Приложение № 1
к приказу № 01-01/34-1
от 12.05.2025 г.

КОНЦЕПЦИЯ
информационной безопасности информационных систем государственного бюджетного учреждения социального обслуживания Владимирской области «Арбузовский психоневрологический интернат имени Александра Лукича Лосева»

1. Назначение и правовая основа документа

Настоящая Концепция информационной безопасности информационных систем (ИС) государственного бюджетного учреждения социального обслуживания Владимирской области «Арбузовский психоневрологический интернат имени Александра Лукича Лосева» (далее по тексту – ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева») определяет систему взглядов на вопрос обеспечения безопасности персональных данных (ПДн) и представляет собой систематизированное изложение целей и задач защиты, как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации.

Законодательной основой настоящей Концепции являются Конституция Российской Федерации, Гражданский, Административный, Уголовный кодексы, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федеральный закон, законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации, документы ФСТЭК и ФСБ России.

Использование данной Концепции в качестве основы для построения комплексной системы информационной безопасности информации ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» позволит оптимизировать затраты на ее построение.

При разработке Концепции учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

Основные положения Концепции базируются на качественном осмыслении вопросов безопасности информации и не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защиту информации.

Концепция является методологической основой для:

– формирования и проведения единой политики в области обеспечения безопасности ПДн в ИС ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева»;

– принятия управленческих решений и разработки практических мер по безопасности ПДн и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ПДн;

– координации деятельности структурных подразделений ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» при проведении работ по развитию и эксплуатации ИС с соблюдением требований обеспечения безопасности ПДн;

– разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИС ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева».

2. Термины и определения

В настоящем документе применяются следующие термины:

Автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники;

Безопасность ПДн – состояние защищенности ПДн, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах ПДн;

Биометрические ПДн – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию;

Блокирование ПДн – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению;

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию, ПДн или ресурсы информационной системы;

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения ПДн, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки ПДн или в помещениях, в которых установлены информационные системы ПДн;

Доступ в операционную среду компьютера (информационной системы ПДн) – получение возможности запуска на выполнение штатных команд, функций,

процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ;

Доступ к информации – возможность получения информации и ее использования;

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

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;

Информационная система ПДн (ИСПДн) – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий, и технических средств;

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

Использование ПДн – действия (операции) с ПДн, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн или других лиц либо иным образом затрагивающих права и свободы субъекта ПДн или других лиц;

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации;

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств;

Конфиденциальность ПДн – обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не допускать их распространение без согласия субъекта ПДн или наличия иного законного основания;

Нарушитель безопасности ПДн – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности ПДн при их обработке техническими средствами в ИСПДн;

Неавтоматизированная обработка ПДн – обработка ПДн, содержащихся в ИСПДн либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с ПДн, как использование, уточнение, распространение, уничтожение ПДн в отношении каждого из субъектов ПДн, осуществляются при непосредственном участии человека;

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации;

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых ИСПДн;

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин;

Обезличивание ПДн – действия, в результате которых невозможно определить принадлежность ПДн конкретному субъекту ПДн;

Обработка ПДн – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение Пдн;

Общедоступные ПДн – ПДн, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

Оператор ПДн – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн;

Перехват информации – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов;

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);

Персональные данные, разрешенные субъектом ПДн для распространения – ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн путем дачи согласия на обработку ПДн, разрешенных субъектом ПДн для распространения в порядке, предусмотренном Федеральным законом от 27.07.2006 № 152-ФЗ;

Пользователь ИСПДн – лицо, участвующее в функционировании ИСПДн или использующее результаты ее функционирования;

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа;

Предоставление ПДн – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;

Раскрытие ПДн – умышленное или случайное нарушение конфиденциальности ПДн;

Распространение ПДн – действия, направленные на раскрытие ПДн неопределенному кругу лиц;

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы;

Специальные категории ПДн – ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта ПДн;

Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа;

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

Трансграничная передача ПДн – передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

Угрозы безопасности ПДн – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональ ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий при их обработке в ИСПДн;

Уничтожение ПДн – действия, в результате которых невозможно восстановить содержание ПДн в ИСПДн или в результате которых уничтожаются материальные носители ПДн;

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации;

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации;

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

3. Общие положения

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) ИС ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева». Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

СЗПДн представляет собой совокупность организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними.

Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий.

Структура, состав и основные функции СЗПДн определяются исходя из класса ИС. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

Эти меры призваны обеспечить:

– конфиденциальность информации (защиту от несанкционированного ознакомления);

– целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

– доступность информации (возможность за приемлемое время получить требуемую информационную услугу).

Стадии создания СЗПДн включают:

– предпроектная стадия, включающая предпроектное обследование ИС, разработку технического (частного технического) задания на ее создание;

– стадия проектирования (разработки проектов) и реализации ИС, включающая разработку СЗПДн в составе ИС;

– стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИС требованиям безопасности информации.

Организационные меры предусматривают создание и поддержание правовой базы безопасности ПДн и разработку (введение в действие) организационно-распорядительных документов.

Технические меры защиты реализуются при помощи соответствующих программно-технических средств и методов защиты.

Перечень необходимых мер защиты информации определяется по результатам оценки угроз безопасности для ИС ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева».

4. Задачи СЗПДн

Основной целью СЗПДн является минимизация ущерба от возможной реализации угроз безопасности ПДн.

Для достижения основной цели система безопасности ПДн ИС должна обеспечивать эффективное решение следующих задач:

– защиту от вмешательства в процесс функционирования ИС посторонних лиц;

– разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИС, т.е. защиту от несанкционированного доступа:

– к информации, циркулирующей в ИС;

– средствам вычислительной техники ИС;

– аппаратным, программным и криптографическим средствам защиты, используемым в ИС;

– регистрацию действий пользователей при использовании защищаемых ресурсов ИС в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;

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

– защиту от несанкционированной модификации и контроль целостности используемых в ИС программных средств, а также защиту системы от внедрения несанкционированных программ;

– защиту ПДн, хранимых и обрабатываемых, от несанкционированного разглашения или искажения;

– своевременное выявление источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн 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 ПДн.

5. Объекты защиты

Объектами защиты являются – информация, обрабатываемая в ИС, и технические средства ее обработки и защиты. Перечень ПДн, подлежащие защите, утвержден директором ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева».

К объектам защиты относятся:

– обрабатываемая информация;

– технологическая информация;

– программно-технические средства обработки;

– средства защиты ПДн;

– помещения, в которых размещены компоненты ИС.

6. Классификация субъектов доступа к ИС

Среди субъектов доступа к ИС выделяются четыре группы:

– пользователь ИС;

– администратор информационной безопасности (ответственный за защиту информации);

– системный администратор ИС;

– разработчик программного обеспечения обработки защищаемой информации.

Пользователем ИСПДн является сотрудник ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева», участвующий в процессе эксплуатации ИС. Пользователь ИС обладает следующим уровнем доступа:

– обладает всеми необходимыми атрибутами, обеспечивающими доступ к некоторому подмножеству ПДн;

– располагает конфиденциальными данными, к которым имеет доступ.

Администратором информационной безопасности (ответственным за защиту информации) является сотрудник ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева», отвечающий за принятие и контроль мер по защите ИС и информации, обрабатывающейся в ней. Администратор информационной безопасности (ответственный за защиту информации) обладает следующим уровнем доступа:

– обладает полной информацией о возможных каналах утечки информации;

– обладает полной информацией о системе защиты ИС, программных и программно-аппаратных средствах защиты информации;

– имеет право выработки мер защиты информации.

