|  |  |  |
| --- | --- | --- |
| |  | | --- | | МИНОБРНАУКИ РОССИИ | | Федеральное государственное бюджетное образовательное учреждение высшего образования **«МИРЭА − Российский технологический университет»**  **РТУ МИРЭА** |   **Институт комплексной безопасности и специального приборостроения (ИКБСП)** |
|  |

|  |  |
| --- | --- |
| **ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКОЙ РАБОТЫ № 1** | |
| по дисциплине  «Основы информационной безопасности» | |
| ВВыполнил студент группы БИСО-01-19 | Крюковская Екатерина Алексеевна |
|  |

Аккаунт github: https://github.com/moricifosatar

Москва 2020

Компания ООО «СМК Стей». Штат - 62 сотрудников. 8 - руководство, 10 - бухгалтерия, 5 - IT-отдел, 25 - менеджеры по работе с клиентами, 6 - отдел безопасности,3 - отдел маркетинга, 5 - отдел физической безопасности.

Управляющая часть компании использует телефонную связь, MS Office, 1С: Предприятие и т. д.

Бухгалтерия использует телефонную связь, MS Office, 1С: Бухгалтерию.

IT-отдел обеспечивает функционирование внутренней сети организации, а также сайта компании и личных кабинетов клиентов.

Менеджеры по работе с клиентами осуществляют работу с ними посредством Интернет, Телефонной связи и др.

Отдел безопасности обеспечивает целостность и сохранность личных данных клиентов и компании.

Отдел маркетинга обеспечивает конкурентоспособность, различные исследования и аналитику и др.

Отдел физической безопасности обеспечивает охрану от доступа посторонних лиц, защиту имущества компании и защиту сотрудников.

1. **Общие положения**

Настоящая «Политика информационной безопасности Общества» (далее – Политика) представляет собой официально принятую систему взглядов на проблему обеспечения информационной безопасности в автоматизированных системах (АС) Общества. Политика содержит систематизированное изложение целей и задач защиты, основных принципов и способов достижения требуемого уровня информационной безопасности, организационных, технологических и процедурных аспектов обеспечения информационной безопасности в АС.

Политика учитывает современное состояние и ближайшие перспективы развития АС, цели, задачи и правовые основы её создания и эксплуатации, режимы функционирования данной системы, а также анализа угроз безопасности для информационных ресурсов Общества.

Правовой основой настоящей Политики являются:

* Конституция Российской Федерации;
* Гражданский и Уголовный кодексы;
* Кодекс об административных правонарушениях;
* законы, указы, постановления и другие нормативные документы действующего законодательства Российской Федерации;
* нормативные документы федерального и территориальных фондов обязательного медицинского страхования, министерств здравоохранения и социального развития, Федеральной службы страхового надзора и др.;
* нормативные и регламентирующие документы государственных органов Российской Федерации (ФСТЭК, ФСБ, Роскомнадзор и др.);
* внутренние нормативно-методические и организационно-распорядительные документы Общества.

Основные положения и требования Политики распространяются на все структурные подразделения Общества, в которых осуществляется автоматизированная и смешанная обработка информации, содержащей сведения, составляющие коммерческую, служебную, врачебную тайну или персональные данные, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования АС. Основные положения Политики могут быть распространены также на подразделения других организаций и учреждений, осуществляющие взаимодействующие с АС в качестве поставщиков и потребителей (пользователей) информации АС.

Политика является методологической основой для:

* формирования и проведения единой политики в области информационной безопасности в АС;
* разработки стратегии информационной безопасности Общества, включая цели, задачи и комплекс мер по её практической реализации;
* принятия управленческих решений и разработки практических мер по воплощению политики информационной безопасности и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз информационной безопасности;
* координации деятельности структурных подразделений Общества при проведении работ по созданию, развитию и эксплуатации АС с соблюдением требований информационной безопасности;
* разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения информационной безопасности АС.

