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

Кафедра КБ-3 «Управление и моделирование систем»

**Отчет**

по выполнению лабораторной работы № 1

«Формирование политики безопасности на предприятии»

по дисциплине «Основы Информационной Безопасности»

Выполнил:

Студент 2 курса

Группа БИСО-02-19

Шифр 19Б1160

Страхов Алексей Леонидович

Проверил:

Изергин Д.А.

Москва, 2020

УТВЕРЖДЕНО

Приказом директора(ФИО)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

№\_\_ от «\_\_»\_\_\_\_\_20\_\_

ООО «Камчатская мечта»

**Политика информационной безопасности ООО "Камчатская мечта".**

Настоящий документ не может быть полностью или частично воспроизведен, тиражирован и распространен без согласования с ООО «Камчатская мечта»

2020

ИНФОРМАЦИОННЫЕ ДАННЫЕ

ВВЕДЕНО В ДЕЙСТВИЕ ПРИКАЗОМ № \_\_ от 9 октября 2020 г.

РАЗРАБОТАНО: Отдел защиты информации

ИСПОЛНИТЕЛИ:

Начальник отдела защиты информации Страхов А.Л. \_\_\_\_\_\_\_\_

СОГЛАСОВАНО:

Директор департамента ИТ Вдовин А.С. \_\_\_\_\_\_\_\_

Начальник юридической службы Косова Ю.А. \_\_\_\_\_\_\_\_

Директор финансового департамента Спирин А.С. \_\_\_\_\_\_\_\_

**СОДЕРЖАНИЕ**

[1. ОБЩИЕ ПОЛОЖЕНИЯ 4](#_Toc477876072)

[2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 5](#_Toc477876073)

[3. СПИСОК ИСПОЛЬЗОВАНЫХ СОКРАЩЕНИЙ 10](#_Toc477876074)

[4. ЦЕЛИ ПОЛИТИКИ 11](#_Toc477876075)

[5. ПРИНЦИПЫ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 12](#_Toc477876076)

[6. ОБЛАСТЬ ПРИМЕНЕНИЯ 15](#_Toc477876077)

[7. ОСНОВНЫЕ ЗАДАЧИ 16](#_Toc477876078)

[8. УГРОЗЫ И ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 18](#_Toc477876079)

[9. УПРАВЛЕНИЕ УГРОЗАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 20](#_Toc477876080)

[10. ОТВЕТСТВЕННОСТЬ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 22](#_Toc477876083)

[11. НОРМАТИВНЫЕ ССЫЛКИ 23](#_Toc477876084)

# ОБЩИЕ ПОЛОЖЕНИЯ

* 1. Политика информационной безопасности (далее – Политика) ООО «Русаков и компания» (далее – Общества), представляет собой совокупность управленческих решений, лежащих в основе организационно-распорядительных документов, регламентирующих правила и нормы информационной безопасности.
  2. Настоящая Политика представляет собой официально принятую руководством Общества систему взглядов на проблему обеспечения информационной безопасности, определяет основные направления деятельности руководящего состава Общества по устранению потенциальных угроз информационной безопасности в процессе деятельности Общества, содержит цели, задачи и принципы достижения требуемого уровня безопасности информации, определяет виды угроз безопасности информации и информационные ресурсы, подлежащие защите.
  3. Политика является внутренним документом верхнего уровня в системе организационно-нормативного обеспечения защиты информации в ИС Общества. Организационно-нормативные документы нижнего уровня создаются в развитие Политики, определяя и уточняя процедуры и порядки, направленные на реализацию положений Политики.
  4. Основу политики информационной безопасности составляет:
* соответствие процессов сбора, накопления, обработки, предоставления и распространения информации требованиям ратифицированного в Российской Федерации международного законодательства, законодательства Российской Федерации, требованиям и нормативным документам регуляторов, а также собственным приоритетам в вопросах защиты коммерческой тайны;
* централизованная разработка документов Общества, регламентирующих вопросы информационной безопасности, обязательность выполнения их требований;
* единство технической политики Общества в области реализации технических, программных и программно-технических мер по защите информационных ресурсов и технологий;
* персональная ответственность за нарушения в сфере информационной безопасности;
* обеспечение постоянного контроля состояния информационной безопасности в Общества.

