Политика информационной безопасности

1. Общие положения

1.1. Термины и определения

- **Автоматизированная система обработки информации** - организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов: серверов системы Tender.Pro, рабочих станций и каналов передачи данных, 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;

- **Авторизованный субъект доступа** - субъект, которому предоставлены соответствующие права доступа к объектам системы (полномочия);

- **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;

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

- **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;

- **Безопасность информационной технологии** - защищенность технологического процесса переработки информации;

- **Безопасность любого ресурса информационной системы** - складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности;

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

- **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.

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

- **Безопасность субъектов информационных отношений** - защищенность жизненно важных интересов субъектов информационных отношений от нанесения им материального, морального или иного вреда путем воздействия на информацию и/или средства ее обработки и передачи. Безопасность достигается проведением единой Концепции в области охраны и защиты важных ресурсов, системой мер экономического, организационного и иного характера, адекватных угрозам жизненно важным интересам;

- **Внешний воздействующий фактор** - воздействующий фактор, внешний по отношению к объекту информатизации;

- **Внутренний воздействующий фактор** - воздействующий фактор, внутренний по отношению к объекту информатизации;

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

- **Выделенное 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;

- **Документ** - зафиксированная на материальном носителе информация с реквизитами, позволяющими его идентифицировать;

- **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;

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

- **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;

- **Естественные угрозы** - это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера

или стихийных природных явлений, независящих от человека;

- **Жизненно важные интересы** - совокупность потребностей, удовлетворение которых необходимо для надежного обеспечения существования и возможности прогрессивного развития субъекта.

- **Замысел защиты** - основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность мероприятий, необходимых для достижения цели защиты информации и объекта;

- **Защита информации** - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на информацию;

- **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;

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

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

- **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;

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

- **Информационные ресурсы** - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах;

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

- **Информационная система ООО “ТендерПро”** - 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 Компании и передаваемых Компании Клиентами.;

- **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;
- нарушение адресности и оперативности информационного обмена;
- нарушение технологии обработки, хранения данных и информационного обмена.

- **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);

- **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;

- **Контролируемая зона** - датацентры в которых расположены сервера проекта, корпуса серверов, офис Компании.

- **Границей контролируемой зоны** могут являться:

  - серверное помещение, корпуса серверов ;

  - периметр офиса.

- **Конфиденциальность информации** - субъективно определяемая (приписываемая) информации характеристика (свойство), 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;

- **Корпоративная информационная система** - автоматизированная система обработки информации Tender.Pro;

- **Морально-этические меры защиты информации** - традиционно сложившиеся в компании 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.

- **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;

- **Несанкционированное действие** - действие субъекта в нарушение установленных в системе правил обработки информации;

- **Несанкционированный доступ** - доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа;

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

- **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.

- **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;

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

- **Пароль** - служебное слово, которое считается известным узкому кругу лиц (одному лицу) и используется для ограничения доступа к информации;

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

- **Правила разграничения доступа** - совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе;

- **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;

- **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.

- **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 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.

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

установленными правилами;

- **Секретная информация** - речевая информация, информация, циркулирующая в средствах вычислительной техники и связи, телекоммуникациях, а также другие информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, представленные в виде информативных акустических и электрических сигналов, физических полей, материальных носителей (в том числе на магнитной и оптической основе), информационных массивов и баз данных.

- **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 Компании;

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

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

- **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;

- **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.);

- **Технология обеспечения информационной безопасности** - определенное распределение функций и регламентация порядка их исполнения, а также порядка взаимодействия подразделений и сотрудников Компании по обеспечению комплексной защиты информационных ресурсов Компании;

- **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;

- **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;

- **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;

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

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

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

- **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;

- **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;

- **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.).

- **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;

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

- **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.

1.2. Назначение и правовая основа документа

Политика информационной безопасности Компании (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 руководствуется организация в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации в Компании.

Политика учитывает современное состояние и ближайшие перспективы развития информационных технологий в Компании, цели, задачи и правовые основы их эксплуатации, режимы функционирования, а также содержит анализ угроз безопасности для объектов и субъектов информационных отношений Компании.

