Министерство образования, науки и молодежи Республики Крым
Государственное бюджетное специализированное учреждение Республики Крым
«Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних»

УТВЕРЖДЕНО
Приказом директора
ГБСУ РК «Керченский
МСРЦН» № 224-ХД
«28» июля 2021 года

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

в Государственном бюджетном специализированном учреждении Республики Крым
«Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних»

г. Керчь
2021 год

С О Д Е Р Ж А Н И Е

ОПРЕДЕЛЕНИЯ **3**
ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ **7**
ВВЕДЕНИЕ **8**
1. ОБЩИЕ ПОЛОЖЕНИЯ **9**
2. ЗАДАЧИ СЗПДН **10**
3. ОБЪЕКТЫ ЗАЩИТЫ **10**
3.1. Перечень информационных систем 10
3.2. Перечень объектов защиты 10
4. КЛАССИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ИСПДН 11
5. **ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ** 11
5.1. Законность 12
5.2. Системность 12
5.3. Комплексность 12
5.4. Непрерывность защиты пдн 12
5.5. Своевременность 13
5.6. Преемственность и совершенствование 13
5.7. Персональная ответственность 13
5.8. Принцип минимизации полномочий 13
5.9. Взаимодействие и сотрудничество 13
5.10. Гибкость системы защиты пдн 13
5.11. Открытость алгоритмов и механизмов защиты 13
5.12. Простота применения средств защиты 14
5.13. Научная обоснованность и техническая реализуемость 14
5.14. Специализация и профессионализм 14
5.15. Обязательность контроля 14
6. МЕРЫ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ТРЕБУЕМОГО УРОВНЯ ЗАЩИЩЕННОСТИ **14**
6.1. Правовые меры защиты 14
6.2. Морально-этические меры защиты 15
6.3. Организационные (административные) меры защиты 15
6.4. Физические меры защиты 16
6.5. Аппаратно-программные средства защиты ПДн 16
7. КОНТРОЛЬ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИСПДН **17**
8. СФЕРЫ ОТВЕТСТВЕННОСТИ ЗА БЕЗОПАСНОСТЬ ПДН **17**
9. МОДЕЛЬ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ **17**
10. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ **18**
11. МЕХАНИЗМ РЕАЛИЗАЦИИ КОНЦЕПЦИИ **18**
12. ОЖИДАЕМЫЙ ЭФФЕКТ ОТ РЕАЛИЗАЦИИ КОНЦЕПЦИИ **18**
13. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ **18**

ОПРЕДЕЛЕНИЯ

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

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

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

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 персональные данные или ресурсы информационной системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – 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.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

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.

Информативный сигнал – электрический сигнал, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств (ст.3 п.9 № 152-ФЗ).

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

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц (ст.3 п.5 № 152-ФЗ).

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 персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и / или выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека (ПП №687 от 15.09.08).

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующими 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 информационными системами персональных данных.

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 персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных (ст.3 п.8 № 152-ФЗ).

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование и уничтожение персональных данных (ст.3 п.3 № 152-ФЗ).

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности (ст.3 п.12 № 152-ФЗ).

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и / или осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных (ст.3 п.2 № 152-ФЗ).

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

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация (ст.3 п.1 № 152-ФЗ).

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

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

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и / или блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом (ст.3 п.4 № 152-ФЗ).

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

Специальные категории персональных данных – персональные данные, касающиеся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

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

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства (ст.3 п.11 № 152-ФЗ).

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

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

Учреждение – государственное образовательное учреждение города Москвы.

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).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АВС	-	антивирусные средства
АРМ	-	автоматизированное рабочее место
ВТСС	-	вспомогательные технические средства и системы
ИСПДн	-	информационная система персональных данных
КЗ	-	контролируемая зона
ЛВС	-	локальная вычислительная сеть
МЭ	-	межсетевой экран
НСД	-	несанкционированный доступ
ОС	-	операционная система
ПДн	-	персональные данные
ПМВ	-	программно-математическое воздействие
ПО	-	программное обеспечение
ПЭМИН	-	побочные электромагнитные излучения и наводки
САЗ	-	система анализа защищенности
СЗИ	-	средства защиты информации
СЗПДн	-	система (подсистема) защиты персональных данных
СОВ	-	система обнаружения вторжений
ТКУИ	-	технические каналы утечки информации
УБПДн	-	угрозы безопасности персональных данных
ФСТЭК России	-	Федеральная служба по техническому и экспортному контролю

ВВЕДЕНИЕ

Настоящая Концепция информационной безопасности ИСПДн Государственного бюджетного специализированного учреждения Республики Крым «Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних» (далее - ГБСУ РК «Керченский МСРЦН») является официальным документом, в котором определена система взглядов на обеспечение информационной безопасности ГБСУ РК «Керченский МСРЦН».

Необходимость разработки Концепции обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов в ГБСУ РК «Керченский МСРЦН», при обработке информации вообще, и персональных данных в частности.

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) ГБСУ РК «Керченский МСРЦН». Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

Концепция разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ПДн, с позиции комплексного применения технических и организационных мер и средств защиты.

Под информационной безопасностью ПДн понимается защищенность персональных данных и обрабатывающей их инфраструктуре от любых случайных или злонамерных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности ГБСУ РК «Керченский МСРЦН», а также нормативных и методических документов, обеспечивающих ее реализацию.

