудники, занимающиеся обеспечением информационной безопасности не должны иметь других обязанностей, связанных с обеспечением функционирования технических компонентов информационной системы;

- сотрудники подразделения обеспечения информационной безопасности должны иметь право доступа во все помещения, где, установлены технические средства информационной системы, право прекращать обработку информации при наличии непосредственной угрозы ее утечки и осуществлять контроль защищаемых помещений;

- руководителю подразделения должно быть предоставлено право запрещать включение новых компонентов информационной системы в число действующих, если они не отвечают требованиям защиты информации и это может привести к серьезным последствиям в случае реализации значимых угроз безопасности информации;

- подразделению обеспечения информационной безопасности должны обеспечиваться все условия, необходимые для выполнения своих функций.

Для решения задач, возложенных на подразделение обеспечения информационной безопасности, его сотрудники должны иметь следующие права:

- определять необходимость и разрабатывать нормативные документы, касающиеся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность пользователей информационной системы в указанной области;

- получать информацию от пользователей информационной системы АО «Гарнизон» по любым аспектам применения информационных технологий в АО «Гарнизон»;

- участвовать в проработке технических решений по вопросам обеспечения безопасности информации при проектировании и разработке новых информационных технологий;

- участвовать в испытаниях разработанных информационных технологий по вопросам оценки качества реализации требований по обеспечению безопасности информации;

- контролировать деятельность пользователей информационной системы АО «Гарнизон» по вопросам обеспечения информационной безопасности;

- требовать письменных объяснений у лиц по фактам нарушений требований информационной безопасности;

- готовить предложения Руководству по обеспечению требований информационной безопасности.

В состав подразделения обеспечения информационной безопасности должны входить следующие специалисты:

- ответственные за управление средствами защиты информации (выбор, установка, настройка, снятие средств защиты, просмотр журналов регистрации событий, оперативный контроль, за работой пользователей, и реагирование на события защиты и т.п.);

- ответственные за управление криптографическими средствами защиты (установка, настройка, снятие СКЗИ, генерация и распределение ключей и т.д.);

- ответственные за решение вопросов защиты информации в разрабатываемых и внедряемых в АО «Гарнизон» информационных технологиях (участие в разработке технических заданий по вопросам защиты информации, выбор средств и методов защиты, участие в испытаниях новых технологий и программ с целью проверки выполнения требований по защите информации и т.д.);

- специалисты по защите от утечки информации по техническим каналам.

8.9 Ответственность за нарушения установленного порядка пользования ресурсами информационной системы. Расследование нарушений

Любое грубое нарушение порядка и правил пользования информационными ресурсами должно расследоваться. К виновным должны применяться адекватные меры воздействия. Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной работы с информацией, должна определяться нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению руководства.

Для создания необходимой юридической основы процедур привлечения сотрудников к ответственности за нарушения в области информационной безопасности необходимо, чтобы:

- во всех положениях о структурных подразделениях и в функциональных (технологических) обязанностях всех сотрудников, участвующих в процессах автоматизированной обработки информации, были отражены требования по обеспечению информационной безопасности;

- каждый сотрудник (при приеме на работу) подписывал обязательство о соблюдении установленных требований по сохранению государственной (при необходимости), служебной и коммерческой тайны, а также об ответственности за нарушение правил работы с защищаемой информацией;

- все пользователи были ознакомлены с перечнем сведений, подлежащих защите, в части их касающейся (в соответствии со своим уровнем полномочий);

- доведение требований, организационно-распорядительных документов по вопросам информационной безопасности до лиц, допущенных к обработке защищаемой информации, осуществлялось руководителями подразделений под подпись.

Работники АО «Гарнизон» несут ответственность по действующему законодательству за разглашение сведений, составляющих (государственную,

служебную, коммерческую) тайну, и сведений ограниченного распространения, ставших им известными по роду работы.

Любое грубое нарушение порядка и правил работы сотрудниками структурных подразделений должно расследоваться. К виновным должны применяться адекватные меры воздействия.

Нарушения установленных правил и требований по ИБ являются основанием для применения к сотруднику (исполнителю) административных мер наказания, вплоть до увольнения и привлечения к уголовной или дисциплинарной ответственности.

Мера ответственности сотрудников за действия, совершенные в нарушение установленных правил обеспечения безопасности информации, должна определяться с учетом нанесенного ущерба, наличия злого умысла и других факторов по усмотрению руководства.

Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

- индивидуальная идентификация пользователей и инициированных ими процессов, т.е. установление за ними идентификатора (login, Use name), на базе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности доступа;
- проверка подлинности пользователей (аутентификация) на основе паролей, ключей на различной физической основе, биометрических характеристик личности и т.п.;
- реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).