Основные положения и требования данного документа распространяются на все структурные подразделения Компании. Основные вопросы Политика также распространяются на другие организации и учреждения, взаимодействующие с Компанией в качестве поставщиков и потребителей информационных ресурсов Компании 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 Государственной технической комиссии при Президенте Российской Федерации, Федерального агентства правительственной связи и информации при Президенте Российской Федерации.

Политика является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности информации в Компании;

- принятия управленческих решений и разработке практических мер по воплощению политика безопасности информации и выработки комплекса согласованных мер, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;

- координации деятельности структурных подразделений Компании 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 Компании.

Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности Компании 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.

2. Объекты защиты

Основными объектами системы информационной безопасности в Компании являются:

- информационные ресурсы с ограниченным доступом, составляющие коммерческую, тайну или иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, а также открытая (общедоступная) информация, необходимая для работы Компании, независимо от формы и вида ее представления;

- процессы обработки информации в информационной системе Компании информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;

- информационная инфраструктура, включающая системы обработки 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.

2.1. Структура, состав и размещение основных объектов защиты, информационные связи

Информационная среда Компании является распределенной структурой, объединяющей информационные подсистемы Центрального офиса и датацентра.

К основным особенностям информационной среды Компании, относятся:

- территориальная распределенность компонентов информационной системы;

- локализация основных угроз информационной безопасности в периметре датацентра и на уровне каналов связи с серверами Компании;

- значительное расширение сферы использования автоматизированных систем обработки информации, широкое многообразие и повсеместное распространение информационно-управляющих систем в Компании;

- большое разнообразие решаемых задач и типов обрабатываемых данных, сложные режимы автоматизированной обработки информации с широким совмещением выполнения информационных запросов различных пользователей;

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

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

- удаленность владельцев данных от физических структур и места размещения данных (информации);

- наличие большого числа информационных каналов взаимодействия с «внешним миром» (источниками и потребителями информации);

- необходимость обеспечения непрерывности функционирования Компании;

- высокая интенсивность информационных потоков;

- разнообразие категорий пользователей и обслуживающего персонала системы.

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

2.2. Категории информационных ресурсов, подлежащих защите

В Компании циркулирует информация различных уровней конфиденциальности, содержащая сведения ограниченного распространения (служебная, коммерческая информация и персональные данные), и открытые сведения.

Защите подлежит вся информация и информационные ресурсы Компании, независимо от ее представления и местонахождения в информационной среде Компании:

- сведения, составляющие коммерческую тайну, доступ к которым ограничен собственником информации в соответствии с Федеральным законом «Об информации, информатизации и защите информации»;

- сведения о частной жизни граждан (персональные данные), доступ к которым ограничен в соответствии с Федеральным законом «Об информации, информатизации и защите

информации»;

- открытая информация, необходимая для обеспечения нормального функционирования Компании.

3. Цели и задачи обеспечения безопасности информации

3.1. Интересы затрагиваемых субъектов информационных отношений

Субъектами информационных отношений при обеспечении информационной безопасности Компании являются:

- Компания, как собственник информационных ресурсов;
- подразделения Компании, участвующие в информационном обмене;
- руководство и сотрудники структурных подразделений Компании, в соответствии с возложенными на них функциями;
- юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационной системе Компании;
- другие юридические и физические лица, задействованные в обеспечении выполнения Компаниям своих функций (клиенты, консультанты, 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 ее тиражирования (защиты авторских прав, прав собственника информации и т.п.).

3.2. Цели защиты

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений Компании 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 уровня операционного и других рисков (риск нанесения урона деловой репутации Компании, правовой риск и т.д.).

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

- доступности информации для легальных пользователей (устойчивого функционирования информационной системы Компании, 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 Компании и передаваемой по каналам связи;

- конфиденциальности - сохранения в тайне определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи;

- шифрования информации и каналов связи.

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

3.3. Основные задачи системы обеспечения безопасности информации Компании

Для достижения основной цели защиты и обеспечения указанных свойств информации система обеспечения информационной безопасности Компании 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 Компании;

- 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 Компании посторонних лиц (доступ к информационным ресурсам должны иметь только

зарегистрированные в установленном порядке пользователи);

- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Компании (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 Компании 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.