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

* 1. **Администратор безопасности** – функциональная роль в информационной системе, отвечающая за информационную безопасность в этой системе и имеющая право назначать иные роли и распределять права доступа.
  2. **Безопасность информации** - состояние защищённости информации, обрабатываемой средствами вычислительной техники или автоматизированной системы от внутренних или внешних угроз.
  3. **Государственная тайна** - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной, оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности государства.
  4. **Доступ к информации** - возможность получения информации и её использования.
  5. **Защита информации** - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
  6. **Защищаемая информация** - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.
  7. **Информационная безопасность** – в рамках данного документа под информационной безопасностью понимается непрерывный во времени процесс обеспечения конфиденциальности (кроме информации, конфиденциальность которой не определена ни на государственном уровне, ни на локальном), целостности и доступности защищаемой информации.
  8. **Информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств.
  9. **Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
  10. **Информационный процесс** - процесс получения, создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации.
  11. **Информация** - сведения (сообщения, данные) независимо от формы их представления.
  12. **Инцидент информационной безопасности (Инцидент ИБ)** - единичное, нежелательное или неожиданное событие информационной безопасности (или совокупность таких событий), которое может скомпрометировать бизнес-процессы Общества или угрожает ее информационной безопасности.
  13. **Коммерческая тайна** - научно-техническая, технологическая, производственная, финансово-экономическая или иная информация, в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введён режим коммерческой тайны.
  14. **Контролируемая зона -** это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных средств.
  15. **Конфиденциальная информация** - информация с ограниченным доступом, за исключением сведений, отнесённых к государственной тайне и персональным данным, содержащейся в информационных системах Общества, накопленная за счёт Общества и являющейся собственностью Общества (к ней может быть отнесена информация, составляющая служебную тайну и другие виды тайн в соответствии с законодательством Российской Федерации, а также сведения конфиденциального характера в соответствии с «Перечнем сведений конфиденциального характера», утверждённого Указом Президента Российской Федерации от 06.03.1997 №188), защита которой осуществляется в интересах Общества.
  16. **Конфиденциальность персональных данных** - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.
  17. **Модель угроз** (безопасности информации) - физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.
  18. **Мультисервисная сеть** предприятия - универсальная многоцелевая среда, предназначенная для передачи речи, изображения и данных с использованием технологии коммутации пакетов.
  19. **Несанкционированный доступ к информации –** доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами информационных систем.
  20. **Носитель защищаемой информации** – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит своё отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.
  21. **Обработка персональных данных** – любое действие (операция) или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (в том числе распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
  22. **Оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.
  23. **Персональные данные** - любая информация, относящаяся прямо или косвенно к определённому или определяемому физическому лицу (субъекту персональных данных).
  24. **Подсистема информационной безопасности** – структурная часть общей системы информационной безопасности Общества. Подсистема информационной безопасности служит для реализации технических защитных мер в отношении: отдельной информационной системы; сети передачи данных или её сегмента; автоматизированного рабочего места; конкретной категории защищаемой информации.
  25. **Режим коммерческой тайны** - режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.
  26. **Сертификация на соответствие требованиям по безопасности информации** - форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки[[1]](#footnote-1) требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров.
  27. **Средство защиты информации** - техническое и(или) программное средство предназначенное или используемое для защиты информации.
  28. **Система обеспечения информационной безопасности** - функционирующая как единое целое совокупность средств и мероприятий, и применяемых при проведении мероприятий мер, устремлённая на ликвидацию внутренних и внешних угроз жизненно важным интересам субъекта безопасности, создание, поддержание и развитие состояния защищённости его информационной среды.
  29. уточнение (обновление, изменение), извлечение, использование, передачу (в том числе распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
  30. **Оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.
  31. **Персональные данные** - любая информация, относящаяся прямо или косвенно к определённому или определяемому физическому лицу (субъекту персональных данных).
  32. **Подсистема информационной безопасности** – структурная часть общей системы информационной безопасности Общества. Подсистема информационной безопасности служит для реализации технических защитных мер в отношении: отдельной информационной системы; сети передачи данных или её сегмента; автоматизированного рабочего места; конкретной категории защищаемой информации.
  33. **Режим коммерческой тайны** - режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.
  34. **Сертификация на соответствие требованиям по безопасности информации** - форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки[[2]](#footnote-2) требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров.
  35. **Средство защиты информации** - техническое и(или) программное средство предназначенное или используемое для защиты информации.
  36. **Система обеспечения информационной безопасности** - функционирующая как единое целое совокупность средств и мероприятий, и применяемых при проведении мероприятий мер, устремлённая на ликвидацию внутренних и внешних угроз жизненно важным интересам субъекта безопасности, создание, поддержание и развитие состояния защищённости его информационной среды.