8.10 Средства обеспечения информационной безопасности

Для обеспечения информационной безопасности используются следующие средства защиты:

- физические средства;
- технические средства;
- средства идентификации и аутентификации пользователей;
- средства разграничения доступа;
- средства обеспечения и контроля целостности;
- средства оперативного контроля и регистрации событий безопасности;
- антивирусная защита;
- криптографические средства.

Средства защиты должны применяться ко всем чувствительным ресурсам информационной системы, независимо от их вида и формы представления информации в них.

8.10.1 Физические средства защиты

Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться охраной путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в них посторонних лиц, хищение документов и носителей информации, самих средств информатизации, а также исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств съема информации.

Для обеспечения физической безопасности компонентов информационной системы необходимо осуществлять ряд организационных и технических мероприятий, включающих: проверку оборудования, предназначенного для обработки закрытой (конфиденциальной) информации, на:

- наличие специально внедренных закладных устройств;
- введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки закрытой информации;
- оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи.

8.10.2 Технические средства защиты

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности информации по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

- средства разграничения доступа к данным; средства криптографической защиты информации;
- средства регистрации доступа к компонентам информационной системы и контроля за использованием информации;
- средства реагирования на нарушения режима информационной безопасности; средства противодействия техническим средствам разведки.

На технические средства защиты возлагается решение следующих основных задач:

- идентификация и аутентификация пользователей при помощи имен или специальных аппаратных средств (Advanto, Touch Memory и т.п.);
- регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам;
- защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;
- регистрация действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;

- защита корпоративной информационной системы от несанкционированных воздействий со стороны информационно-телекоммуникационных сетей общего пользования;

- защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информации, находящейся на нем.

8.10.3 Средства идентификации и аутентификации пользователей

В целях предотвращения работы с ресурсами информационной системы посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей). Для идентификации могут применяться различного рода устройства: магнитные карточки, ключи, ключевые вставки, флеш-карты и т.п.

Аутентификация (подтверждение подлинности) пользователей также может осуществляться:

- путем проверки наличия у пользователей каких-либо специальных устройств (магнитных карточек, ключей, ключевых вставок и т.д.);

- путем проверки знания ими паролей;

- путем проверки уникальных физических характеристик и параметров самих пользователей при помощи специальных биометрических устройств.

8.10.4 Средства разграничения доступа

Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

Технические средства разграничения доступа должны по возможности быть составной частью единой системы контроля доступа:

- на контролируемую территорию; в отдельные помещения;

- к компонентам информационной среды и элементам системы защиты информации (физический доступ);

- к информационным ресурсам (документам, носителям информации, файлам, наборам данных, архивам, справкам и т.д.);

- к активным ресурсам (прикладным программам, задачам и т.п.);

- к операционной системе, системным программам и программам защиты.

8.10.5 Средства обеспечения и контроля целостности

Средства обеспечения целостности включают в свой состав средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

Средства контроля целостности информационных ресурсов системы предназначены для своевременного обнаружения модификации или искажения ресурсов системы. Они позволяют обеспечить правильность функционирования системы защиты и целостность хранимой и обрабатываемой информации.

Контроль целостности информации и средств защиты, с целью обеспечения неизменности информационной среды, определяемой

предусмотренной технологией обработки, и защиты от несанкционированной модификации информации должен обеспечиваться:

- средствами разграничения доступа (в помещения, к документам, к носителям информации, к серверам, логическим устройствам и т.п.);
- средствами электронно-цифровой подписи; средствами учета;
- средствами подсчета контрольных сумм (для используемого программного обеспечения).

8.10.6 Средства оперативного контроля и регистрации событий безопасности

Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток несанкционированного доступа и т.п.), которые могут привести к возникновению кризисных ситуаций. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, их характер, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации. Средства контроля и регистрации должны предоставлять возможности:

- ведения и анализа журналов регистрации событий безопасности (системных журналов);
- получения твердой копии (печати) журнала регистрации событий безопасности; упорядочения журналов, а также установления ограничений на срок их хранения; оперативного оповещения специалиста по ИБ о нарушениях.

При регистрации событий безопасности в журнале должна фиксироваться следующая информация:

- дата и время события;
- идентификатор субъекта, осуществляющего регистрируемое действие;
- действие (тип доступа).

