Утверждаю
Главный врач ОГБУЗ «Поликлиника №4»

_____ А.В. Бовбалан
«___»_____ 2016 г.

Политика информационной безопасности ОГБУЗ «Поликлиника № 4»

1. Определения и сокращения

Дополнительно для целей настоящего документа используются следующие определения и сокращения:
Авторизация – процедура проверки наличия права доступа (запрос и подтверждение законности доступа) к информационной системе Учреждения
Авторизованный пользователь – работник Участника или Оператора, прошедший процедуру авторизации в информационной системе
АРМ - автоматизированное рабочее место
Безопасность – состояние защищенности интересов (целей) Оператора в условиях угроз
ИБ – информационная безопасность
Информационная система (ИС) - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
ИТ-инфраструктура – информационно-технологическая инфраструктура
ЛВС – локальная вычислительная сеть
НСД – несанкционированный доступ
ПДн – персональные данные
СВТ – средства вычислительной техники
СЗИ – средства защиты информации
ФСБ России – Федеральная служба безопасности Российской Федерации
ФСТЭК России – Федеральная служба по техническому и экспортному контролю Российской Федерации

2. Общие положения

В настоящем документе изложены цели и задачи обеспечения ИБ, а также основные принципы и способы достижения требуемого уровня безопасности информации в Учреждения.

Политика информационной безопасности (далее - Политика ИБ) предназначена для специалистов по обеспечению безопасности информации, руководителей, организующих и проводящих работы по обработке подлежащей защите информации в Учреждении.

Положения настоящей Политики ИБ должны быть учтены при разработке политик информационной безопасности Участников.

Цель Политики ИБ: обеспечение конфиденциальности, целостности и доступности информации, обрабатываемой в ИС Учреждения

- конфиденциальность информации: обработка, хранение и передача информации осуществляется только авторизованными пользователями, которые обязаны не передавать информацию, полученную в результате осуществления должностных обязанностей, третьим лицам без согласия ее обладателя;
- целостность информации: состояние информации, при котором отсутствует

  любое ее изменение, либо изменение осуществляется только

- доступность информации: доступ в установленном порядке к информации авторизованных пользователей по мере необходимости.

Разработка и реализация Политики ИБ в Учреждении осуществляется ответственным лицом по ИБ Оператора путем выработки позиции при решении вопросов ИБ. Руководители структурных подразделений Оператора и Участников должны обеспечить регулярный контроль за соблюдением положений Политики ИБ.

Основными условиями обеспечения ИБ в Учреждении являются:

1. Информация, обрабатываемая в рамках Учреждения, должна быть категорирована, т.е. должен быть составлен перечень ИС Учреждения, в котором должны быть выделены данные (или их группы), содержащие информацию ограниченного доступа.

2. Безопасность информации, отнесенной к информации ограниченного доступа, обеспечивается в соответствии с требованиями законодательства Российской Федерации.

3. Внутренние документы, определяющие порядок обращения с информацией ограниченного доступа, должны быть разработаны и введены в действие в установленном порядке и содержать способы и методы достижения ИБ.

4. Для обработки информации ограниченного доступа в рамках Учреждения определяется перечень должностей, которым разрешен доступ к такой информации в объеме, необходимом для исполнения должностных обязанностей.

5. Обработка информации ограниченного доступа в рамках Учреждения осуществляется с учетом следующих требований:
   - все работники, использующие документы, содержащие информацию ограниченного доступа, должны быть обеспечены местами для безопасного хранения таких документов, исключающих доступ третьих лиц;
   - помещения, в которых обрабатывается информация ограниченного доступа, должны быть оборудованы охранной сигнализацией. Доступ в указанные помещения может быть ограничен с использованием автоматизированной системы контроля доступа;
   - для управления доступом к информации ограниченного доступа применяются механизмы аутентификации и идентификации;
   - для передачи информации ограниченного доступа могут быть использованы только защищенные каналы связи;
   - защита документов в бумажном и электронном виде осуществляется равноценно.

6. Все используемые в Учреждении ИС, в которых обрабатывается информация ограниченного доступа, должны быть классифицированы, а документы систематизированы и учтены. Для каждой категории информации должен быть определен порядок использования, хранения, передачи, архивации и уничтожения, при котором любой документ можно быстро найти и проконтролировать его использование.

7. Решения, принятые Участниками в отношении ИС, входящих в Учреждении, должны быть задокументированы, при этом должна обеспечиваться:

- текущая диагностика сети, вычислительной среды и состояния ресурсов ИС;
- подотчетность и индивидуальная ответственность действий авторизованных пользователей, осуществляющих доступ;
- поддержание соответствующего уровня защиты информации в зависимости от категории и области использования информации в Учреждении;
- контроль и своевременное выявление попыток НСД к защищаемой информации и базам данных Учреждения.

8. Участники должны обеспечить непрерывность деятельности и (или) восстановление деятельности, нарушенной в результате непредвиденных обстоятельств. В указанных целях Участники должны иметь план действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности в случае возникновения непредвиденных обстоятельств, предусматривающий использование дублирующих (резервных) автоматизированных систем и (или) устройств, а также восстановление критически важных для деятельности систем, поддерживаемых внешним поставщиком (провайдером) услуг. Участники определяют порядок проверки возможности выполнения плана действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности в случае возникновения непредвиденных обстоятельств.

9. Все работники, допущенные к обработке информации ограниченного доступа в рамках Учреждения, должны быть ознакомлены под подпись с правилами работы с такой информацией в Учреждении.