3.4. Основные пути решения задач системы защиты

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

- строгим учетом всех подлежащих защите ресурсов информационной системы Компании (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

- журналированием действий персонала, осуществляющего обслуживание и модификацию программных и технических средств корпоративной информационной системы;

- полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Компании по вопросам обеспечения безопасности информации;

- подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки;

- наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Компании;

- четким знанием и строгим соблюдением всеми пользователями информационной системы Компании требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

- персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам Компании;

- непрерывным поддержанием необходимого уровня защищенности элементов информационной среды Компании;

- применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

- эффективным контролем над соблюдением пользователями информационных ресурсов Компании требований по обеспечению безопасности информации;

- юридической защитой интересов Компании 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;

4. Основные угрозы безопасности информации Компании

4.1. Угрозы безопасности информации и их источники

Все множество потенциальных угроз безопасности информации по природе их возникновения разделяются на два класса: естественные (объективные) и искусственные (субъективные).

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

- 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).

Источники угроз по отношению к самой информационной системе могут быть как внешними, так и внутренними.

Основными источниками угроз безопасности информации Компании 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 Компании (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 Компании 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 Компании;

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

- удаленное несанкционированное вмешательство посторонних лиц из территориально удаленных сегментов корпоративной информационной системы и внешних сетей общего назначения (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 Компании 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 Компании (способами нанесения ущерба субъектам информационных отношений) являются:

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

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

4.2. Пути реализации непреднамеренных искусственных (субъективных) угроз безопасности информации

Сотрудники Компании, зарегистрированные как легальные пользователи информационной системы Компании 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 Компании (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 Компании 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;

- проектирование архитектуры систем, технологий обработки данных, разработка программного обеспечения с возможностями, представляющими опасность для функционирования информационной системы Компании и безопасности информации;

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

- ввод ошибочных данных;

- неумышленная порча носителей информации;

- неумышленное повреждение каналов связи;

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

- заражение компьютеров вирусами;

- несанкционированный запуск технологических программ, способных вызвать потерю работоспособности компонентов Корпоративной 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.

4.3. Пути реализации преднамеренных искусственных (субъективных) угроз безопасности информации

Основные возможные пути умышленной дезорганизации работы, вывода компонентов информационной системы Компании 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 Компании или разрушению информационных или программно-технических ресурсов;

- “взлом” системы - несанкционированный доступ к ресурсам компании с использованием уязвимостей в информационной безопасности системы;

- несанкционированное копирование документов и носителей информации; умышленное искажение информации, ввод неверных данных;

- незаконное получение атрибутов разграничения доступа (агентурным путем, используя халатность пользователей, путем подделки, подбора и т.п.);

- несанкционированный доступ к ресурсам Корпоративной информационной системы с рабочих станций легальных пользователей;

- хищение или вскрытие шифров криптозащиты информации;

4.4. Пути реализации основных естественных угроз безопасности информации

- 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.

4.5. 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 Компании 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 Компании (или подразделения другой организации, являющийся легальным пользователем информационной системы Компании), 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 Компании (или подразделения другого организации, являющийся зарегистрированным пользователем информационной системы Компании), 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 Компании (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 Компании. 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 Компании.

- 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 Компании.

Внутренним нарушителем может быть лицо из следующих категорий сотрудников Компании:

- зарегистрированные пользователи информационной системы Компании;

- сотрудники Компании, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационной системы Компании, но имеющие доступ в здания и помещения;

- персонал, обслуживающий технические средства корпоративной информационной системы Компании;

- сотрудники подразделений Компании, задействованные в разработке и сопровождении программного обеспечения;

- сотрудники подразделений обеспечения безопасности Компании;

- руководители различных уровней.

Категории лиц, которые могут быть внешними нарушителями:

- уволенные сотрудники Компании;

- представители организаций, взаимодействующих по вопросам технического обеспечения Компании;

- клиенты Компании;

- посетители (представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.);

- представители конкурирующих организаций;

- члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;

- лица, случайно или умышленно проникшие в корпоративную информационную систему Компании из внешних телекоммуникационных сетей (хакеры).