Политика не регламентирует вопросы организации охраны помещений и обеспечения сохранности и физической целостности компонентов АС, защиты от стихийных бедствий, сбоев в системе энергоснабжения, а также меры по обеспечению личной безопасности персонала и клиентов Общества. Однако она предполагает построение системы информационной безопасности на тех же концептуальных основах, что и система безопасности Общества в целом (имущественная, физическая и т.д.). Это позволяет не только принципиально, но и практически сопрягать их, оптимизируя затраты на построение такой системы.

При разработке Политики учитывались основные принципы создания комплексных систем обеспечения информационной безопасности, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам информационной безопасности, а также текущее состояние и перспективы развития информационных технологий.

**2.Список терминов и определений.**

***Автоматизированная система обработки информации (АС)*** – организационно- техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов: технических средств обработки и передачи данных (средств вычислительной техники и связи), методов и алгоритмов обработки в виде соответствующего программного обеспечения, массивов (наборов, баз) данных на различных носителях, персонала и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных с целью удовлетворения информационных потребностей государственных органов, общественных или коммерческих организаций (юридических лиц), отдельных граждан (физических лиц) и иных 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 автоматизированную систему*** – любое действие, выполняемое *нарушителем*, которое приводит к реализации *угрозы*, путем использования *уязвимостей АС.*

***Безопасность*** – состояние защищенности жизненно важных интересов личности, предприятия, общества и государства от внутренних и внешних угроз. Безопасность достигается проведением единой политики в области охраны и защиты важных ресурсов, системой мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства.

***Информационная безопасность*** – 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 компьютерной информации*** – достижение требуемого уровня защиты (класса и категории защищенности) объекта информатизации при обработке информации и её передаче через сети передачи данных (СПД), обеспечивающего сохранение таких ее качественных характеристик (свойств), как: секретность (конфиденциальность), целостность и доступность.

***Безопасность информационной технологии*** – защищенность технологического процесса переработки информации.

***Безопасность субъектов информационных отношений* –** защищенность субъектов информационных отношений от нанесения им материального, морального или иного ущерба путем воздействия на информацию и/или средства ее обработки и передачи.

***Безопасность АС (компьютерной системы)*** – защищенность АС от несанкционированного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, незаконной модификации или разрушения ее компонентов.

***Безопасность информационного ресурса (в частности АС)*** – складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности.

Конфиденциальность заключается в том, что ресурс доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия. Целостность, что ресурс может быть модифицирован только субъектом, имеющим для этого соответствующие права. Целостность является гарантией корректности (неизменности, работоспособности) ресурса в любой момент времени.

Доступность информационного ресурса означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к нему.

***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 (ОИ), приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ОИ.

***Вспомогательные технические средства и системы (ВТСС)*** защищаемого объекта информатизации – технические средства и системы, не предназначенные для передачи, обработки и хранения секретной информации, устанавливаемые совместно с *ОТСС* или в выделенных помещениях.

К ним относятся:

* различного рода телефонные аппараты и системы;
* средства вычислительной техники;
* системы передачи данных в системе радиосвязи;
* системы охранной и пожарной сигнализации;
* системы оповещения и сигнализации;
* контрольно-измерительная аппаратура;
* системы кондиционирования;
* системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, системы радиовещания; телевизоры и радиоприемники и т.д.);
* оргтехника;
* средства и системы электрочасофикации.

***Выделенное помещение (ВП)*** – 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.

***Документированная информация (документ)*** – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать, при этом, документирование информации является обязательным условием включения информации в информационные ресурсы.

***Жизненно важные интересы*** – совокупность потребностей, удовлетворение которых необходимо для надежного обеспечения существования и возможности прогрессивного развития субъекта (личности, организации, общества или государства).

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

***Защита информации (ЗИ)*** – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на информацию (ГОСТ Р 50922).

***Защита информации от несанкционированного доступа (НСД)*** – деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой̆ информации (ГОСТ Р 50922).

***Информация в АС*** – сведения о лицах, фактах, событиях, процессах и явлениях в некоторой предметной области, включенные в систему обработки информации, или являющиеся ее результатом в различных формах представления на различных носителях и используемые (необходимые) для оптимизации принимаемых решений в процессе управления объектами данной предметной области.