10. Участники должны осуществлять мониторинг законодательства Российской Федерации в области защиты информации и принимать меры к совершенствованию способов и средств защиты информации.

3. Ответственность руководства и работников

Оператор и Участники устанавливают цели обеспечения безопасности информации, подлежащей защите в Учреждении, обеспечивают ознакомление работников Оператора и Участников с Политикой ИБ.

Оператор и Участники в рамках своей компетенции принимают стратегические решения по вопросам обеспечения ИБ, утверждают основные документы, регламентирующие порядок функционирования и развития системы обеспечения ИБ в Учреждении.

Оператор и Участники определяют степень защиты информации, координируют деятельность по управлению системой защиты и распределению обязанностей по обеспечению ИБ.

Оператор и Участники обязанны обеспечивать кадровую политику, направленную на минимизацию рисков от ошибок, связанных с человеческим фактором, мошенничества или неправомерного использования информации.

Оператор и Участники устанавливают ответственность работников, нарушивших Политику ИБ, в соответствии с законодательством Российской Федерации.

У Оператора и Участников должны быть назначены должностные лица, ответственные за ИБ, осуществляющее руководство и координацию внедрения мероприятий по управлению ИБ.

Уровни доступа к информации должны быть определены внутренними документами Оператора и Участников. Работники должны быть ознакомлены со своими полномочиями в отношении использования ими информациии и действовать строго в соответствии с предоставленными полномочиями.

Должностные инструкции работников Участника, имеющих доступ к информации ограниченного доступа, должны включать требования по соблюдению положений документов, регулирующих Политику ИБ Учреждения и Участника, а также нормативных актов Российской Федерации по обеспечению ИБ. Условия трудового договора должны определять ответственность работника за нарушение ИБ.

4. Объекты защиты

Основными объектами защиты системы обеспечения ИБ являются:

- информация, содержащая коммерческую тайну, банковскую тайну, ПДн физических лиц, другая информация ограниченного доступа;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации.

4.1. Структура, состав и размещение основных элементов Учреждения, информационные связи с другими объектами

ИС Учреждения является распределенной системой, объединяющей ИС Участников в единую вычислительную (информационно - телекоммуникационную) сеть.

Комплекс технических средств ИС Учреждения включает средства обработки данных (персональные ПК, сервера баз данных, файловые сервера и т.п.), средства обмена данными в ЛВС с возможностью выхода в глобальные информационные сети (кабельная система, мосты, шлюзы, модемы и т.д.), а также средства хранения (в т.ч. архивирования) данных. Указанные технические средства распределены по подсистемам различных Участников.

Взаимодействие с ведомствами (федеральными органами исполнительной власти, внебюджетными федеральными фондами) осуществляется посредством Системы межведомственного электронного взаимодействия (СМЭВ).

Взаимодействие между Участниками осуществляется по защищенным каналам связи.

Для защиты информации применяются программные и аппаратные средства криптографической защиты.

К основным особенностям функционирования Учреждения, относятся:

- значительный географический охват Учрежденем территории субъекта РФ;
- объединение в единую систему большого количества разнообразных технических средств обработки и передачи информации;
- широкий диапазон решаемых задач и типов обрабатываемых сведений (данных), сложные режимы автоматизированной обработки информации с широким совмещением выполнения информационных запросов авторизованных пользователей;
- объединение в единых базах данных информации различного назначения, принадлежности и конфиденциальности;
- непосредственный доступ к ИС Учреждения большого числа различных категорий пользователей (потребителей информации – пользователей УЭК

  и авторизованных пользователей);
- наличие каналов взаимодействия с внешними источниками

  и потребителями информации;
- непрерывность функционирования Учреждения;
- высокая интенсивность информационных потоков в Учреждении;

- наличие в структуре Учреждения ярко выраженных функциональных подсистем с различными требованиями по уровням защищенности (физически объединенных в единую сеть).

Общая структурная и функциональная организация определяется Правилами Учреждения, а также задачами, решаемыми Участниками в зависимости от их роли в Учреждении с применением средств автоматизации.

Объекты информатизации Учреждения включают:

- технологическое оборудование (средства вычислительной техники, сетевое и кабельное оборудование);
- программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение);
- автоматизированные системы связи и передачи данных (средства телекоммуникации);
- каналы связи, по которым передается информация (в том числе информация ограниченного доступа);
- служебные помещения, в которых обрабатывается информация ограниченного доступа.

Обеспечение функционирования и эксплуатация подсистем в части выполнения роли Участником осуществляется соответствующим подразделением Участника на основании требований Правил Учреждения и внутренних документов Участника.

4.2. Информация, подлежащая защите

В ИС Учреждения обрабатывается общедоступная информация и информация ограниченного доступа.

В документообороте Учреждения присутствуют:

- ПДн граждан – работников и пациентов;
- платежные поручения и другие платежные и расчетные документы;
- отчеты (финансовые, аналитические и др.);
- обобщенная информация и другие документы, содержащие информацию ограниченного доступа.

Защите подлежит вся информация, обрабатываемая в Учреждении и содержащая:

- сведения, составляющие банковскую тайну, доступ к которым ограничен в соответствии с Федеральным законом от 2 декабря 1990 г. №395-1 «О банках и банковской деятельности»;

- ПДн граждан, доступ к которым ограничен в соответствии с Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных»;

- технологическая информация, необходимая для поддержания безопасного функционирования Учреждения.