Пользователи и обслуживающий персонал из числа сотрудников Компании 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 находится 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 Компании знания и опыт выделяют их среди других источников внешних угроз.

Криминальные структуры являются наиболее агрессивным источником внешних угроз. Для осуществления своих замыслов эти структуры могут идти на открытое нарушение закона и вовлекать в свою деятельность сотрудников Компании 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 Компании и криминальными структурами.

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. Конкурирующие организации, криминальные структуры и спецслужбы могут использовать эти организации для временного устройства на работу своих членов с целью доступа к ресурсам информационной системы Компании.

Принимаются следующие ограничения и предположения о характере действий возможных нарушителей:

- нарушитель скрывает свои несанкционированные действия от других сотрудников Компании;

- 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.

4.6. Утечка информации по техническим каналам

При проведении мероприятий и эксплуатации технических средств возможны следующие каналы утечки или нарушения целостности информации, нарушения работоспособности технических средств:

- просмотр информации с экранов дисплеев и других средств ее отображения с помощью оптических средств;

- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности информационного обмена, в том числе электромагнитное, через специально внедренные электронные и

программные средства («закладки»).

Перехват информации ограниченного распространения или воздействие на нее с использованием технических средств может вестись непосредственно из зданий, расположенных в непосредственной близости от объектов Компании, мест временного пребывания заинтересованных в перехвате информации или воздействии на нее лиц при посещении ими подразделений Компании, а также с помощью скрытно устанавливаемой в районах важнейших объектов и на их территориях автономной автоматической аппаратуры.

В качестве аппаратуры разведок или воздействия на информацию и технические средства могут использоваться:

- средства разведки для перехвата радиоизлучений от средств радиосвязи, радиорелейных станций, и приема сигнала от автономных автоматических средств разведки и электронных устройств перехвата информации («закладок»);
- стационарные средства, размещаемые в зданиях;
- портативные возимые и носимые средства, размещаемые в зданиях, в транспортных средствах, а также носимые лицами, ведущими разведку;

Кроме перехвата информации техническими средствами разведки возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах контролируемой зоны. Такого рода утечка информации возможна в следствии:

- непреднамеренного прослушивания без использования технических средств разговоров, ведущихся в выделенном помещении, из-за недостаточной звукоизоляции его ограждающих конструкций, систем вентиляции и кондиционирования воздуха;
- случайного прослушивания телефонных переговоров при проведении профилактических работ на АТС, кроссах, кабельных коммуникациях с помощью контрольной аппаратуры;
- просмотра информации с экранов дисплеев и других средств ее отображения.

5. Основные принципы построения системы информационной безопасности Компании

Построение системы, обеспечения безопасности информации Компании, 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.

5.1. Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности информации Компании в соответствии с действующим законодательством в области информации, информатизации и защиты информации, а также других нормативных актов по безопасности информации, 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 безопасности информации не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях к информации конкретных подсистем.

Все пользователи информационной системы Компании должны иметь представление об ответственности за правонарушения в области информации.

Реализация данного принципа необходима для защиты имени и репутации Компании.

5.2. Системность

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

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационной системы Компании, 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.

5.3. 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.

5.4. Непрерывность защиты

Обеспечение безопасности информации - процесс, осуществляемый Руководством Компании, подразделениями защиты информации 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 Компании и каждый сотрудник Компании должен принимать участие в этом процессе. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности Компании. И ее эффективность зависит от участия руководства Компании 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.

5.5. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите информации и реализацию мер обеспечения безопасности информации 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.

5.6. Преемственность и совершенствование

Предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационной системы Компании 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.

5.7. Разумная достаточность (экономическая целесообразность)

Предполагает соответствие уровня затрат на обеспечение безопасности информации 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 Компании. 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.

5.8. 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.

5.9. 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.

5.10. 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 Компании. 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.

5.11. Взаимодействие и сотрудничество

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

Важным элементом эффективной системы обеспечения безопасности информации в Компании является высокая культура работы с информацией. Руководство Компании несет ответственность за строгое соблюдение этических норм и стандартов профессиональной деятельности, за создание корпоративной культуры, подчеркивающей и демонстрирующей персоналу на всех уровнях важность обеспечения информационной безопасности Компании. Все сотрудники Компании 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.