# СПИСОК ИСПОЛЬЗОВАНЫХ СОКРАЩЕНИЙ

* 1. **АРМ** – автоматизированное рабочее место.
  2. **ИС** – информационная система.
  3. **ИСПДн** – информационная система, содержащая персональные данные.
  4. **КЗ** – контролируемая зона.
  5. **КТ** – коммерческая тайна; информация, составляющая коммерческую тайну.
  6. **МСС** – мультисервисная сеть.
  7. **ОЗИ** – отдел защиты информации.
  8. **ОС** – операционная система.
  9. **НСД –** несанкционированный доступ к информации.
  10. **ПДн** – персональные данные.
  11. **ПИБ** – подсистема информационной безопасности.
  12. **ПО** – программное обеспечение.
  13. **Пользователи ИС** – сотрудники Общества, использующие в процессе выполнения своих должностных обязанностей те или иные информационные системы Общества.
  14. **СВТ** – средство вычислительной техники.
  15. **СОИБ** – система обеспечения информационной безопасности.
  16. **СКЗИ**– средство криптографической защиты информации.
  17. **СТР-К -** Специальные требования и рекомендации по технической защите конфиденциальной информации одобренные решением коллегии Гостехкомиссии России от 02.03.2001 г.
  18. **ТЗ** – техническое задание.
  19. **ФСБ России** – Федеральная служба безопасности Российской Федерации.
  20. **ФСТЭК России** – Федеральная служба по техническому и экспортному контролю Российской Федерации.

# ЦЕЛИ ПОЛИТИКИ

* 1. Политика представляет собой систематизированное изложение целей и задач защиты, основных принципов построения системы информационной безопасности, требований к организационным и техническим мерам защиты информации в информационных системах Общества.
  2. Целями разработки и применения Политики являются:
     + защита интересов Общества от актуальных угроз информационной безопасности путем их исключения или минимизации;
     + определение стратегии построения, реализации и дальнейшего развития системы информационной безопасности ИС Общества;
     + формирование требований по защите ИС Общества, единых для всех подразделений Общества;
     + выполнение требований действующего законодательства, подзаконных актов, требований профильных регуляторов в сфере информационной безопасности;
     + применение лучших мировых практик в области защиты информации и обеспечения непрерывности критичных технологических процессов.