4.3. Категории пользователей, режимы использования и уровни доступа к информации

Авторизованные пользователи должны иметь различные уровни доступа к информационным, программным и другим ресурсам:

- пользователи баз данных;
- операторы баз данных;
- администраторы серверов (файловых серверов, серверов приложений, серверов баз данных) и ЛВС;
- разработчики прикладного программного обеспечения;
- специалисты по обслуживанию технических средств вычислительной техники;
- работники специализированного подразделения по ИБ и др.

У каждого Участника должны быть установлены правила, определяющие разграничение уровня доступа авторизованных пользователей к ИС Учреждения.

5. Цели и задачи обеспечения информационной безопасности

5.1. Защитные меры ИБ в Учреждении

Защитные меры ИБ в Учреждении - это действия, процедуры и механизмы, способные обеспечить соответствующий уровень защиты от возникновения угрозы, уменьшить уязвимость, ограничить воздействие Инцидента в системе безопасности, обнаружить Инциденты и облегчить восстановление информации. Эффективная безопасность требует комбинации различных защитных мер для обеспечения заданных уровней безопасности при защите информации.

Для достижения основной цели защиты и обеспечения ИБ Учреждения должна обеспечивать эффективное решение следующих задач:

- защиту от НСД в процессе функционирования Учреждения (возможность использования Учреждения и доступ к ее ресурсам должны иметь только авторизованные пользователи Участников и Оператора);
- разграничение уровня доступа авторизованных пользователей к аппаратным, программным средствам Учреждения (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы для выполнения своих должностных обязанностей):

  –к информации, обрабатываемой в ИС Участника и Оператора;

  –к средствам вычислительной техники ИС Участника и Оператора;

  – к аппаратным, программным и криптографическим средствам защиты, используемым в ИС Участника и Оператора;
- регистрацию действий авторизованных пользователей при использовании защищаемых ресурсов Учреждения в системных журналах и периодический анализ сведений, содержащихся в них, работниками специализированного подразделения по ИБ;

- контроль целостности среды исполнения программ и ее восстановление в случае нарушения;

- защиту от несанкционированной модификации и контроль целостности используемых в ИС Участников программных средств, а также защиту ИС от внедрения несанкционированных и (или) вредоносных программ;

- защиту информации ограниченного доступа от утечки по техническим каналам, несанкционированного разглашения или искажения при ее обработке, хранении и передаче по защищенным каналам связи;
- обеспечение аутентификации авторизованных пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
- обеспечение фунционирования криптографических средств защиты информации при компрометации части ключевой системы;

- своевременное выявление источников угроз ИБ, причин и условий, способствующих нанесению ущерба субъектам информационных отношений, создание механизма оперативного реагирования на угрозы безопасности информации;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями злоумышленников, ослабление негативного влияния и ликвидация последствий нарушения ИБ.

5.2. Основные пути достижения целей защиты и решения задач ИБ

Основные цели защиты и решение задач ИБ достигаются:

- разработка, внесение изменений и дополнений в Политику ИБ и поддерживающие ее документы;
- полнотой и отсутствием противоречий в требованиях документов Учреждения и внутренних документов Участников, регулирующих вопросы обеспечения ИБ;
- строгим учетом всех объектов защиты;
- регламентацией процессов обработки информации ограниченного доступа, с применением средств автоматизации и действий работников структурных подразделений Участников, использующих ИС, а также действий персонала, осуществляющего обслуживание и модификацию программных и
- назначением и подготовкой работников, ответственных за организацию и осуществление практических мероприятий по обеспечению ИБ;
- наделением каждого работника необходимыми для выполнения им своих функциональных обязанностей полномочиями в соответствии с уровнем доступа к ресурсам Учреждения;
- соблюдением всеми работниками, использующими и обслуживающими аппаратные и программные средства ИС, требований Правил Учреждения, регулирующих вопросы обеспечения ИБ;
- персональной ответственностью за свои действия каждого работника, участвующего в рамках своих функциональных обязанностей, в процессах автоматизированной обработки информации и имеющего соответствующий уровень доступа к ресурсам ИС;
- реализацией технологических процессов обработки информации с использованием комплексов организационно-технических мер защиты программного обеспечения, технических средств и данных;
- принятием эффективных мер обеспечения физической целостности технических средств и непрерывным поддержанием необходимого уровня защищенности компонентов ИС;
- применением физических и программно-аппаратных средств защиты ресурсов ИС и непрерывной административной поддержкой их использования;
- разграничением потоков информации, а также запрет на передачу информации ограниченного доступа по незащищенным каналам связи;
- контролем за соблюдением работниками Участников требований по обеспечению ИБ;
- юридической защитой интересов Участников при взаимодействии с внешними организациями (связанном с обменом информацией) от противоправных действий

как со стороны этих организаций, так и от несанкционированных действий третьих лиц;

- проведением постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации, разработкой и реализацией предложений по совершенствованию ИБ Учреждения;
- назначение и подготовка работников, ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации;
- закрепление в должностных инструкциях установленного разграничения полномочий в области обеспечения ИБ;
- контроль соблюдения пользователями ИС требований норм законодательства Российской Федерации в области ПДн, документов Учреждения и внутренних документов Участника, регулирующим вопросы обеспечения безопасности информации;
- проведение постоянного анализа эффективности и достаточности применяемых мер и средств защиты информации, разработка и реализация предложений по совершенствованию нормативной базы системы защиты информации.

