|  |  |
| --- | --- |
|  | |
| МИНОБРНАУКИ РОССИИ | |
| Федеральное государственное бюджетное образовательное учреждение  высшего профессионального образования  **"Российский технологический университет"**  **МИРЭА** | |
| Институт «Комплексной безопасности и специального приборостроения» | |
| Кафедра «Управление и моделирование систем» (КБ-2) | |

|  |  |
| --- | --- |
| **ОТЧЕТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ** | |
| **по дисциплине** | |
| **«Основы информационной безопасности»** | |
|  | |
| Выполнил студент группы БИСО-01-19 | Доронина Анастасия Алексеевна |
|  |  |

|  |  |  |
| --- | --- | --- |
| Лабораторные работы выполнены | «\_\_»\_\_\_\_\_\_\_2020г. |  |
|  |  |  |
| «Зачтено» | «\_\_»\_\_\_\_\_\_\_2020г. |  |

Москва 2020

Оглавление

[**1.** **Общие положения** 3](#_Toc56000459)

[**2.** **Список терминов и определений** 4](#_Toc56000460)

[**3.** **Описание объекта защиты** 9](#_Toc56000461)

[**4.** **Цели и задачи деятельности по обеспечению информационной безопасности** 9](#_Toc56000462)

[**5.** **Угрозы информационной безопасности** 10](#_Toc56000463)

[**6.** **Модель нарушителя информационной безопасности** 11](#_Toc56000464)

[**7.** **Основные положения технической политики в области обеспечения информационной безопасности АС** 12](#_Toc56000465)

[**8.** **Контроль за соблюдением положений Политики** 13](#_Toc56000466)

[**9.** **Заключительные положения** 13](#_Toc56000467)

## **Общие положения**

Настоящая «Политика информационной безопасности» ООО «Солнышко» (далее – Общество) представляет собой официально принятую систему взглядов на проблему обеспечения информационной безопасности в автоматизированных системах. Политика содержит в себе структурированное изложение целей и задач защиты, способы достижения требуемого уровня информационной безопасности, технологических и организационных аспектов обеспечения информационной безопасности в АС.

Политика учитывает современное состояние и перспективы развития АС, цели и задачи, правовые основы её создания и эксплуатации, а также анализа угроз безопасности.

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 основой для:

* Формирования и проведения единой политике в основе информационной безопасности в АС;
* 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;
* Разработки стратегии информационной безопасности Общества, включая цели, задачи и комплекс мер по её практической реализации;

Требования настоящей Политики распространяются на всех сотрудников Фирмы (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

## **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.

***Вредоносные программы*** – программы или измененные программы объекта информатизации (ОИ), приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ОИ.

***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.

***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.

***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.

***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 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.

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

***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.).

## **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;
* Сотрудники Общества, являющиеся разработчиками и пользователями информационных систем Общества;
* 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;

## **Цели и задачи деятельности по обеспечению информационной безопасности**

Целью деятельности по обеспечению информационной безопасности Общества является снижение угроз информационной безопасности до приемлемого для Общества уровня.

Субъектами правоотношений при использовании АС и обеспечении информационной безопасности являются:

* Должностные лица и работники Общества и его подразделений, как пользователи АС и поставщики информации в неё в соответствии с их должностными обязанностями;
* Юридические и физические лица, информация о которых накапливается, хранится и обрабатывается в АС;
* Другие физические и юридические лица, задействованные в процессе создания и регулировки работы АС;
* ИТ подразделения общества, обеспечивающие эксплуатацию систем обработки информации;

Основные задачи деятельности по обеспечению информационной безопасности Общества:

* Выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты;
* Регистрация действий пользователя при использовании ресурсов АС и периодический контроль корректности действий пользователя системы;
* Запись всех исходящих и входящих звонков с телефона организации Общества;
* Обеспечение идентификации всех пользователей, участвующих в обмене информации (подтверждение подлинности отправителя и получателя);
* Выявление источников угроз информационной безопасности, способствующих нанесению любого ущерба Общества;

# **Угрозы информационной безопасности**

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.

# **Модель нарушителя информационной безопасности**

Нарушитель – лицо, которое предприняло попытку выполнения запрещенных операций по ошибке, незнанию или осознанно со злым умыслом или без такового и использующее для этого различные возможности, методы и средства.

По отношению к Обществу нарушители могут быть разделены на внешних и внутренних нарушителей.

*Внутренний нарушитель»* — 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 сеть АС из внешних (по отношению к Обществу) сетей телекоммуникации («хакеры»).

Принимаются следующие ограничения и предположения о характере действий возможных нарушителей:

* работа по подбору персонала и специальные мероприятия исключают возможность создания сообществ нарушителей.
* 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.

# **Основные положения технической политики в области обеспечения информационной безопасности АС**

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;
* 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;

# **Контроль за соблюдением положений 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.

Текущий контроль соблюдения настоящей Политики осуществляет штаб Руководства. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов информационной безопасности Общества, по результатам оценки информационной безопасности.

# **Заключительные положения**

* Невыполнение сотрудниками Общества требований по обеспечению ИБ приравнивается к невыполнению должностных обязанностей и приводит, как минимум, к дисциплинарной ответственности;
* Изменение настоящей Политики предусмотрено не реже одного раза за два календарных года;
* Изменения в настоящей Политике в праве вносить только назначенный член руководства;
* Политика в праве быть признанной недействующей только в случае принятия соответствующего решения главы отдела Безопасности вместе с главой руководства;