# ПРИНЦИПЫ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

При достижении поставленных целей Общество намерено руководствоваться следующими принципами:

* 1. **Законность.** Предполагает осуществление защитных мероприятий и разработку системы безопасности информации в Обществе в соответствии с действующим законодательством в области информации, информатизации и защиты информации и других нормативных актов по безопасности, утверждённых органами государственной власти, в пределах их компетенции с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией.
  2. **Системность.** Системный подход к защите информации в Обществе предполагает учёт всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения информационной безопасности в Обществе. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей, пути проникновения в распределённые системы и НСД к информации. Система защиты должна строиться с учётом не только всех известных каналов проникновения и НСД к информации, но и с учётом возможности появления принципиально новых путей реализации угроз безопасности.
  3. **Комплексность.** Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) векторы угроз информационной безопасности и не содержащей слабых мест на стыках отдельных её компонентов. Защита должна строиться эшелонировано. Внешняя защита ИС должна обеспечиваться физическими средствами, организационными, технологическими и правовыми мерами. Одним из наиболее укреплённых рубежей призваны быть средства защиты, реализованные на уровне операционных систем СВТ в силу того, что ОС - это та часть компьютерной системы, которая управляет использованием всех её ресурсов. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.
  4. **Непрерывность защиты.** Защита информации - непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС Общества, начиная с самых ранних стадий проектирования, а не только на этапе её эксплуатации. Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имён, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления её функционирования.
  5. **Своевременность.** Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите ИС Общества и реализацию мер обеспечения безопасности информации на ранних стадиях разработки ИС в целом и её системы информационной безопасности, в частности. Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счёте, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищённые системы.
  6. **Преемственность и совершенствование.** Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, анализа функционирования информационных систем и их систем информационной безопасности с учётом изменений в методах и средствах перехвата информации и воздействия на компоненты ИС, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.
  7. **Разумная достаточность** (экономическая целесообразность, сопоставимость возможного ущерба и затрат). Предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов, 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 ИС Общества, в которых эта информация циркулирует. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).
  8. **Персональная ответственность.** Предполагает возложение ответственности за обеспечение безопасности информации и системы её 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 чётко известен или сведён к минимуму.

**Минимизация полномочий.** Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью.

.

* 1. **Открытость алгоритмов и механизмов защиты.** Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счёт секретности структурной организации и алгоритмов функционирования её подсистем. Знание алгоритмов работы системы защиты не должно давать возможности её преодоления (даже авторам). Это, однако, не означает, что информация о конкретной системе защиты должна быть общедоступна.
  2. **Специализация и профессионализм.** Предполагает привлечение к разработке средств и реализации мер защиты информации сотрудников, имеющих соответствующее образование и опыт. Реализация административных мер и эксплуатация средств защиты также должна осуществляться профессионально подготовленными сотрудниками (специалистами подразделений, отвечающих за безопасности информации).
  3. **Обязательность контроля.** Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и средств защиты информации. 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.

**Вовлеченность руководства**. Вовлеченность руководства Общества в процесс обеспечения информационной безопасности. Деятельность по обеспечению информационной безопасности инициирована и контролируется руководством Общества. Руководство Общества выполняет те же правила по обеспечению информационной безопасности, что и все работники Общества.

# ОБЛАСТЬ ПРИМЕНЕНИЯ

* 1. Положения Политики распространяются на всех работников Общества, имеющих доступ к информационным активам и ИТ-инфраструктуре Общества, а также учитываются в отношениях с контрагентами (потребителями продукции, поставщиками, партнерами, консультантами, стажерами, практикантами и т.д.).
  2. В общем случае предметом настоящей Политики являются информация или носитель защищаемой информации, или информационный процесс, которые необходимо защищать в соответствии с целями Политики. Причём основным объектом защиты является именно информация, необходимость защиты носителей информации и информационных процессов вытекает из необходимости защиты информации.
  3. Информацию, обрабатываемую в обществе, следует относить к одной из следующих категорий:
     + персональные данные;
     + коммерческая тайна;
     + иная информация, не отнесенная к предыдущим категориям.
  4. Исходя из целей Политики к объектам защиты следует относить:
     + средства и системы информатизации, используемые для обработки защищаемой информации;
     + технические средства и системы, не обрабатывающие непосредственно защищаемую информацию, но размещённые в помещениях, где она обрабатывается (циркулирует);
     + любые носители информации, в том числе не относящиеся к системам автоматизированной обработки информации;
     + защищаемые помещения.