5.3. Политика ИБ Участника

В целях обеспечения ИБ каждый Участник разрабатывает частную политику ИБ в рамках своей организации, с учетом роли Участника и индивидуальных особенностей. В частной политике ИБ Участника должны быть сформулированы цели

и стратегия обеспечения ИБ организации и обеспечены согласованность всех защитных мер с Политикой ИБ Учреждения. Для повышения эффективности целей и стратегии обеспечения безопасности они должны быть интегрированы в программы обучения и повышения квалификации работников специализированных подразделений Участника в области ИБ.

Цели, стратегия, политика и процедуры, обеспечивающие ИБ Участника должны быть определены документально и реализованы в соответствующих подразделениях и на соответствующих уровнях организации. Внутренние документы Участника должны включать в себя требования ИБ.

6. Общие принципы обеспечения ИБ в Учреждении

Построение системы обеспечения ИБ в Учреждении и ее функционирование осуществляется в соответствии со следующими основными принципами:

- Законности

Защита информации в Учреждении основывается на положениях и требованиях нормативных правовых актов Российской Федерации, стандартов и иных документов по обеспечению ИБ.

- Системности

Системный подход предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени и пространстве элементов, условий и факторов, существенно значимых для понимания проблемы и решения задачи обеспечения безопасности информации в Учреждении.

- Комплексности

Безопасность информации обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер, реализуемых Оператором и Участником.

Применение различных средств и технологий защиты информации должно перекрывать все каналы реализации угроз безопасности информации и минимизировать количество уязвимых мест.

Должен быть обеспечен отраслевой подход к разработке рекомендаций и требований по защите информации в Учреждении с учетом особенностей обработки информации Участников.

- Непрерывности и совершенствования

Защита информации должна обеспечиваться на всех технологических этапах обработки подлежащих защите данных и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

Совершенствование мер и средств ИБ на основе результатов анализа функционирования ИС и системы защиты информации с учетом выявления новых способов и средств реализации угроз безопасности, положительного опыта в сфере ИБ должно производиться регулярно.

Участник должен определять действия, необходимые для устранения причин потенциальных несоответствий требованиям по безопасности с целью предотвратить их повторное появление, в том числе руководствуясь рекомендациями Оператора.

- Своевременности

Принимаемые меры по обеспечению безопасности должны носить упреждающий характер. Каждый Участник принимает необходимые меры по защите информации до начала обработки подлежащей защите информации, которые должны обеспечить надлежащий уровень безопасности.

Система защиты информации разрабатывается одновременно с развитием ИС Участника, что позволяет учитывать требования по безопасности на этапе проектирования и при модернизации ИС.

- Достаточности и адекватности

Состояние и стоимость реализации мер защиты должны быть соизмеримы с рисками, связанными с нарушением ИБ.

Программно-технические средства защиты не должны ухудшать основные функциональные характеристики и производительность Учреждения.

Уровень рекомендаций и требований по ИБ должен соответствовать имеющемуся уровню развития информационных технологий и средств защиты информации.

- Персональной ответственности

Ответственность за обеспечение ИБ и в Учреждении возлагается на каждого работника Оператора и Участника в пределах его полномочий.

Распределение обязанностей и полномочий работников должно обеспечивать выявление виновных лиц в случаях нарушения ИБ.

Роли и обязанности работников должны быть определены и документально установлены в соответствии с организационной политикой ИБ Участников.

- Минимизации полномочий

Предоставление и использование прав на доступ к информации ограниченного доступа должно быть ограничено и управляемо.

Авторизованным пользователям должны предоставляться минимально необходимые права на доступ к информации ограниченного доступа, объем и длительность предоставления прав должно определяться производственной необходимостью для выполнения должностных обязанностей.

- Гибкости

В процессе функционирования Учреждения могут меняться ее характеристики, и также объем и категории обрабатываемой в Учреждении информации ограниченного доступа.

- Кадровой политики

Участники должны реализовывать кадровую политику, позволяющую исключить или минимизировать возможность нарушения положений по ИБ работниками.

Реализация мер по обеспечению и эксплуатации системы обеспечения ИБ Участников должны осуществляться профессионально подготовленными специалистами.

- Контролируемости обеспечения безопасности

Применяемые Участником меры по обеспечению ИБ должны быть организованны в соответствии с требованиями законодательства Российской Федерации и рекомендациями органов власти, осуществляющими функции по контролю и надзору ИБ, а также Оператора.

Участником должны быть определены процедуры для постоянного контроля применения мер по обеспечению ИБ. Результаты контроля должны анализироваться и корректироватьтся на регулярной основе.

7. Общие методы обеспечения ИБ

7.1. Классификация методов обеспечения ИБ

Методы обеспечения ИБ разделяются на:

- административно-правовые;

К административно-правовым методам обеспечения ИБ относится соблюдение требований:

- законодательства Российской Федерации в области ИБ,
- Политик ИБ Оператора и Участников, регламентирующие правила обращения с информацией ограниченного доступа, закрепляющие права и обязанности Участников в процессе обработки и использования информации ограниченного доступа, а также устанавливающие ответственность за нарушения этих требований, препятствуя неправомерной обработке и являющиеся сдерживающим фактором для реализации угроз безопасности злоумышленникам.