Системным администратором ИС является сотрудник ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» или сторонней организации, которая занимается настройкой, внедрением и сопровождением программ обработки защищаемой информации и в целом программной среды функционирования ИС. Системный администратор ИС обладает следующим уровнем доступа:

– обладает полной информацией о системном и прикладном программном обеспечении ИС;

– обладает полной информацией о технических средствах и конфигурации ИС;

– имеет доступ ко всем техническим средствам обработки информации и данным ИС;

– обладает правами конфигурирования и административной настройки технических средств ИС.

Разработчиков программного обеспечения обработки защищаемой информации является сторонняя организация, реализующая автоматизацию процесса обработки информации или обеспечивающая программную среду для функционирования такого программного обеспечения. Разработчик программного обеспечения обработки защищаемой информации обладает следующим уровнем доступа:

– обладает информацией об алгоритмах и программах обработки информации в ИС;

– обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИС на стадии ее разработки, внедрения и сопровождения;

– может располагать любыми фрагментами информации о топологии ИС и технических средствах обработки и защиты ПДн, обрабатываемых в ИС.

7. Основные принципы построения системы комплексной защиты информации

Построение системы, обеспечения безопасности информации ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева», и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

– Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности информации ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» в соответствии с действующим законодательством в области защиты информации, а также других законодательных актов по безопасности информации РФ, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией. Принятые меры безопасности ПДн не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях.

Все пользователи ИС ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева», которые осуществляют обработку ПДн, должны иметь представление об ответственности за правонарушения в области защиты информации.

– Системность

Системный подход к построению системы защиты информации в ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности информации.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем, в которых производится обработка ПДн, а также характер, возможные объекты и направления атак на нее со стороны нарушителей (особенно высококвалифицированных злоумышленников).

Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

– Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

– Непрерывность защиты

Обеспечение безопасности информации - процесс, осуществляемый руководством ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева», администратором безопасности информации (ответственным за защиту информации) и сотрудниками. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность средств защиты, сколько процесс, который должен постоянно идти на всех уровнях внутри ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева», и каждый сотрудник должен принимать участие в этом процессе. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева». И ее эффективность зависит от участия руководства ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» в обеспечении информационной безопасности информации.

Кроме того, большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления защиты.

– Своевременность

Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите информации и реализацию мер обеспечения безопасности информации на ранних стадиях разработки информационных систем в целом и их систем защиты, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самих защищаемых информационных систем. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) системы, обладающие достаточным уровнем защищенности.

– Преемственность и совершенствование

Предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» и системы их защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

– Разумная достаточность (экономическая целесообразность)

Предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы компонентов ИС. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока информация находится в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

– Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности информации и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

– Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

– Исключение конфликта интересов (разделение функций)

Эффективная система обеспечения информационной безопасности предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться, и находится под строгим независимым контролем. Реализация данного принципа предполагает, что ни один сотрудник не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Наделение сотрудников полномочиями, порождающими конфликт интересов, дает ему возможность подтасовывать информацию в корыстных целях или с тем, чтобы скрыть проблемы или понесенные убытки. Для снижения риска манипулирования информацией и риска хищения, такие полномочия должны в максимально возможной степени быть разделены между сотрудниками или подразделениями ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева». Необходимо проводить периодические проверки обязанностей, функций и деятельности сотрудников, выполняющих ключевые функции с тем, чтобы они не имели возможности скрывать совершение неправомерных действий. Кроме того, необходимо принимать специальные меры по недопущению сговора между сотрудниками.

– Взаимодействие и сотрудничество

Сотрудники ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» должны осознанно соблюдать установленные правила и оказывать содействие деятельности администратора безопасности информации (ответственного за обработку ПДн).

Важным элементом эффективной системы обеспечения безопасности информации в ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» является высокая культура работы с информацией. Руководство ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» несет ответственность за строгое соблюдение этических норм и стандартов профессиональной деятельности, подчеркивающей и демонстрирующей персоналу на всех уровнях важность обеспечения информационной безопасности ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева». Все сотрудники ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе. Несмотря на то, что высокая культура обеспечения информационной безопасности не гарантирует автоматического достижения целей, ее отсутствие создает больше

возможностей для нарушения безопасности или не обнаружения фактов ее нарушения.