5.12. Гибкость системы защиты

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

- изменения организационной и штатной структуры Компании;
- корпоративная реструктуризация, слияния и поглощения;
- расширение или приобретение бизнеса за рубежом (включая влияние изменений в соответствующей экономической или правовой среде);
- 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.

5.13. 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.

5.14. 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.

5.15. 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 безопасности информации и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по безопасности информации.

5.16. 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 Компании (специалистами подразделений защиты информации).

5.17. 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 Компании или подразделениями обеспечения безопасности должны немедленно доводиться до сведения руководителей соответствующего уровня и оперативно устраняться. О существенных недостатках необходимо сообщать руководству Компании. 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.

6. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов

6.1. Меры обеспечения информационной безопасности

Все меры обеспечения безопасности информационной системы Компании подразделяются на:

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

Законодательные (правовые) 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 Компании.

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 Компании 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.

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, периодическое подведение общего баланса всех учетных счетов и т.п.

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.

6.2. 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 Компании целесообразно разбить на два уровня. К верхнему уровню относятся решения руководства, затрагивающие деятельность Компании 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 секретов и разграничения доступа к информации ограниченного распространения;

- выбирать программно-технические (аппаратные) средства криптозащиты, противодействия НСД, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

6.3. Регламентация доступа в помещения

Чувствительные к воздействиям компоненты информационной системы Компании должны размещаться в помещениях, оборудованных надежными автоматическими замками, средствами сигнализации и постоянно 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 Компании, должны сдаваться под охрану с включением сигнализации и с отметкой в книге приема и сдачи служебных помещений.

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

В случае оснащения помещений средствами охранной сигнализации, а также автоматизированной системой приема и регистрации сигналов от этих средств, прием-сдача таких помещений под охрану осуществляется на основании специально разрабатываемой инструкции.

Помещения должны быть обеспечены средствами уничтожения документов.

6.4. 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 Компании 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 Компании. 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 Компании, ответственным за информационное сопровождение данного ресурса;

- начальник имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями;

- наиболее ответственные технологические операции должны производиться по правилу «в две руки» - правильность введенной информации подтверждается другим должностным лицом, не имеющим права ввода информации.

Все сотрудники Компании или других организаций, зарегистрированные как легальные пользователи информационной системы Компании 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 в Компании.

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

6.5. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов

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

В целях поддержания режима информационной безопасности аппаратно-программная конфигурация автоматизированных рабочих мест сотрудников Компании, 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 (COM, LPT, USB, IR порты, дисководы НГМД, CD) 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 с подразделениями обеспечения информационной безопасности Компании.

В компонентах корпоративной информационной системы и на рабочих местах пользователей должны устанавливаться и использоваться программные средства, только полученные от Управления информационных технологий. Использование программного обеспечения, не прошедшего проверку и не учтенного в Компании, должно быть запрещено.

Для решения специальных задач по оценке защищенности информационной сети Компании и построении системы защиты информации в сети Компании может применяться специальное программное обеспечение, согласованное с Управлением информационных технологий.

6.6. 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 – начальником Службы экономической безопасности.

6.7. Подбор и подготовка персонала, обучение пользователей

Пользователи информационной системы Компании, 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 Компании.

Обеспечение безопасности информации возможно только после выработки у пользователей определенной культуры работы, т.е. норм, обязательных для исполнения всеми, кто работает с информационными ресурсами Компании. К таким нормам можно отнести запрещение любых умышленных или неумышленных действий, которые нарушают нормальную работу компонентов информационной системы Компании, вызывают дополнительные затраты ресурсов, нарушают целостность хранимой и обрабатываемой информации, нарушают интересы законных пользователей, владельцев или собственников.

Все пользователи информационной системы Компании должны быть ознакомлены с организационно - распорядительными документами по обеспечению информационной безопасности Компании, 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.