8.10.7 Средства антивирусной защита

Средства антивирусной защиты должны обеспечивать обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Реализация антивирусной защиты должна предусматривать:

- применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), мобильных технических средствах и иных точках доступа в информационную систему, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы);

- установку, конфигурирование и управление средствами антивирусной защиты;

- предоставление доступа средствам антивирусной защиты к объектам информационной системы, которые должны быть подвергнуты проверке средством антивирусной защиты;

- проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов);

- проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов;

- оповещение администраторов безопасности в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов);

- определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами).

Правила и процедуры антивирусной защиты информационной системы регламентируются в организационно-распорядительных документах АО «Гарнизон».

Требования к усилению:

1) в информационной системе должно обеспечиваться предоставление прав по управлению (администрированию) средствами антивирусной защиты администратору безопасности;

2) в информационной системе должно обеспечиваться централизованное управление (установка, удаление, обновление, конфигурирование и контроль актуальности версий программного обеспечения средств антивирусной защиты) средствами антивирусной защиты, установленными на компонентах информационной системы (серверах, автоматизированных рабочих местах);

3) оператором должен обеспечиваться запрет использования съемных машинных носителей информации, которые могут являться источниками вредоносных компьютерных программ (вирусов);

5) в информационной системе должны обеспечиваться проверка работоспособности, актуальность базы данных признаков компьютерных вирусов и версии программного обеспечения средств антивирусной защиты;

6) в информационной системе должна обеспечиваться проверка объектов файловой системы средством антивирусной защиты до загрузки операционной системы;

7) в информационной системе должна обеспечиваться регистрация событий о неуспешном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);

8) оператором должна обеспечиваться антивирусная защита на этапе инициализации микропрограммного обеспечения средства вычислительной техники.

Должно быть обеспечено обновление базы данных признаков вредоносных компьютерных программ (вирусов).

Обновление базы данных признаков вредоносных компьютерных программ (вирусов) должно предусматривать:

- получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);
- получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов);
- контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

Правила и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов) регламентируются в организационно-распорядительных документах АО «Гарнизон».

Требования к усилению:

1) в информационной системе должно обеспечиваться централизованное управление обновлением базы данных признаков вредоносных компьютерных программ (вирусов);

2) в информационной системе должно обеспечиваться автоматическое обновление базы данных признаков вредоносных компьютерных программ (вирусов) на всех компонентах информационной системы;

3) в информационной системе должен обеспечиваться запрет изменений настроек системы обновления базы данных признаков вредоносных компьютерных программ (вирусов) на автоматизированных рабочих местах и серверах;

4) в информационной системе должна обеспечиваться возможность возврата (отката) к предыдущим обновлениям базы данных признаков вредоносных компьютерных программ (вирусов).

8.10.8 Криптографические средства защиты информации

Основными элементами системы, обеспечения безопасности информации являются криптографические методы и средства защиты. Перспективным направлением, использования криптографических методов, является создание инфраструктуры безопасности и использованием открытых ключей.

Организация в АО «Гарнизон» системы информационной безопасности на основе инфраструктуры с открытым ключом позволит решить следующие задачи, дающие преимущества:

- организация обеспечения защищенного документооборота с использованием имеющихся систем, как внутри, так и при взаимоотношениях с другими организациями. Это позволит повысить эффективность и снизить накладные расходы на администрирование системы и использовать единые стандарты защиты данных;
- возможность реализации централизованно контролируемой системы информационной безопасности, при этом гибкой и динамически управляемой;
- универсализация методов обеспечения доступа пользователей и защиты для системы электронной почты, системы доступа в Internet и других систем с

использованием уже имеющихся в этих приложениях механизмов обеспечения информационной безопасности;

- использование имеющихся реализаций российских криптографических алгоритмов в операциях с сертификатами и при защите электронного документооборота.

Организация защищенного on-line взаимодействия удаленных сетей филиалов, и организаций партнеров на основе использования средств криптозащиты, позволит:

- защитить конфиденциальную информацию при ее передаче по каналам связи; защитить внутренние ЛВС, от несанкционированных воздействий извне; оптимизировать затраты на администрирование сетей удаленных подразделений.

Все средства криптографической защиты информации должны строиться на основе базисного криптографического ядра, прошедшего всесторонние исследования специализированными организациями.

Ключевая система применяемых в АО «Гарнизон» средств криптографической защиты информации должна обеспечивать криптографическую живучесть, разделение пользователей по уровням обеспечения защиты и зонам их взаимодействия между собой и пользователями других уровней.

8.11 Защита речевой информации

Под акустической (речевой) понимается информация, носителем которой являются акустические сигналы. В том случае, если источником информации является человеческая речь, акустическая информация называется речевой.