- организационно-технические;

Организационно-технические методы обеспечения ИБ основаны на использовании организационных мер, программных, аппаратных, программно-аппаратных средств, входящих в состав системы обеспечения ИБ и выполняющих функции защиты информации, и направленных на решение следующих задач:

- учет всех подлежащих защите ресурсов ИС (ПДн, других подлежащих защите данных, сервисов, каналов связи, серверов, автоматизированных рабочих мест и т.д.);
- предотвращение НСД к информации ограниченного доступа и(или) передачи ее лицам, не имеющим права на доступ к такой информации;
- своевременное обнаружение фактов НСД к информации ограниченного доступа;
- недопущение воздействия на технические средства автоматизированной обработки информации ограниченного доступа, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления данных, модифицированных или уничтоженных вследствие НСД к ним;
- постоянный контроль за обеспечением уровня защищенности информации.

- экономические.

Экономические методы обеспечения ИБ включают:

- разработку Оператором и Участниками программ обеспечения ИБ;

- разработка Участниками мер поощрения и наложения штрафных санкций за соблюдение или не соблюдение установленных правил и процедур обработки информации ограниченного доступа.

По времени применения методы обеспечения ИБ разделяются на:

- превентивные;

Превентивные методы обеспечения ИБ осуществляются на основе применения в процессе эксплуатации Учреждения комплекса организационных, технических и технологических мероприятий, а также методов и средств обеспечения функциональной устойчивости и безопасности работы ИС Участников.

Организационные мероприятия по обеспечению ИБ направлены на организацию:

- деятельности работников, использующих ИС Участников;
- порядка применения информационных технологий в зданиях и сооружениях;
- систематического применения мер по поддержанию штатного функционирования Учреждения.

Технические мероприятия по обеспечению ИБ заключаются в обслуживании, поддержке и управлении составом технических средств Учреждения, обеспечивающих обработку информации ограниченного доступа в Учреждении в защищенном режиме.
Технологические мероприятия по обеспечению безопасности информации направлены на реализацию заданных функций и алгоритмов работы Учреждения, технологий обработки информации ограниченного доступа и защиту программ и данных от преднамеренных и непреднамеренных нарушений.

- восстановительные.

Осуществление восстановительных методов обеспечения ИБ определяется Правилами Учреждения и внутренними документами Участников, устанавливающими требования к обязательным мероприятиям, проводимым как заблаговременно, так и после возникновения нарушений, угрожающих штатному функционированию Учреждения.

7.2. Основные этапы работ по обеспечению ИБ

Основные этапы работ по обеспечению ИБ информации ограниченного доступа включают:

- определение объектов защиты;
- установление целей защиты;
- определение угроз объектам защиты;
- установление требований к системе обеспечения ИБ информации;
- создание системы обеспечения ИБ;
- определение порядка контроля.

Определение угроз ИБ проводится путем формирования общей модели угроз и модели нарушителя Учреждения. При этом модель нарушителя формируется как составная часть модели угроз, определяющая возможные специфические угрозы.
Установление требований к системе обеспечения ИБ основано на формировании моделей угроз и нарушителя.
На основе общей модели угроз и модели нарушителя Учреждения, сформированной в соответствии с нормативными и методическими документами ФСТЭК России и ФСБ России, определяются требования к средствам защиты информации, а также требования к поддерживающим эти средства организационным мерам.

8. Общая модель угроз и нарушителя Учреждения

На основании общей модели угроз и нарушителя Учреждения возможна разработка частных моделей угроз и моделей нарушителя для ИС подключенных к Учреждения.

8.1. Угрозы безопасности информации и их источники

В качестве основных типов угроз безопасности информации в ИС Учреждения рассматриваются нарушение:

- доступности информации подразумевает, что доступ к информации блокируется для авторизованных пользователей. Это может происходить по причине того, что программные или технические средства, при помощи которых осуществляется доступ к информации, потеряли свои потребительские качества и не могут в означенные сроки предоставить пользователю необходимую информацию;
- целостности информации подразумевает, что информация была несанкционированно искажена (разрушена), потеряла достоверность и отличается от информации, которая была сформирована первоначально как исходная информация;
- конфиденциальности информации подразумевает, что информация была перехвачена злоумышленником и защищаемые сведения стали доступны кругу лиц, не имеющих на это соответствующих прав.

Все угрозы безопасности информации в ИС Учреждения подразделяются на два класса:

- угрозы, не являющиеся атаками;
- атаки (потенциальные или проводимые).

К угрозам ИС Учреждения, не являющимся атаками, относятся:

- угрозы, не связанные с деятельностью человека;
- угрозы социально-политического и террористического характера;

- ошибочные действия и/или нарушения, связанные с недобросовестностью, халатностью, безответственностью, некомпетентностью и т.д.;
- угрозы техногенного характера.

К угрозам, не связанным с деятельностью человека, относятся стихийные бедствия и природные явления (землетрясения, наводнения, ураганы и т.д.), которые могут, в частности, привести к пожарам в помещениях с оборудованием ИС Учреждения, затоплениям этих помещений, их разрушению, выходу из строя оборудования ИС Учреждения. Необходимо отметить, что ликвидация последствий этих угроз связана с возможным проникновением в помещения с оборудованием ИС Учреждения посторонних лиц (пожарные расчеты, спасатели и т.п.), среди которых могут находиться нарушители.

К угрозам социально-политического и террористического характера относятся забастовки, саботаж, локальные конфликты, террористические акты, сопровождаемые нападением на объекты ИС Учреждения, и т.д. Угрозы данного вида могут не только привести к временной неработоспособности ИС Учреждения, выходу из строя оборудования и/или потере, искажению и компрометации информации, но и создать условия, которые может использовать в своих целях нарушитель.