***Информативный сигнал*** – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта *секретная информация*, передаваемая, хранимая или обрабатываемая в *ОТСС* и обсуждаемая в *ВП*.

***Компьютерная информация*** – информация в виде:

* записей в памяти ЭВМ, 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);
* программно-информационного продукта, являющегося результатом генерации новой или обработки исходной документированной информации, представляемого непосредственно на экранах мониторов ОИ, 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 (КЗ)*** – это пространство, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

Границей КЗ могут являться:

* + периметр охраняемой территории предприятия (учреждения);
  + ограждающие конструкции охраняемого здания, охраняемой̆ части здания, выделенного помещения.

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

***Конфиденциальная информация*** – информация, содержащая сведения, составляющие врачебную, коммерческую, служебную тайну или персональные данные, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

***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.

***Лицензия в области защиты информации*** – разрешение на право проведения тех или иных работ в области защиты информации (в соответствии с Постановление Правительства РФ от 15.08.2006 No 504 «О лицензировании деятельности по технической защите конфиденциальной информации»).

***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 (чисто агентурные методы получения сведений, технические средства перехвата без модификации компонентов системы, штатные средства и недостатки систем защиты, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ и т.п.).

***Несанкционированное действие*** – действие *субъекта* в нарушение установленных в системе правил обработки информации.

***Несанкционированный доступ (НСД)*** – доступ *субъекта* к *объекту* в нарушение установленных в системе правил разграничения доступа.

***Обработка информации в АС*** – совокупность операций (сбор, накопление, хранение, преобразование, отображение, выдача и т.п.), осуществляемых над информацией (сведениями, данными) с использованием средств АС.

***Объект*** – пассивный компонент системы, единица ресурса автоматизированной системы (устройство, диск, каталог, файл и т.п.), доступ к которому регламентируется правилами разграничения доступа.

***Основные технические средства и системы (ОТСС)*** защищаемого объекта информатизации – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи *секретной информации*. К ним могут относиться средства и системы информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных), технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео-, смысловой и буквенно-цифровой информации), используемые для обработки секретной информации.

***Пароль*** – служебное слово, которое считается известным узкому кругу лиц (одному лицу) и используется для ограничения доступа к информации, в помещение, на территорию.

***Показатель эффективности защиты информации*** – мера или характеристика для оценки эффективности защиты информации (ГОСТ Р 50992).

***Правила разграничения доступа*** – совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе.

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

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

***Субъект 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.

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

***Естественные угрозы*** – это угрозы, вызванные воздействиями на АС и ее элементы объективных физических процессов техногенного характера или стихийных природных явлений, не зависящих от человека;

***Искусственные угрозы*** – это угрозы АС, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

* ***непреднамеренные (неумышленные, случайные) угрозы***, вызванные ошибками в проектировании АС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.;
* ***преднамеренные (умышленные) угрозы***, связанные с корыстными устремлениями людей (*злоумышленников*).

***Угроза автоматизированной системе*** – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба ресурсам АС.

***Угроза информационной безопасности*** – случайное (неумышленное) или преднамеренное (злоумышленное) воздействие, приводящее к нарушению целостности, доступности и конфиденциальности информации или поддерживающей ее инфраструктуры, которое наносит ущерб собственнику, распорядителю или пользователю информации.

***Угроза информационной безопасности*** – потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию.

***Угроза интересам субъектов информационных отношений*** – потенциально возможное событие, действие, процесс или явление, которое посредством воздействия на информацию и другие компоненты АС может привести к нанесению ущерба интересам данных субъектов.

***Уровень защиты (класс и категория защищенности) ОИ*** – характеристика, описываемая в нормативных документах определённой группой требований к данному классу и категории защищенности.

***Уязвимость автоматизированной системы*** – любая характеристика АС, 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.

***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).

***Информационные способы нарушения информационной безопасности –*** *включают:*

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

***Программно-математические способы нарушения информационной безопасности –*** *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.

***Физические способы нарушения информационной безопасности*** *– 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 информационной безопасности;
* диверсионные действия по отношению к объектам информационной безопасности (взрывы, поджоги, технические аварии и т.д.).