6.8. Подразделение обеспечения информационной безопасности

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

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

- формирование требований к системам защиты в процессе создания и дальнейшего развития существующих компонентов информационной системы Компании;
- подготовка решений по обеспечению конфиденциальности, доступности, целостности данных, в том числе решений по обеспечению надежной защиты от мошенничества при использовании пластиковых карт;
- 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 Компании;
- 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 Компании 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 Компании должен определяться следующим образом:

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

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

- сотрудники подразделения обеспечения информационной безопасности должны иметь право доступа во все помещения, где, установлены технические средства информационной системы Компании, и право прекращать обработку информации при наличии непосредственной угрозы для нее;

- руководителю подразделения должно быть предоставлено право запрещать включение новых компонентов информационной системы Компании 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 Компании в указанной области;

- получать информацию от пользователей информационной системы Компании по любым аспектам применения информационных технологий в Компании;

- 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 Компании по вопросам обеспечения 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 Компании 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.

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

Любое грубое нарушение порядка и правил пользования информационными ресурсами Компании 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 Компании.

Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

- индивидуальная идентификация пользователей и инициированных ими процессов, т.е. установление за ними идентификатора (login, Username), 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.).

6.10. Средства обеспечения информационной безопасности Компании

Для обеспечения информационной безопасности Компании 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;
- криптографические средства.

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

6.10.1. 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.

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

- наличие специально внедренных закладных устройств;
- побочные электромагнитные излучения и наводки;
- 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.

6.10.2. 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 снижения уровня и информативности побочных излучений, создаваемых компонентами информационной системы Компании, предназначенными для обработки закрытой информации;

На технические средства защиты возлагается решение следующих основных задач:

- идентификация и аутентификация пользователей при помощи имен или специальных аппаратных средств (Advantor, Touch Memory, Smart Card 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 всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;
- защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информации, находящейся на нем.

6.10.3. Средства идентификации и аутентификации пользователей

В целях предотвращения работы с ресурсами информационной системы Компании посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей).

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.

6.10.4. 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 Компании 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.

6.10.5. 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).

6.10.6. Средства оперативного контроля и регистрации событий безопасности

Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т.п.), которые могут повлечь за собой нарушение Концепции безопасности и 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 администратора безопасности о нарушениях.

При регистрации событий безопасности в журнале должна фиксироваться следующая информация:

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

6.10.7. Криптографические средства защиты информации

Основными элементами системы, обеспечения безопасности информации Корпоративной информационной системы Компании являются криптографические методы и средства защиты. Перспективным направлением, использования криптографических методов, является создание инфраструктуры безопасности и использованием открытых ключей (PKI, Public Key Infrastructure).

Организация в Компании системы информационной безопасности на основе инфраструктуры с открытым ключом позволит решить следующие задачи, дающие преимущества бизнесу Компании:

- организация обеспечения защищенного документооборота (в том числе платежного) с использованием имеющихся систем, как внутри Компании, так и при взаимоотношениях с организациями-корреспондентами и клиентами Компании. Это позволит повысить эффективность и снизить накладные расходы на администрирование системы и использовать единые стандарты защиты данных;
- возможность реализации системы информационной безопасности в Компании, централизованно контролируемой из центрального офиса Компании, при этом гибкой и

динамически управляемой;

- универсализация методов обеспечения доступа пользователей и защиты транзакций для системы электронной почты, автоматизированной банковской системы, системы дистанционного обслуживания, 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, дополнительных офисов и партнеров Компании на основе использования средств криптозащиты, в том числе при осуществлении финансовых операций, позволит:

- защитить конфиденциальную информацию Компании при ее передаче по каналам связи;

- защитить внутренние ЛВС Центрального офиса Компании, региональных филиалов, дополнительных офисов от несанкционированных воздействий извне;

- сделать информационные взаимодействия Компании более эффективным за счет централизации управления ресурсами;

- оптимизировать затраты на администрирование сетей удаленных подразделений.

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

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

Конфиденциальность и защита информации при ее передаче по каналам связи должна обеспечиваться также за счет применения в системе шифросредств абонентского шифрования. В корпоративной информационной системе, являющейся структурой с распределенными информационными ресурсами, также должны использоваться средства формирования и проверки электронной цифровой подписи, обеспечивающие целостность и юридически доказательное подтверждение подлинности сообщений, а также аутентификацию пользователей, абонентских пунктов и подтверждение времени отправления сообщений.