К ошибочным действиям и/или нарушениям, связанным с недобросовестностью, халатностью, безответственностью, некомпетентностью и т.д., в частности, относятся:

- непредумышленное искажение или удаление информации (электронных документов);
- нарушение правил хранения персональной ключевой, аутентифицирующей информации, а также любой другой информации ограниченного доступа;
- предоставление неаваторизованным пользователям возможности обработки информации ограниченного доступа, доступа к средствам защиты информации, а так же к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований;
- внедрение и использование неучтенных программ;
- непредумышленное искажение или удаление программных компонентов автоматизированной системы защиты информации;
- несообщение о фактах утраты, компрометации персональной ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа.

Угрозы данного вида также могут представлять как самостоятельную опасность, так и служить основой для реализации атак со стороны нарушителя (например, в случае нарушения правил хранения персональной ключевой информации и других требований нормативных документов по защите информации).

Основными угрозами техногенного характера являются:

- аварии (отключение электропитания, системы заземления, аварии системы водоснабжения и канализации, разрушение инженерных сооружений);
- неисправности, сбои (выход из строя технических средств ИС Учреждения: серверов, АРМ авторизованных пользователей, коммуникационного и сетевого

оборудования), нестабильность параметров системы электропитания, заземления и т.д.;
- помехи и наводки, приводящие к сбоям в работе технических средств ИС Учреждения.

Угрозами безопасности для информационных и телекоммуникационных средств и функционально-технологических подсистем ИС Учреждения являются:
- противоправный сбор, разглашение и использование технологической информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия (недекларированных возможностей);
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- вирусные атаки на объекты информатизации ИС Учреждения;
- компрометация ключевой информации и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств для перехвата информации в технические средства обработки и передачи информации по каналам связи, а также в служебные помещения;
- уничтожение, повреждение, разрушение или хищение материальных носителей информации;
- перехват информации в ЛВС и навязывание ложной информации;
- использование не сертифицированных по требованиям безопасности информации отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи;
- несанкционированный доступ к информации, обрабатываемой и циркулирующей на объектах Учреждения;
- нарушение законных ограничений на распространение информации.

Угрозы ИБ могут быть направлены на следующие компоненты ИС Учреждения:

- серверы информационных систем;
- АРМ администраторов и операторов;
- программно-технические средства защиты;
- программное обеспечение функционально-технологических подсистем Участников;
- сетевую инфраструктуру: маршрутизаторы, коммутаторы и другое активное и пассивное оборудование;

Источники угроз безопасности информации могут носить как субъективный, так и объективный характер. Все источники угроз безопасности информации делятся на три основные группы:

- обусловленные действиями субъекта (антропогенные источники угроз);

- обусловленные техническими средствами (техногенные источники угрозы);
- обусловленные стихийными бедствиями.

8.2. Модель угроз информационной безопасности для Учреждения

Модель угроз ИБ для Учреждения представляет собой перечень возможных угроз ИБ, под которыми понимается совокупность условий и факторов, создающих опасность нарушения безопасности защищаемой информации.

Разработка модели угроз является необходимым условием определения требований, которым должны удовлетворять средства защиты информации, используемые в Учреждении. Именно этим обусловлено требование полноты и обоснованности модели угроз.

8.3. Модель нарушителя Учреждения

Под моделью нарушителя Учреждения понимается перечень предположений о возможностях нарушителя, которые он способен использовать для разработки и проведения атак, а также об ограничениях этих возможностей.

Нарушитель может действовать на различных этапах жизненного цикла средств защиты информации, используемых в Учреждении. Под этими этапами в настоящем документе понимаются разработка указанных средств, их производство, хранение, транспортировка, ввод в эксплуатацию (пуско-наладочные работы), эксплуатация и демонтаж.

На этапах разработки, производства, хранения, транспортировки и ввода в

эксплуатацию используемых в Учреждении технических и программных СКЗИ и среды функционирования криптосредств обработка информации не производится. Поэтому объектами угроз и атак на этих этапах являются только сами эти средства и документация на них.

Обеспечение безопасности указанных объектов достигается путем использования организационно - технических мер защиты и проведением обязательных проверок во

время ввода в эксплуатацию криптосредств и среды функционирования криптосредств на соответствие эталонным образцам и заданным алгоритмам функционирования.

СКЗИ для обеспечения безопасности информации при их обработке в ИС должны быть сертифицированы ФСБ России.

На этапе эксплуатации защита от угроз безопасности, не являющихся атаками, как правило, регламентируется различного рода инструкциями и положениями (разработанными с учетом особенностей эксплуатации ИС и действующей нормативной базы), в которых описываются регламенты действий должностных лиц, допущенных к работе с Учреждения. При этом возникновение угроз связано с ошибочными действиями или нарушениями тех или иных требований указанными лицами.

Угрозы безопасности, являющиеся атаками, готовятся и осуществляются нарушителем целенаправленно и определяются его конкретными возможностями.

Возможными объектами атак в Учреждении являются следующие объекты:

- документация на криптосредства и на технические и программные компоненты среды функционирования криптосредств;
- информация ограниченного доступа;
- ключевая, аутентифицирующая и парольная информация;
- криптографически опасная информация;
- программные и аппаратные компоненты СЗИ;
- программные и аппаратные компоненты криптосредств;
- технические и программные компоненты среды функционирования криптосредств;
- данные, передаваемые по каналам связи;
- помещения, в которых находятся подлежащие защите ресурсы ИС.

При передаче информации по каналам связи она должна быть зашифрована с использованием криптосредств или для ее передачи должны использоваться защищенные каналы связи. Должна осуществляться защита информации, записываемой на материальные носители (магнитные, магнито-оптические, оптические, смарт-карты, карты флэш-памяти и т.п.).