***Радиоэлектронные способы нарушения информационной безопасности*** *– 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.

***Организационно-правовые способы нарушения информационной безопасности*** *– включают:*

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

***Система защиты АС (информации)*** – 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 безопасности АС (циркулирующей в АС информации).

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

***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.

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

***Организационные (административные) 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.

***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 компонентам АС и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной̆ сигнализации.

***Технические (аппаратно-программные) средства защиты*** – различные электронные устройства и специальные программы, входящие в состав АС, 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.).

**3.Описание объекта защиты**

Объекты информационной безопасности – это компоненты информационной среды, угрозы которым представляют опасность для застрахованных, страхователей, работников, акционеров Общества и т.д. Основными объектами информационной безопасности в Обществе являются:

* информационные ресурсы с ограниченным доступом, составляющие коммерческую, врачебную, служебную тайну, персональные данные, иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, в том числе открытая (общедоступная) информация, представленные в виде документов и массивов информации, независимо от формы и вида их представления;
* процессы обработки информации в АС – информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков, администраторов и пользователей АС;
* информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные компоненты АС.

**4.Цели и задачи деятельности по обеспечению информационной безопасности.**

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений (интересы которых затрагиваются при создании и функционировании АС) от возможного нанесения им ощутимого материального, физического, морального или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования АС или несанкционированного доступа к циркулирующей в ней информации и её незаконного использования.

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

* доступности обрабатываемой информации для зарегистрированных пользователей (устойчивого функционирования АС, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время);
* сохранения в тайне (обеспечения конфиденциальности) определённой части информации, хранимой, обрабатываемой средствами вычислительной техники (СВТ) и передаваемой по каналам связи;
* целостности и достоверности информации, хранимой и обрабатываемой в АС и передаваемой по каналам связи.

Для достижения основной цели защиты и обеспечения указанных свойств информации и системы её обработки система безопасности АС должна обеспечивать эффективное решение следующих задач:

* защиту от вмешательства в процесс функционирования АС посторонних лиц (возможность использования автоматизированной системы и доступ к её ресурсам должны иметь только зарегистрированные установленным порядком пользователи – работники структурных подразделений Общества);
* разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам АС (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям АС для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:
* к информации, циркулирующей в АС;
* средствам вычислительной техники (СВТ) АС;
* аппаратным, программным и криптографическим средствам защиты, используемым в АС;
* регистрацию действий пользователей при использовании защищаемых ресурсов АС в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов ответственными за информационную безопасность;
* контроль целостности (обеспечение неизменности) среды исполнения программ и её восстановление в случае нарушения;
* защиту от несанкционированной модификации и контроль целостности используемых в АС программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;
* защиту информации ограниченного распространения от утечки по техническим каналам при её обработке, хранении и передаче по каналам связи;
* защиту информации ограниченного распространения, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;
* обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
* обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;
* своевременное выявление источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции;
* создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения информационной безопасности.

**5.Угрозы информационной безопасности.**

Наиболее опасными (значимыми) угрозами информационной безопасности АС (способами нанесения ущерба субъектам информационных отношений) являются:

* нарушение конфиденциальности (разглашение, утечка) сведений, составляющих коммерческую или врачебную тайну, а также персональных данных;
* нарушение работоспособности (дезорганизация работы) АС, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;
* нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов АС, а также фальсификация (подделка) документов.

***Основными источниками угроз информационной безопасности АС являются:***

* непреднамеренные (ошибочные, случайные, необдуманные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований информационной безопасности и другие действия работников (в том числе администраторов средств защиты) структурных подразделений Общества при эксплуатации АС, приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности отдельных рабочих станций (АРМ), подсистем или АС в целом;
* преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия работников подразделений Общества, допущенных к работе с АС, а также работников подразделений Общества, отвечающих за обслуживание, администрирование программного и аппаратного обеспечения, средств защиты и обеспечения информационной безопасности;
* воздействия из других логических и физических сегментов АС со стороны работников других подразделений Общества, в том числе программистов-разработчиков прикладных задач, а также удаленное несанкционированное вмешательство посторонних лиц из телекоммуникационных сетей Общества и внешних сетей общего назначения (Internet) через легальные и несанкционированные каналы подключения сети Общества к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к ресурсам АС;
* деятельность международных и отечественных преступных групп и формирований, политических и экономических структур, а также отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности системы в целом и её отдельных компонентов;
* ошибки, допущенные при проектировании АС и её системы защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации и контроля эффективности защиты) АС;
* аварии, стихийные бедствия и т.п.