# ОСНОВНЫЕ ЗАДАЧИ

* 1. Основными задачами Политики являются:
     + определение единых для всех ИС Общества подходов к обеспечению информационной безопасности, обеспечивающих необходимый уровень защиты информационных ресурсов;
     + обеспечение выполнения в Обществе требований законодательства Российской Федерации по защите информации;
     + защита собственной конфиденциальной информации Общества;
     + создание основы для проведения единой технической политики в области применения информационных технологий, создания единой СОИБ в Обществе.
  2. Для достижения целей Политики и обеспечения безопасности информации СОИБ Общества должно быть обеспечено 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 ИС и подразделений Общества;
     + управление инцидентами информационной безопасности;
     + повышение уровня осведомленности сотрудников Общества в области информационной безопасности;
     + 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 информационных систем Общества посторонних лиц (доступ к защищаемым ИС Общества должны иметь только зарегистрированные в установленном порядке пользователи);
     + разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Общества (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей);
     + обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
     + защиту от несанкционированной модификации, используемых в информационных системах Общества программных средств, а также защита информационных систем от внедрения несанкционированных программ, включая компьютерные вирусы;
     + защиту информации ограниченного доступа от утечки по любым возможным каналам при её обработке, хранении и передаче по каналам связи;
     + обеспечение жизненного цикла СКЗИ в соответствии с требованиями законодателя и регуляторов;
     + обеспечение возобновления работы защищаемых ИС Общества в случае возникновения инцидента ИБ;
     + система информационной безопасности Общества должна полностью соответствовать требованиям действующего законодательства в вопросах защиты КТ, ПДн, а также требованиям профильных нормативно-правовых и методических документов регуляторов;
     + система информационной безопасности Общества должна использовать передовые мировые практики в вопросах разработки, внедрения и управления систем информационной безопасности, не нарушая при этом требования предыдущего подпункта.
  3. Действенность системы обеспечения информационной безопасности Общества должна достигаться установлением порядка, правил и зон ответственности в сфере защиты информации, которые должны определять цели и содержание деятельности Общества по обеспечению процессов управления информационной безопасностью.
  4. В Обществе для достижения поставленных целей и эффективного выполнения задач по обеспечению информационной безопасности определяется совокупность индивидуальных правил, устанавливающих допустимое взаимодействие между работником и объектами информатизации.
  5. Правила должны быть персонифицированы для каждого работника в виде обязанностей с установлением ответственности за их исполнение. Ответственность за их надлежащее исполнение для каждого работника должна быть закреплена в должностной инструкции.
  6. Исполнение обязанностей по информационной безопасности работников Общества должно быть обеспечено необходимыми ресурсами.
  7. Не должно допускаться совмещение обязанностей работника, включающих функции сопровождения, исполнения, администрирования и обязанностей, включающих функции контроля.

# УГРОЗЫ И ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

* 1. Угроза информационной безопасности — совокупность условий и факторов, создающих опасность нарушения информационной безопасности.
  2. Угрозы информационной безопасности Общества подлежат классификации по следующим признакам:
* По аспекту информационной безопасности, на который направлены угрозы:
* Угрозы конфиденциальности (неправомерный доступ к информации).
* Угрозы целостности (неправомочное изменение данных).
* Угрозы доступности (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы).
* По степени преднамеренности действий:
* Случайные (неумышленные действия, например, сбои в работе систем, стихийные бедствия).
* Преднамеренные (умышленные действия, например, шпионаж и диверсии).
* По расположению источника угроз:
* Внутренние (источники угроз располагаются внутри системы).
* Внешние (источники угроз находятся вне системы).
* По размерам наносимого ущерба:
* Общие (нанесение ущерба объекту безопасности в целом, причинение значительного ущерба).
* Локальные (причинение вреда отдельным частям объекта безопасности).
* Частные (причинение вреда отдельным свойствам элементов объекта безопасности).
* По степени воздействия на информационную систему:
* Пассивные (структура и содержание системы не изменяются).
* Активные (структура и содержание системы подвергается изменениям).
  1. Объектами угроз информационной безопасности общества являются все виды информации, указанные в п.п. 6.3
  2. При определении угроз необходимо руководствоваться:
     + для коммерческой тайны – требованиями, указанными в п.п. 11.20, 11.29 Политики;
     + для персональных данных – методикой, указанной в п.п. 11.19 Политики;
     + для иной, подлежащей защите информации, защита которой не является обязательной с точки зрения законодателя и регуляторов – перечень актуальных угроз определяется экспертным методом, допустимом применение наиболее подходящих из существующих руководящих документов (например, те, которые определены для коммерческой тайны).
  3. Перечень нормативных ссылок, указанный в п.п. 8.4, не является исчерпывающим. При проведении работ по моделированию угроз безопасности информации необходимо применять наиболее актуальные на момент выполнения работ руководящие документы.