8.4. Описание нарушителей (субъектов атак)

Возможности потенциальных нарушителей Учреждения существенно зависят от реализованной Политики ИБ и принятыми режимными, организационно-техническими и техническими мерами по обеспечению безопасности.

Все физические лица, имеющие доступ к техническим и программным средствам Учреждения, относятся к источникам угроз и могут рассматриваться как потенциальные нарушители. Согласно проведенному анализу, к потенциальным нарушителям Учреждения можно отнести следующих нарушителей:

- внешнего нарушителя;
- внутреннего нарушителя, имеющего санкционированный доступ к Учреждения, но не имеющего доступа к подлежащей защите информации;
- внутреннего нарушителя, имеющего санкционированный доступ к Учреждения и имеющего доступ к подлежащей защите информации.

С учетом специфики функционирования Учреждения и характера обрабатываемой в ней информации предполагается, что авторизованные пользователи Учреждения,

которые имеют права администраторов на осуществление технического управления и обслуживания аппаратных и программных средств, в том числе и средств защиты, включая их настройку, конфигурирование и распределение ключевой и парольной документации относятся к особо доверенным лицам и исключаются из числа потенциальных нарушителей.

8.5. Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что потенциальные нарушители обладают информацией, необходимой для подготовки и проведения атак, за исключением информации, доступ к которой исключается системой обеспечения ИБ.

При определении ограничений на степень информированности потенциального нарушителя рассматривались:

- содержание технической документации на технические и программные компоненты среды функционирования криптосредств;
- долговременные ключи криптосредств;
- все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от НСД по отношению к информации организационно-техническими мерами (фазовые пуски, синхропосылки, незашифрованные адреса, команды управления и т.п.);
- сведения о линиях связи, по которым передается подлежащая защите информация;
- все сети связи, работающие на едином ключе;
- все проявляющиеся в каналах связи, не защищенных от НСД по отношению к информации организационно-техническими мерами, нарушения правил эксплуатации криптосредств и их среды функционирования;
- все проявляющиеся в каналах связи, не защищенных от НСД по отношению к информации организационно-техническими мерами, неисправности и сбои криптосредств и среды функционирования криптосредств;
- сведения, получаемые в результате анализа любых сигналов от технических средств криптосредств и среды их функционирования, которые может перехватить нарушитель;
- исходные тексты прикладного программного обеспечения ИС.

8.6. Предположения об имеющихся у нарушителя средствах атак

Предполагается, что потенциальный нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства.

При определении ограничений на имеющиеся у потенциального нарушителя средства атак рассмотрены:

- аппаратные компоненты криптосредств и среда их функционирования;
- доступные в свободной продаже технические средства и программное обеспечение;
- специально разработанные технические средства и программное обеспечение;
- штатные средства.

8.7. Описание каналов атак

Основными каналами атак являются каналы связи, не защищенные от НСД по отношению к информации организационно-техническими мерами.

Другими возможными каналами атак могут являться:

1. Каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический) – возможность реализации атаки потенциальным нарушителем ограничена применением комплекса режимных мероприятий: ограничением доступа в помещения Учреждения.
2. Материальные носители информации – канал актуален в случае хищения материальных носителей у авторизованного пользователя с целью копирования подлежащей защите информации, получения криптографически опасной и ключевой информации.
3. Носители информации, выведенные из употребления – недоступны потенциальному нарушителю (все носители информации, используемые для обработки и хранения подлежащей защите информации, зарегистрированы и при выводе их из употребления до момента уничтожения находятся под контролем).
4. Сигнальные цепи, цепи электропитания, цепи заземления – объем информации, который может быть получен в результате успешной реализации атаки крайне ограничен, что несопоставимо со сложностью реализации и затратами на проведение атаки.
5. Канал утечки за счет электронных устройств негласного получения информации. Доступ в контролируемую зону (охраняемая территория Оператора, обеспечивающая необходимый уровень ИБ) Учреждения ограничен в соответствии с внутренними документами Оператора. Несмотря на это, поскольку часть СВТ Учреждения находится за пределами контролируемой зоны, канал может быть использован потенциальным злоумышленником для получения информации о проводимых авторизованным пользователем операциях, ПДн, нанесенных на поверхность УЭК, а также ПИН-кода.
6. Информационные и управляющие интерфейсы СВТ – недоступны потенциальному нарушителю, защищены средствами, описанными в предыдущих разделах, а также организационными мерами.
7. Каналы утечки подлежащей защите информации, содержащейся в побочных сигналах, возникающих при функционировании криптосредств – объем информации, который может быть получен в результате успешной реализации атаки крайне ограничен, что несопоставимо со сложностью реализации и затратами на проведение атаки.

8.8. Определение типа нарушителя

В результате рассмотренных предположений о доступных каналах и способах получения информации нарушителем, которые он может использовать для разработки и проведения атак, а также ограничениях этих возможностей, в соответствии с «Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» определены и согласованы с ФСБ России базовые уровни криптографической защиты данных для ИС Участников.

1. Для Оператора:

Для защиты от внешнего нарушителя, осуществляющего атаки из-за пределов контролируемой зоны, требуется применение СКЗИ соответствующего требованиям ФСБ России по классу не ниже КВ2 для обеспечения безопасного взаимодействия с ЦИ и ЦП, и не ниже КС3 для обеспечения безопасного взаимодействия с другими Участниками.