6.11. Локализация и сегментация

Локализация защищенного периметра в пределах датацентра и отдельных серверов в совокупности снижает риски за счет уменьшения потенциальных уязвимостей в системе информационной безопасности.

Информация за пределы защищенного периметра должна предоставляться строго в необходимых, ограниченных объемах в соответствии с функциями и ролями пользователей.

6.12. Управление системой обеспечения безопасности информации

Управление системой обеспечения безопасности информации 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 Компании информации в условиях реализации основных угроз безопасности.

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

Целями управления системой обеспечения безопасности информации 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 безопасности информации;
    - организация и координация взаимодействия в этой области разработчиков;
    - создание действенной организационной структуры, обеспечивающей комплексное решение задач безопасности информации при функционировании компонентов информационных технологий;
- на этапе эксплуатации компонентов информационной системы:
    - обязательное и неукоснительное выполнение предусмотренных на этапе создания процедур, направленных на обеспечение безопасности информации, 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 безопасности информации. 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 секретной (конфиденциальной) информации возлагается на сотрудников подразделений информационной безопасности.

6.13. 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 Компании, 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.

7. Основные направления технической Концепции в области обеспечения безопасности информации в Компании

7.1. Техническая Концепция в области обеспечения безопасности информации

Реализация технической Концепции в области обеспечения безопасности информации должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищенности информации не только с помощью одного отдельного средства (мероприятия), но и с помощью их простой совокупности. Необходимо их системное согласование между собой (комплексное применение), а отдельные разрабатываемые элементы информационной системы должны рассматриваться как часть единой информационной системы в защищенном исполнении при оптимальном соотношении технических (аппаратных, программных) средств и организационных мероприятий.

Основными направлениями реализации технической Концепции обеспечения безопасности информации Компании являются:

- обеспечение защиты информационных ресурсов от хищения, утраты, утечки, уничтожения, искажения или подделки за счет несанкционированного доступа и специальных воздействий;

- обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и при передаче по каналам связи.

Система обеспечения безопасности информации Компании должна предусматривать комплекс организационных, программных и технических средств и мер по защите информации в процессе ее обработки и хранения, при передаче информации по каналам связи, при ведении конфиденциальных переговоров, раскрывающих сведения с ограниченным доступом, при использовании технических и программных средств.

В рамках указанных направлений технической Концепции обеспечения безопасности информации осуществляются:

- реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к работам, документам и информации; * реализация системы инженерно-технических и организационных мер охраны, предусматривающей многорубежность и равнопрочность построения охраны (территории, здания, помещения) с комплексным применением современных технических средств охраны, обнаружения, наблюдения, сбора и обработки информации, обеспечивающих достоверное отображение и объективное документирование событий;

- ограничение доступа в здания и помещения, где проводятся работы конфиденциального характера и размещены средства информатизации и коммуникации, на которых обрабатывается (хранится, передается) информация, а также непосредственно к самим средствам информатизации и коммуникациям;

- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защита информации в информационной системе Компании;

- учет документов, информационных массивов, регистрация действий пользователей и обслуживающего персонала, контроль за несанкционированным доступом и действиями пользователей, обслуживающего персонала и посторонних лиц;

- предотвращение внедрения в корпоративную информационную систему Компании программ-вирусов, программных закладок.

- реализация инфраструктуры с открытым ключом, криптографическая защита информации ограниченного пользования, обрабатываемой и передаваемой средствами вычислительной техники по открытым каналам связи;

- надежное хранение документов и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее хищение, подмену и уничтожение;

- необходимое резервирование технических средств и дублирование массивов и носителей информации;

- обеспечение акустической защиты помещений, в которых обсуждается информация конфиденциального характера;

- противодействие оптическим и лазерным средствам наблюдения.

7.2. Формирование режима безопасности информации

С учетом выявленных угроз безопасности информации Компании режим защиты должен формироваться как совокупность способов и мер защиты циркулирующей в информационной среде Компании информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, влекущих за собой нанесение ущерба владельцам или пользователям информации.