**6. Модель нарушителя информационной безопасности**

НАРУШИТЕЛЬ — это лицо, которое предприняло попытку выполнения запрещенных операций (действий̆) 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.

Система защиты АС должна строиться исходя из предположений о следующих возможных типах нарушителей в системе (с учетом категории лиц, мотивации, квалификации, наличия специальных средств и др.):

*«Неопытный (невнимательный) пользователь»* — работник Общества (или другой организации, зарегистрированный как пользователь системы), который может предпринимать попытки выполнения запрещенных операций, доступа к защищаемым ресурсам АС с превышением своих полномочий, ввода некорректных данных и т.п. действия по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (доступные ему) аппаратные и программные средства.

*«Любитель»* — работник Общества (или другой организации, зарегистрированный как пользователь системы), пытающийся преодолеть систему защиты без корыстных целей и злого умысла, для самоутверждения или из «спортивного интереса». Для преодоления системы защиты и совершения запрещенных действий̆ он может использовать различные методы получения дополнительных полномочий доступа к ресурсам (имен, паролей и т.п. других пользователей), недостатки в построении системы защиты и доступные ему штатные (установленные на рабочей станции) программы (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств). Помимо этого он может пытаться использовать дополнительно нештатные инструментальные и технологические программные средства (отладчики, служебные утилиты), самостоятельно разработанные программы или стандартные дополнительные технические средства.

*«Мошенник»* — работник Общества (или другой организации, зарегистрированный как пользователь системы), который̆ может предпринимать попытки выполнения незаконных технологических операций, ввода подложных данных и тому подобные действия в корыстных целях, по принуждению или из злого умысла, но использующий при этом только штатные (установленные на рабочей станции и доступные ему) аппаратные и программные средства от своего имени или от имени другого работника (зная его имя и пароль, используя его кратковременное отсутствие на рабочем месте и т.п.).

*«Внутренний злоумышленник»* — работник Общества, зарегистрированный как пользователь системы, действующий целенаправленно из корыстных интересов или мести за нанесенную обиду, возможно, в сговоре с лицами, не являющимися работниками Общества. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы получения реквизитов доступа, пассивные средства (технические средства перехвата без модификации компонентов системы), 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 – из сетей общего пользования.

*Внутренним нарушителем* может быть лицо из следующих категорий персонала Общества:

* зарегистрированные конечные пользователи АС (работники Общества);
* работники, не допущенные к работе с АС;
* персонал, обслуживающий технические средства АС (инженеры, техники);
* работники подразделений разработки и сопровождения ПО (прикладные и системные программисты);
* технический персонал, обслуживающий здания (уборщицы, электрики, сантехники и другие работники, имеющие доступ в здания и помещения, где расположены компоненты АС);
* работники и подразделения информационной безопасности;
* руководители различных уровней.

*«Внешний нарушитель (злоумышленник)»* — постороннее лицо или работник Общества (или другой организации, зарегистрированный как пользователь системы), действующий целенаправленно из корыстных интересов, из мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор радиоэлектронных способов нарушения информационной безопасности, методов и средств взлома систем защиты, характерных для сетей общего пользования (в особенности сетей на основе IP-протокола), включая удаленное внедрение программных закладок и использование специальных инструментальных и технологических программ, используя имеющиеся слабости протоколов обмена и системы защиты узлов сети АС.