Для защиты от внутреннего нарушителя требуется применение СКЗИ, соответствующего требованиям ФСБ России по классу не ниже КВ2 для обеспечения безопасного взаимодействия с ЦИ и ЦП, и не ниже КС3 для обеспечения безопасного взаимодействия с другими Участниками. Эти СКЗИ должны обеспечивать защиту внутреннего контура ЛВС ИС Оператора. СКЗИ должны обеспечивать выполнение специальных требований по уровню КВ и КС.

2. Для УОС:

Для защиты от внешнего нарушителя, осуществляющего атаки из-за пределов контролируемой зоны, требуется применение СКЗИ соответствующего требованиям ФСБ России по классу не ниже КС3. Эти СКЗИ должны обеспечивать защиту каналов связи ИС УОС.

Для защиты от внутреннего нарушителя требуется применение СКЗИ, соответствующего требованиям ФСБ России по классу не ниже КС3. Эти СКЗИ должны обеспечивать защиту внутреннего контура ЛВС ИС УОС.

Окончательное определение возможных угроз и типа нарушителя целесообразно осуществить на основе частных моделей угроз и нарушителя, разработанных для каждого отдельного УОС с учетом особенностей их функционирования и необходимости обеспечения общего уровня защиты.

3. Для ЦИ:

Для защиты от внешнего нарушителя, осуществляющего атаки из-за пределов контролируемой зоны, требуется применение СКЗИ соответствующего требованиям ФСБ России по классу не ниже КВ2. Эти СКЗИ должны обеспечивать защиту каналов связи ИС ЦИ.

Для защиты от внутреннего нарушителя требуется применение СКЗИ, соответствующего требованиям ФСБ России по классу не ниже КВ2. Эти СКЗИ должны обеспечивать защиту внутреннего контура ЛВС ИС ЦИ. СКЗИ также должны обеспечивать выполнение специальных требований по уровню КВ2.

Окончательное определение возможных угроз и типа нарушителя целесообразно осуществить на основе частных моделей угроз и нарушителя, разработанных для каждого отдельного ЦИ с учетом особенностей их функционирования и необходимости обеспечения общего уровня защиты.

4. Для ЦП:

   Для защиты от внешнего нарушителя, осуществляющего атаки из-за пределов контролируемой зоны, требуется применение СКЗИ соответствующего требованиям ФСБ России по классу не ниже КВ2. Эти СКЗИ должны обеспечивать защиту каналов связи ИС ЦП.

   Для защиты от внутреннего нарушителя требуется применение СКЗИ, соответствующего требованиям ФСБ России по классу не ниже КВ2. Эти СКЗИ должны обеспечивать защиту внутреннего контура ЛВС ИС ЦП. СКЗИ должны обеспечивать выполнение специальных требований по уровню КВ2.

   Окончательное определение возможных угроз и типа нарушителя целесообразно осуществить на основе частных моделей угроз и нарушителя, разработанных для каждого отдельного ЦП с учетом особенностей их функционирования и необходимости обеспечения общего уровня защиты.

5. Для ОКО:

   Для защиты каналов связи между терминалами и серверной частью ИС ОКО от внешнего и внутреннего нарушителя требуется применение СКЗИ соответствующего требованиям ФСБ России по классу КС1. СКЗИ должны обеспечивать выполнение специальных требований по уровню КС.

   Вместе с тем, при информационном взаимодействии ИС ОКО с другими Участниками для защиты каналов связи в ОКО должны использоваться СКЗИ, обеспечивающие уровень криптографической защиты не ниже, чем у другого Участника.

   Окончательное определение возможных угроз и типа нарушителя целесообразно осуществить на основе частных моделей угроз и нарушителя, разработанных для каждого отдельного ОКО с учетом особенностей их функционирования и необходимости обеспечения общего уровня защиты.

6. Для прочих Участников:

   При информационном взаимодействии ИС Участника с другими Участниками Учреждения для защиты каналов связи в ИС Участника должны использоваться СКЗИ, обеспечивающие уровень криптографической защиты не ниже, чем у другого Участника.

   Окончательное определение возможных угроз и типа нарушителя целесообразно осуществить на основе частных моделей угроз и нарушителя, разработанных для каждого отдельного Участника с учетом особенностей их функционирования и необходимости обеспечения общего уровня защиты.

9. Порядок пересмотра Политики ИБ

Ответственным органом, ответственным за Политику ИБ в целом, который отвечает за ее реализацию и пересмотр в соответствии с установленной процедурой, является Управление безопасности Оператора.

Ответственными органами за реализацию и пересмотр частных политик безопасности Участников, являются подразделения Участников, ответственные за обеспечение ИБ.

Положения настоящей Политики ИБ и частные политики Участников пересматриваются в порядке, установленном Правилами Учреждения и внутренними документами Участников не реже одного раза в 3 года.

Внеплановый пересмотр Политики ИБ проводится в случае существенных изменений международного или национального законодательства в сфере защиты информации или по усмотрению Оператора в связи с необходимостью дополнить или скорректировать положения Политики ИБ.

При внесении изменений в положения Политики ИБ учитываются:

- уровень развития и внедрения информационных технологий в телекоммуникационной отрасли;
- рекомендации российских и международных профильных организаций по ИБ и защите информации;
- рекомендации регулирующих органов, уполномоченных в области защиты информации;
- результаты проверки эффективности политики, исходя из характера, числа и последствий зарегистрированных инцидентов нарушения ИБ;
- определение стоимости мероприятий по управлению ИБ и их влияние на эффективность деятельности Учреждения;
- оценка влияния изменений в технологиях.