Воздушные:

- перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по радиоканалу;
- перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по сети электропитания;
- перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по оптическому каналу в ИК-диапазоне;
- перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по телефонным линиям;
- перехват акустических сигналов микрофонами, комплексированными с устройствами их подключения к телефонным линиям по сигналу вызова от внешнего телефонного абонента;
- перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по трубам водоснабжения, отопления, металлоконструкциям.

Электроакустические:

- перехват акустических колебаний через вспомогательные технические средства (ВТСС), обладающие микрофонным эффектом, путем подключения их к соединительным линиям;
- перехват акустических колебаний через ВТСС, путем ВЧ-навязывания.

Вибрационные:

- перехват акустических сигналов с помощью электронных стетоскопов;
- перехват акустических сигналов стетоскопами, комплексированными с устройствами перехвата информации по радиоканалу, оптическому каналу в ИК- диапазоне, по трубам водоснабжения, отопления, металлоконструкциям и т.д.

Параметрические:

- перехват акустического сигнала путем приема и детектирования побочных электромагнитных излучений (на частотах ВЧ-генераторов) технических средств обработки информации и ВТСС при модуляции информативным сигналом;
- перехват акустического сигнала путем ВЧ-облучения специальных полуактивных закладных устройств.

Оптикоэлектронный (лазерный):

- перехват акустического сигнала путем лазерного зондирования оконных стекол.

Помещения, в которых предусматривается ведение конфиденциальных переговоров, должны быть проверены на предмет отсутствия в них (в стеновых панелях, фальшполах и фальшпотолках, мебели, технических средствах, размещенных в этих помещениях) закладных устройств, технические средства передачи информации (телефоны, телефаксы, модемы), а также различные электрические и прочие цепи, трубопроводы, системы вентиляции и кондиционирования и т.д. должны быть защищены таким образом, чтобы акустические сигналы не могли быть перехвачены за пределами контролируемой зоны, а в необходимых случаях и за пределами данного выделенного помещения.

В этих целях используются проектные решения, обеспечивающие звукоизоляцию помещений, специальные средства обнаружения закладных устройств, на технические средства передачи информации устанавливаются устройства, предотвращающие перехват акустических сигналов с линий связи, на электрические цепи, выходящие за пределы контролируемой зоны, ставятся фильтры, а на трубопроводы диэлектрические вставки, используются системы активной защиты в акустическом и других диапазонах.

8.12 Управление системой обеспечения информационной безопасности

Управление системой обеспечения информационной безопасности представляет собой целенаправленное воздействие на компоненты системы обеспечения безопасности (организационные, технические, программные и криптографические) с целью достижения требуемых показателей и норм защищенности циркулирующей в информационной системе информации в условиях реализации основных угроз безопасности.

Главной целью организации управления системой обеспечения информационной безопасности является повышение надежности защиты информации в процессе ее обработки, хранения и передачи.

Целями управления системой обеспечения информационной безопасности являются: на этапе создания и ввода в действие новых информационных технологий:

- разработка и реализация технических программ и координационных планов создания нормативно-правовых основ и технической базы, обеспечивающей использование передовых средств и технологий обработки и передачи информации в защищенном исполнении в интересах обеспечения информационной безопасности;

- организация и координация взаимодействия в этой области разработчиков; создание действенной организационной структуры, обеспечивающей комплексное решение задач информационной безопасности при функционировании компонентов информационных технологий;

- на этапе эксплуатации компонентов информационной системы:

- обязательное и неукоснительное выполнение предусмотренных на этапе создания процедур, направленных на обеспечение информационной безопасности, всеми задействованными в системе участниками, эффективное пресечение посягательств на информационные ресурсы, технические средства и информационные технологии, своевременное выявление негативных тенденций и совершенствование управления в области защиты информации.

Управление системой обеспечения безопасности информации реализуется специализированной подсистемой, представляющей собой совокупность органов управления, технических, программных и криптографических средств и организационных мероприятий и взаимодействующих друг с другом пунктов управления различных уровней. Функциями подсистемы управления являются: информационная и управляющая.

Информационная функция заключается в непрерывном контроле состояния системы защиты, проверке соответствия показателей защищенности допустимым значениям и немедленном информировании о возникающих в ситуациях, способных привести к нарушению информационной безопасности. К контролю состояния системы защиты предъявляются два требования: полнота и достоверность. Полнота характеризует степень охвата всех средств защиты и параметров их функционирования. Достоверность контроля характеризует степень адекватности значений контролируемых параметров их истинному значению. В результате обработки данных контроля формируется информация состояния системы защиты.