Категории лиц, которые могут быть *внешними нарушителями*:

* уволенные работники Общества;
* представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т.п.);
* посетители (приглашенные представители организаций, граждане), представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.;
* члены преступных организаций, работники спецслужб или лица, действующие по их заданию;
* лица, случайно или умышленно проникшие в сети АС из внешних (по отношению к Обществу) сетей телекоммуникации («хакеры»).

Пользователи и обслуживающий персонал из числа работников Общества имеют наиболее широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определенных полномочий по доступу к ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связано с нарушением действующих правил и инструкций. Особую опасность эта группа нарушителей представляет при взаимодействии с криминальными структурами или спецслужбами.

Уволенные работники могут использовать для достижения целей свои знания о технологии работы, защитных мерах и правах доступа. Полученные в Обществе знания и опыт выделяют их среди других источников внешних угроз.

Криминальные структуры представляют наиболее агрессивный источник внешних угроз. Для осуществления своих замыслов эти структуры могут идти на открытое нарушение закона и вовлекать в свою деятельность работников Общества всеми доступными им силами и средствами.

Профессиональные «хакеры» имеют наиболее высокую техническую квалификацию и знания об уязвимостях программных средств, используемых в АС. Наибольшую угрозу представляют при взаимодействии с работающими и уволенными работниками Общества и криминальными структурами.

Организации, занимающиеся разработкой, поставкой и ремонтом оборудования, информационных систем, представляют внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к информационным ресурсам. Криминальные структуры и спецслужбы могут использовать эти организации для временного устройства на работу своих членов, с целью доступа к защищаемой информации в АС.

Принимаются следующие ограничения и предположения о характере действий возможных нарушителей:

* работа по подбору персонала и специальные мероприятия исключают возможность создания сообществ нарушителей, т.е. объединения (сговора) и целенаправленных действий двух и более нарушителей – работников Общества по преодолению системы защиты;
* нарушитель скрывает свои несанкционированные действия от других работников Общества;
* несанкционированные действия могут быть следствием ошибок пользователей, администраторов безопасности, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;
* в своей противоправной 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.

**7. Основные положения технической политики в области обеспечения информационной безопасности АС**

Реализация технической политики в области обеспечения информационной безопасности 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 взаимное 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 политики обеспечения информационной безопасности АС являются:

* обеспечение защиты информационных ресурсов от хищения, утраты, утечки, уничтожения, искажения или подделки за счет несанкционированного доступа и специальных воздействий (от НСД);
* обеспечение защиты информации от утечки по техническим каналам при её обработке, хранении и при передаче по каналам связи.

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

В рамках указанных направлений технической политики обеспечения информационной безопасности осуществляются:

* реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к работам, документам и информации конфиденциального характера;
* 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 исполнителей и посторонних лиц в здания и помещения, где проводятся работы конфиденциального характера и размещены средства информатизации и коммуникации, на которых обрабатывается (хранится, передается) информация конфиденциального характера, непосредственно к самим средствам информатизации и коммуникациям;
* разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации в подсистемах различного уровня и назначения, входящих в АС;
* учет документов, информационных массивов, регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступы и действий пользователей, обслуживающего персонала и посторонних лиц;
* предотвращение внедрения в автоматизированные подсистемы программ-вирусов, программных закладок и т.п.
* криптографическое преобразование информации, обрабатываемой и передаваемо средствами вычислительной техники и связи;
* надежное хранение традиционных 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;
* снижение уровня и информативности побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых различными элементами автоматизированных подсистем;
* обеспечение акустической защиты помещений, в которых обсуждается информация конфиденциального характера;
* электрическая развязка цепей питания, заземления и других цепей объектов информатизации, выходящих за пределы контролируемой зоны;
* активное зашумление в различных диапазонах;
* противодействие оптическим и лазерным средствам наблюдения.

**8.Ответственность и контроль соблюдения Политики.**

Контроль может проводиться как выделенными работниками ИТ-подразделений (оперативный контроль в процессе информационного взаимодействия в АС), так и привлекаемыми для этой цели компетентными 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.

Контроль может осуществляться как с помощью штатных средств системы защиты информации от НСД, так и с помощью специальных программных средств контроля.