Комплекс мер по формированию режима обеспечения безопасности информации включает:

- установление в Компании организационно-правового режима обеспечения безопасности информации (разработку необходимых нормативных документов, работа с персоналом, правил делопроизводства);

- организационные и программно-технические мероприятия по предупреждению несанкционированных действий (доступа) к информационным ресурсам корпоративной информационной системы Компании;

- комплекс мероприятий по контролю функционирования средств и систем защиты информационных ресурсов ограниченного пользования после случайных или преднамеренных воздействий;

- комплекс оперативных мероприятий подразделений безопасности по предотвращению (выявлению) проникновения в Компания лиц, имеющих отношение к криминальным структурам.

Организационно-правовой режим предусматривает создание и поддержание правовой базы безопасности информации, в частности, разработку (введение в действие) следующих организационно-распорядительных документов:

- Положение о коммерческой тайне. Указанное Положение регламентирует организацию, порядок работы со сведениями, составляющими коммерческую тайну Компании, обязанности и ответственность сотрудников, допущенных к этим сведениям, порядок передачи материалов, содержащих сведения, составляющим коммерческую тайну Компании, государственным (коммерческим) учреждениям и организациям;

- Перечень сведений, составляющих служебную и коммерческую тайну. Перечень определяет сведения, отнесенные к категориям конфиденциальных, уровень и сроки обеспечения ограничений по доступу к защищаемой информации;

- Приказы и распоряжения по установлению режима безопасности информации:
    - допуске сотрудников к работе с информацией ограниченного распространения;
    - назначении администраторов и лиц, ответственных за работу с информацией ограниченного распространения в корпоративной информационной системе;
- Инструкции и функциональные обязанности сотрудникам:
    - по организации охранно-пропускного режима;
    - по организации делопроизводства;
    - по администрированию информационных ресурсов корпоративной информационной системы;
    - другие нормативные документы.
- Организационно-технические мероприятия по защите информации ограниченного распространения от утечки по техническим каналам предусматривают:
    - комплекс мер и соответствующих технических средств, ослабляющих утечку речевой и сигнальной информации - пассивная защита (защита);
    - комплекс мер и соответствующих технических средств, создающих помехи при съеме информации - активная защита (противодействие);
    - комплекс мер и соответствующих технических средств, позволяющих выявлять каналы утечки информации - поиск (обнаружение).

Физическая охрана объектов информатизации (компонентов Информационной системы Компании) включает:

- организацию системы охранно-пропускного режима и системы контроля допуска на объект;
- введение дополнительных ограничений по доступу в помещения, предназначенные для хранения информации ограниченного пользования (кодовые и электронные замки, карточки допуска и т.д.);
- визуальный и технический контроль контролируемой зоны объекта защиты; применение систем охранной и пожарной сигнализации.

Выполнение режимных требований при работе с информацией ограниченного пользования предполагает:

- разграничение допуска к информационным ресурсам ограниченного пользования; разграничение допуска к ресурсам корпоративной информационной системы;

- ведение учета ознакомления сотрудников с информацией ограниченного пользования;
- включение в функциональные обязанности сотрудников обязательства о неразглашении и сохранности сведений ограниченного пользования;
- организация уничтожения информационных отходов (бумажных, магнитных и т.д.);
- оборудование служебных помещений сейфами, шкафами для хранения бумажных и магнитных носителей информации.

Мероприятия технического контроля предусматривают:

- контроль за проведением технического обслуживания, ремонта носителей информации и средств вычислительной техники;
- проверки определенной части поступающего оборудования, предназначенного для обработки информации ограниченного пользования, на наличие специально внедренных закладных программ и устройств;
- оборудование компонентов и подсистем корпоративной информационной системы устройствами защиты от сбоев электропитания и помех в линиях связи;
- защита выделенных помещений при проведении закрытых (секретных) работ (переговоров);
- постоянное обновление технических и программных средств защиты от несанкционированного доступа к информации в соответствие с меняющейся оперативной обстановкой.

8. Порядок утверждения, внесения изменений и дополнений

Настоящая Политика вступает в законную силу с даты утверждения Правлением Компании.

Изменения и дополнения в настоящую Политику вносятся по инициативе Правления, Председателя Правления, Руководителя Службы внутреннего контроля, Начальника Управления информационных технологий, Начальника Управления безопасности, Начальника Отдела информационной безопасности и утверждаются решением Правления Компании.

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