Управляющая функция заключается в формировании планов реализации технологических операций с учетом требований безопасности информации в условиях, сложившихся для данного момента времени, а также в определении места возникновения ситуации уязвимости информации и предотвращении ее утечки за счет оперативного блокирования участков информационной системы, на которых возникают угрозы безопасности информации. К управляющим функциям относятся учет, хранение, и выдача документов и информационных носителей, паролей и ключей. При этом генерация паролей, ключей, сопровождение средств разграничения доступа, а также контроль за ходом

технологического процесса обработки конфиденциальной информации возлагается на сотрудников подразделений информационной безопасности.

8.13 Контроль эффективности системы защиты

Контроль эффективности защиты информации осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, за счет несанкционированного доступа к ней, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации, разрушение средств информатизации. Контроль может проводиться как подразделениями обеспечения информационной безопасности, так и привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности.

Оценка эффективности мер защиты информации проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

9 Порядок утверждения, внесения изменений и дополнений

Настоящая Политика вступает в законную силу с даты утверждения Генеральным директором АО «Гарнизон».

Изменения и дополнения в настоящую Политику вносятся по инициативе Генерального директора, заместителей Генерального директора, ПДТК и утверждаются Генеральным директором.

В случае вступления отдельных пунктов в противоречие с новыми законодательными актами, эти пункты утрачивают юридическую силу до момента внесения изменений в настоящую Политику.

Разработал:

Специалист по ИБ _____

Согласовано:

Заместитель Генерального директора	С.А.Штыкулин
Заместитель Генерального директора	С.И.Тен
Начальник Управления делами	А.Г.Клюшкин
Начальник отдела общего обеспечения Управления делами	С.А.Рудяк
Заместитель начальника отдела – заведующий сектором администрирования компьютерных сетей и технической поддержки отдела общего обеспечения Управления делами	А.В.Бобровников

Приложение Б
(рекомендуемое)

УТВЕРЖДАЮ
Генеральный директор

_____ И.О. Фамилия
«____»_____201__г

ПЛАН
РАБОТ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
на _____ год
(срок действия плана)

№ п/п	Наименование мероприятия	Цель	Срок исполнения	Исполнитель	Отметка о выполнении
1	2	3	4	5	6

Специалист по информационной безопасности

_____ И.О. Фамилия

«____»_____201__г

СОГЛАСОВАНО
Зам. Генерального директора

_____ И.О. Фамилия

«____»_____201__г

Приложение В
(рекомендуемое)

УТВЕРЖДАЮ
Генеральный директор

_____ И.О. Фамилия
«____»_____201__г

ПЛАН
ПРОВЕДЕНИЯ ВНУТРЕННИХ АУДИТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

на _____ год
(срок действия плана)

№ п/п	Проверяемое подразделение	Процедура	Пункт НД	Срок проведения аудита (месяц)												Примечание
				1	2	3	4	5	6	7	8	9	10	11	12	

Специалист по информационной безопасности

_____ И.О. Фамилия

«____»_____201__г

СОГЛАСОВАНО
Зам. Генерального директора
по общим вопросам и вопросам
защиты государственной тайны
_____ И.О. Фамилия

«____»_____201__г

Приложение Г
(рекомендуемое)

Форма решения заседания ПДТК

Гриф (при необходимости)
Экз. № _____

УТВЕРЖДАЮ
Генеральный директор

_____
подпись, инициалы и фамилия

«____»_____201__г

РЕШЕНИЕ
заседания ПДТК

№_____ от «___»_____201____г.

Повестка _____
_____

Присутствовали: _____
_____

С докладом выступил:_____ _____
должность Ф.И.О.

Выступили с предложениями:
_____
_____

Принятые решения:

№ п.п.	Код[1] мероприятия	Содержание мероприятия	Срок исполнения	Должность, фамилия исполнителя	Отметка о выполнении
1	2	3	4	5	6

Специалист по ИБ _____ _____
подпись инициалы, фамилия

[1]Указывают:
К- мероприятия, относящиеся к коррекции

КрД – корректирующие действия

ПрД – предупреждающие действия

П – прочие действия

Библиография

[1] Постановление Правительства РФ № 3-1 от 05 января 2004 года «Инструкция по обеспечению режима секретности в Российской Федерации»

[2] «Инструкция по обеспечению режима секретности в АО «Гарнизон», утверждена приказом Генерального директора _____

[3] «Инструкция по обеспечению внутриобъектового и пропускного режима в АО «Гарнизон», утверждена приказом Генерального директора _____

Лист регистрации изменений

Изменения	Номера листов (страниц)			Номер документа	Подпись	Дата изменения	Срок введения изменения
	измен.	замен.	новых				