– Гибкость системы защиты

Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» своей деятельности. В число таких изменений входят:

- изменения организационной и штатной структуры ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева»;
- изменение существующих или внедрение принципиально новых информационных систем;
- новые технические средства.

Свойство гибкости системы обеспечения информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

– Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

– Простота применения средств защиты

Механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

– Обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по безопасности информации.

– Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально

подготовленными специалистами ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» (ответственных за организацию обработки ПДн).

– Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности информации, на основе используемых систем и средств защиты информации, при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

Кроме того, эффективная система обеспечения информационной безопасности требует наличия адекватной и всеобъемлющей информации о текущем состоянии процессов, связанных с движением информации и сведений о соблюдении установленных нормативных требований, а также дополнительной информации, имеющей отношение к принятию решений. Информация должна быть надежной, своевременной, доступной и правильно оформленной.

Недостатки системы обеспечения информационной безопасности, выявленные сотрудниками ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» должны немедленно доводиться до сведения руководителя ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» и оперативно устраняться. Вопросы, которые кажутся незначительными, когда отдельные процессы рассматриваются изолированно, при рассмотрении их наряду с другими аспектами могут указать на отрицательные тенденции, грозящие перерасти в крупные недостатки, если они не будут своевременно устранены.

8. Меры обеспечения информационной безопасности

Все меры обеспечения безопасности ИС ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» подразделяются на:

– Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе их обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом ИС ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева».

– Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» в целом. Морально-

этические нормы бывают как неписаные, так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективе.

– Технологические меры защиты

К данному виду мер защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

– Организационные (административные) меры защиты

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки информации, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Формирование Концепции безопасности

Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать политику в области обеспечения безопасности информации (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

С практической точки зрения политику в области обеспечения безопасности информации в ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» целесообразно разбить на два уровня. К верхнему уровню относятся решения руководства, затрагивающие деятельность ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» в целом. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности информации, определить какими ресурсами (материальные, структурные, организационные) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью.

Политика нижнего уровня, определяет процедуры, и правила достижения целей и решения задач безопасности информации и детализирует (регламентирует) эти правила:

– каковы роли и обязанности должностных лиц, отвечающие за проведение Концепции безопасности информации;

– кто имеет права доступа к информации, кто и при каких условиях может читать и модифицировать информации и т.д.

Политика нижнего уровня должна:

– предусматривать регламент информационных отношений, исключающих возможность произвольных, монопольных или несанкционированных действий в отношении информационных ресурсов;

– определять коалиционные и иерархические принципы и методы разделения секретов и разграничения доступа к информации;

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

Регламентация доступа в помещения

Компоненты информационных систем должны размещаться в помещениях, находящихся под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, АРМ и т.п.). Уборка таких помещений должна производиться в присутствии ответственного сотрудника, за которым закреплены данные компоненты, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым информационным ресурсам.

Все посторонние лица допускаются в помещения с компонентами информационной системы только в присутствии сотрудников ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева».

По окончании рабочего дня, помещения, в которых размещаются компоненты ИС ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева», должны запираться на ключ, по возможности опечатываться.

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

Регламентация допуска сотрудников к использованию информационных ресурсов

В рамках разрешительной системы (матрицы) доступа устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.

Допуск пользователей к работе с информационными системами и доступ к их ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком.

Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

– каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которыми ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, должно согласовываться с администратором безопасности информации (ответственным за организацию обработки ПДн);

– директор ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями.

Все сотрудники ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева», должны нести персональную ответственность за нарушения установленного порядка обработки информации, правил хранения, использования и передачи, находящихся в их распоряжении защищаемых ресурсов ИС. Каждый сотрудник (при трудоустройстве) должен подписывать обязательство о соблюдении и ответственности за нарушение установленных требований по обеспечению безопасности информации ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева».

Обработка ПДн в компонентах ИС ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» должна производиться в соответствии с утвержденными технологическими инструкциями.

Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов

В целях поддержания режима информационной безопасности аппаратно-программная конфигурация автоматизированных рабочих мест сотрудников ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева», с которых возможен доступ к ресурсам информационной системы, должна соответствовать кругу возложенных на данных пользователей функциональных обязанностей.

В компонентах информационной системы и на рабочих местах пользователей должны устанавливаться и использоваться лицензионные программные средства.

Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов

Оборудование ИС, используемое для доступа и хранения информации, к которому доступ обслуживающего персонала в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к его компонентам, должно закрываться.

Подбор и подготовка персонала, обучение пользователей

Пользователи ИС ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева», а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации в ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева».

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

Все пользователи ИС должны быть ознакомлены с организационно - распорядительными документами по обеспечению безопасности информации (ПДн) ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева», в части, их касающейся, должны знать и неукоснительно выполнять инструкции, и знать общие обязанности по обеспечению безопасности информации. Доведение требований указанных документов до лиц, допущенных к обработке защищаемой информации, должно осуществляться под роспись.

Ответственность за нарушения установленного порядка пользования ресурсами ИС

Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной работы с информацией, должна определяться нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению руководства ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева».

Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

- индивидуальная идентификация пользователей и инициированных ими процессов, т.е. установление за ними идентификатора (login, Username), на базе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности доступа;
- проверка подлинности пользователей (аутентификация) на основе паролей;
- реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).

Средства обеспечения безопасности информации

Для обеспечения информационной безопасности используются следующие средства защиты:

– Физические средства защиты

Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Для обеспечения физической безопасности компонентов ИС необходимо осуществлять ряд организационных и технических мероприятий, включающих: проверку оборудования, предназначенного для обработки информации, на:

- наличие специально внедренных закладных устройств;
- введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки информации;
- оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи.

Технические средства защиты

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции

защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности информации по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

- средства разграничения доступа к данным;
- средства регистрации доступа к компонентам ИС и контроля за использованием информации;
- средства реагирования на нарушения режима информационной безопасности.

На технические средства защиты возлагается решение следующих основных задач:

- идентификация и аутентификация пользователей при помощи имен или специальных аппаратных средств (Advantor, Touch Memory, Smart Card и т.п.);
- регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам;
- защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;
- регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;
- защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информации, находящейся на нем.

Средства идентификации и аутентификации пользователей

В целях предотвращения работы с ресурсами ИС посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей). Для идентификации могут применяться различного рода устройства: магнитные карточки, ключи, ключевые вставки, дискеты и т.п.

Аутентификация (подтверждение подлинности) пользователей также может осуществляться:

- путем проверки наличия у пользователей каких-либо специальных устройств (магнитных карточек, ключей, ключевых вставок и т.д.);
- путем проверки знания ими паролей;
- путем проверки уникальных физических характеристик и параметров самих пользователей при помощи специальных биометрических устройств.

Средства разграничения доступа

Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

Технические средства разграничения доступа должны по возможности быть составной частью единой системы контроля доступа:

- на контролируемую территорию;
- в отдельные помещения;

- к компонентам информационной среды и элементам системы защиты ПДн (физический доступ);
- к информационным ресурсам (документам, носителям информации, файлам, наборам данных, архивам, справкам и т.д.);
- к активным ресурсам (прикладным программам, задачам и т.п.);
- к операционной системе, системным программам и программам защиты.

Средства обеспечения и контроля целостности

Средства обеспечения целостности включают в свой состав средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

Средства контроля целостности информационных ресурсов систем предназначены для своевременного обнаружения модификации или искажения ресурсов системы. Они позволяют обеспечить правильность функционирования системы защиты и целостность хранимой и обрабатываемой информации.