# УПРАВЛЕНИЕ УГРОЗАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

# Направления обеспечения информационной безопасности в информационных системах

* + 1. Информационная безопасность информационных систем обеспечивается на всех стадиях их жизненного цикла с учетом степени участия в этом процессе субъектов отношений в информационной сфере (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и иных организаций).
       1. В процессе создания информационных систем обеспечивается:
* обоснованная формулировка требований к обеспечению информационной безопасности создаваемых информационных систем в соответствии с действующей нормативной базой и значимостью защищаемой информации, а также их полноценная реализация;
* выбор оптимальных проектных решений;
* выбор адекватной модели жизненного цикла;
* разработка необходимой эксплуатационной документации и организационно-распорядительных документов, регламентирующих порядок работы с защищаемой информацией;
* приемка в эксплуатацию (при необходимости, с проведением в установленном;
* оценка соответствия выбранных мер защиты информации установленным требованиям ИБ;
* предотвращение внесения недокументированных возможностей в программное обеспечение и оборудование.
  + - 1. При эксплуатации информационных систем в первую очередь обеспечивается их защита от следующих факторов:
* несанкционированного доступа к информации, ее модификации или уничтожения;
* неумышленной модификации или уничтожения информации;
* недоставки или ошибочной доставки информации;
* отказа в обслуживании или ухудшения обслуживания;
* отказа от авторства.

В процессе эксплуатации недопустимо внесение изменений в автоматизированные системы и вычислительные сети, приводящих к нарушению их функциональности или появлению недокументированных возможностей.

* + - 1. На стадии вывода из эксплуатации информационных систем (отдельных элементов) обеспечивается удаление из запоминающих устройств информации, несанкционированное использование которой может нанести ущерб коммерческой деятельности Общества.
      2. Требования по информационной безопасности включаются в договоры и контракты на проведение работ или оказание услуг, заключаемые на всех стадиях жизненного цикла информационных систем, а также в соответствующую проектную документацию.
      3. Разработка и создание в Обществе информационных систем, в которых обрабатывается информация, доступ к которой ограничен федеральными законами, осуществляется в соответствии с требованиями нормативных актов и методических документов (ФСБ России и ФСТЭК России, регламентирующих создание автоматизированных систем в защищенном исполнении
    1. При создании систем и средств защиты информационных систем технические задания и требования, предъявляемые к ним, согласовываются с ответственным за защиту информации в Обществе.
    2. Проектирование, ввод в эксплуатацию, эксплуатация и вывод из эксплуатации информационных систем в части вопросов информационной безопасности осуществляются при участии ответственного за защиту информации в Обществе.
    3. Информационная безопасность реализуется с помощью средств защиты и управления защитой, средств контроля и регистрации, средств обеспечения безотказной работы и восстановления информационных систем.

# Меры по обеспечению информационной безопасности в информационных системах

* + 1. В общем случае реализация требований настоящей Политики состоит из следующих шагов:
    - разработка внутренних организационно распорядительных документов, регламентирующих обработку защищаемой информации;
    - реализация организационных мер защиты информации;
    - оценка состояния защищенности ИС, разработка ТЗ на ПИБ;
    - реализация технических мер защиты информации с последующей оценкой их эффективности;
    - систематическая работа по уточнению набора мер и оценки эффективности как отдельных ПИБ, так и всей системы ИБ в целом.
    1. **Реализация организационных мер защиты информации**
       1. Организационная основа системы обеспечения информационной безопасности должна решать следующие основные задачи:
    - формирование и совершенствование элементов системы обеспечения информационной безопасности;
    - обеспечение соответствия организации защиты информации установленным требованиям;
    - реализация единой технической политики безопасности информации при организации работы Общества;
    - мониторинг внутренних и внешних условий функционирования объектов защиты, анализ эффективности управления защитой информации и подготовка решений по корректировке состава и содержания структурных элементов системы информационной безопасности.
      1. Основными участниками организационной основы системы обеспечения информационной безопасности Общества являются:
    - генеральный директор Общества;
    - начальник отдела защиты информации;
    - начальник юридического отдела;
    - начальник отдела информационных технологий.
    1. **Разработка внутренних организационно-распорядительных документов.**
       1. Для обеспечения деятельности по защите информации в Обществе должны быть разработаны следующие документы (список не является исчерпывающим):
    - положение об ответственном за защиту информации в Обществе;
    - стандарты предприятия по информационной безопасности для каждой категории защищаемой информации;
    - документы, устанавливающие режим КТ;
    - документы, регламентирующие порядок обработки ПДн;
    - модели угроз;
    - частные ТЗ на ПИБ для каждой ИС, не зависимо от вида обрабатываемой в ней информации.
      1. Для разработки внутренних кументов, регламентирующих защиту информации ограниченного доступа (в том числе ПДн) в Общества, допускается привлечение сторонней экспертной организации, имеющей соответствующие лицензии.
    1. Технические меры по защите информации

Для повышения эффективности защитных мероприятий наряду с организационными мерами предусматриваются технические меры по защите информации, разрабатываемые по результатам обследования информационных систем и оценки возможностей реализации замысла защиты на основе применения организационных мер, активизации

# НОРМАТИВНЫЕ ССЫЛКИ

* 1. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28.01.1981 с поправками, одобренными Комитетом министров Совета Европы 15.06.1999, ратифицированная Федеральным законом РФ от 19.12.2005 №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» в рамках, определяемых данным Федеральным законом, заявлений.
  2. Конституция РФ;
  3. Доктрина информационной безопасности РФ, утверждённая Президентом РФ 09.09.2000 № Пр.-1895;
  4. Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных»;
  5. Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
  6. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
  7. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
  8. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
  9. Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении Требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
  10. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищенности, утвержденные приказом ФСБ России от 10.07.2014 №378;
  11. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена ФСТЭК России 14.02.2008 г.;
  12. Специальные требования и рекомендации по технической защите конфиденциальной информации одобренные решением коллегии Гостехкомиссии России от 02.03.2001 № 7.2;
  13. Требования о защите информации, содержащейся в информационных системах общего пользования, утверждённые совместным приказом ФСБ России и ФСТЭК России от 31.08.2010 № 416/489;
  14. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённые приказом ФСТЭК России от 18.02.2013 № 21;
  15. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утверждённые руководством 8 Центра ФСБ России 21.02.2008 №149/5-144;
  16. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при обработке в информационных системах персональных данных, утверждённые руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622;
  17. ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения»;
  18. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
  19. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»;
  20. ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство».

**ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Основание для изменений  (дата, № документа) | Номера листов | | | Дата внесе-ния измене-ний | Дата введе-ния измене-ний в дейст-вие | Всего листов в доку-менте | Фамилия лица, ответственного за внесение изменений |
| Изменен-ных | Новых | Анну-ли-рован-ных |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

1. [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)