Контроль целостности информации и средств защиты, с целью обеспечения неизменности информационной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной модификации информации должен обеспечиваться:

- средствами разграничения доступа (в помещения, к документам, к носителям информации, к серверам, логическим устройствам и т.п.);
- средствами электронной подписи;
- средствами подсчета контрольных сумм (для используемого программного обеспечения**).**

Средства оперативного контроля и регистрации событий безопасности

Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т.п.), которые могут повлечь за собой нарушение безопасности и привести к возникновению кризисных ситуаций. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, их характер, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации. Средства контроля и регистрации должны предоставлять возможности:

- ведения и анализа журналов регистрации событий безопасности (системных журналов);
- получения твердой копии (печати) журнала регистрации событий безопасности;
- упорядочения журналов, а также установления ограничений на срок их хранения;
- оперативного оповещения администратора безопасности информации (ответственного за организацию обработки ПДн) о нарушениях.

При регистрации событий безопасности в журнале должна фиксироваться следующая информация:

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

9. Контроль эффективности системы защиты ИС

Контроль эффективности СЗПДн должен осуществляется на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а также прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

Контроль может проводиться как администраторами информационной безопасности ИС (оперативный контроль в процессе информационного взаимодействия в ИС), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности.

Контроль может осуществляться администратором информационной безопасности как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля.

Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям

10. Сферы ответственности за безопасность ПДн

Ответственным за разработку мер и контроль над обеспечением безопасности ПДн является должностное лицо ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева», назначаемое приказом директора ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева». Он может делегировать часть полномочий по обеспечению безопасности ПДн. Сфера ответственности включает курирование вопросов информационной безопасности.

Сфера ответственности администратора информационной безопасности (ответственного за защиту информации), так же назначаемого приказом директора ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева», включает:

- планирование и реализация мер по обеспечению безопасности ПДн;
- анализ угроз безопасности ПДн;
- разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности;
- контроль защищенности ИТ-инфраструктуры ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» от угроз безопасности;
- обучение и информирование пользователей ИС, о порядке работы с ПДн, ИС и средствами защиты;
- предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к объектам защиты, с этими организациями должно быть заключено соглашение о конфиденциальности либо соглашение о соблюдении режима безопасности ПДн при выполнении работ в ИС.

11. Модель нарушителя безопасности

Под нарушителем в ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты.

Нарушители подразделяются по признаку доступа к ИС. Все нарушители делятся на две группы:

- внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИС;
- внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИС.

Классификация нарушителей представляется в Модели угроз безопасности ПДн каждой ИС.

12. Модель угроз безопасности

Для ИС ГБУСОВО «Арбузовский ПНИ им. А.Л. Лосева» выделяются следующие основные категории угроз безопасности ПДн:

Угрозы от утечки по техническим каналам.

Угрозы несанкционированного доступа к информации:

- угрозы уничтожения, хищения аппаратных средств ИС, носителей информации путем физического доступа к элементам ИС;
- угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);
- угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз не антропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений ит.п.) характера;
- угрозы преднамеренных действий внутренних нарушителей;
- угрозы несанкционированного доступа по каналам связи.

Описание угроз, вероятность их реализации, опасность и актуальность представляются в Модели угроз безопасности ПДн каждой ИС.

13. Механизм реализации Концепции

Реализация Концепции должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

- федеральных законов в области обеспечения информационной безопасности и защиты информации;
- постановлений Правительства Российской Федерации;
- руководящих, организационно-распорядительных и методических документов ФСТЭК России и ФСБ России;
- потребностей ИС в средствах обеспечения безопасности информации.

14. Ожидаемый эффект от реализации Концепции

Реализация Концепции безопасности ПДн в ИС позволит:

- оценить состояние безопасности информации ИС, выявить источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;
- разработать распорядительные и нормативно-методические документы применительно к ИС;
- провести классификацию и сертификацию (аттестацию) ИС;
- провести организационно-режимные и технические мероприятия по обеспечению безопасности ПДн в ИС;
- обеспечить необходимый уровень безопасности объектов защиты.

Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности ИС и создаст условия для ее дальнейшего совершенствования.