Концепция является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности ПДн в ИСПДн в ГБСУ РК «Керченский МСРЦН»;
- принятия управленческих решений и разработки практических мер по воплощению политики 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 администрации и структурных подразделений ГБСУ РК «Керченский МСРЦН» при проведении работ по развитию и эксплуатации ИСПДн с соблюдением требований обеспечения безопасности ПДн;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн ГБСУ РК «Керченский МСРЦН».
- правовой базой для разработки настоящей Концепции служат требования действующих в Российской Федерации законодательных и нормативных документов по обеспечению безопасности персональных данных (ПДн).

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) ГБСУ РК «Керченский МСРЦН», в соответствии с Перечнем ИСПДн. 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 персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн. 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 (защита 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 ИСПДн, разработку технического (частного технического) задания на ее создание;
- стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;
- стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

Организационные меры предусматривают создание и поддержание правовой базы безопасности ПДн и разработку (введение в действие) предусмотренных Политикой информационной безопасности ИСПДн следующих организационно-распорядительных документов:

План мероприятий по обеспечению защиты ПДн при их обработке в ИСПДн;

План мероприятий по контролю обеспечения защиты ПДн;

Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ;

Должностная инструкция администратора ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;

Должностная инструкция администратора безопасности ИСПДн;

Должностная инструкция пользователя ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;

Инструкция на случай возникновения внештатной ситуации;

Рекомендации по использованию программных и аппаратных средств защиты информации.

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

Перечень необходимых мер защиты информации определяется по результатам внутренней проверки безопасности ИСПДн в ГБСУ РК «Керченский МСРЦН».

2. ЗАДАЧИ СЗПДН

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

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

- защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования АС и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);
- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

к информации, циркулирующей в ИСПДн;

средствам вычислительной техники ИСПДн;

аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн;

- регистрацию действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;
- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
- защиту от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защиту системы от внедрения несанкционированных программ;
- защиту ПДн от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
- защиту ПДн, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;
- обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;
- 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.

3. ОБЪЕКТЫ ЗАЩИТЫ

3.1 ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ

В ГБСУ РК «Керченский МСРЦН» производится обработка персональных данных в информационных системах обработки персональных данных (ИСПДн).

Перечень ИСПДн определяется на основании Отчета по результатам внутренней проверки.

3.2. ПЕРЕЧЕНЬ ОБЪЕКТОВ ЗАЩИТЫ

Объектами защиты являются – информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты. Перечень персональных данных, подлежащие защите, определен в Перечне персональных данных, подлежащих защите в ИСПД.

Объекты защиты включают:

- обрабатываемая информация;
- технологическая информация;
- программно-технические средства обработки;

- средства защиты ПДн;
- каналы информационного обмена и телекоммуникации;
- объекты и помещения, в которых размещены компоненты ИСПДн.

4. КЛАССИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ИСПДН

Пользователем ИСПДн является лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования. Пользователем ИСПДн является любой сотрудник ГБСУ РК «Керченский МСРЦН», имеющий доступ к ИСПДн и ее ресурсам в соответствии с установленным порядком, в соответствии с его функциональными обязанностями.

Пользователи ИСПДн делятся на три основные категории:

1. Администратор ИСПДн. Сотрудник ГБСУ РК «Керченский МСРЦН», который занимается настройкой, внедрением и сопровождением системы. Администратор ИСПДн обладает следующим уровнем доступа:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

2. Программист-разработчик ИСПДн. Сотрудники ГБСУ РК «Керченский МСРЦН» или сторонних организаций, которые занимаются разработкой программного обеспечения. Разработчик ИСПДн обладает следующим уровнем доступа:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

3. Оператор ИСПДн. Администрация учреждения**,** специалисты, воспитатели, сотрудники структурных подразделений ГБСУ РК «Керченский МСРЦН», участвующие в процессе эксплуатации ИСПДн. Оператор ИСПДн обладает следующим уровнем доступа:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

Категории пользователей должны быть определены для каждой ИСПДн. Должно быть уточнено разделение сотрудников внутри категорий, в соответствии с типами пользователей определенными в Политике информационной безопасности.

Все выявленные группы пользователей отражаются в Отчете по результатам внутренней проверки. На основании Отчета определяются права доступа к элементам ИСПДн для всех групп пользователей и отражаются в Матрице доступа (таблица №1), в Положении о разграничении прав доступа к обрабатываемым персональным данным.

5. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Построение системы обеспечения безопасности ПДн ИСПДн ГБСУ РК «Керченский МСРЦН» и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;

- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

5.1. ЗАКОННОСТЬ

Предполагает осуществление защитных мероприятий и разработку СЗПДн ГБСУ РК «Керченский МСРЦН» в соответствии с действующим законодательством в области защиты ПДн и другими нормативными правовыми актами по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.

Пользователи и обслуживающий персонал ПДн ИСПДн ГБСУ РК «Керченский МСРЦН» должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиту ПДн.

5.2. СИСТЕМНОСТЬ

Системный подход к построению СЗПДн ГБСУ РК «Керченский МСРЦН» предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн ГБСУ РК «Керченский МСРЦН».

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

5.3. КОМПЛЕКСНОСТЬ

Комплексное использование методов и средств защиты 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. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

5.4. НЕПРЕРЫВНОСТЬ ЗАЩИТЫ ПДн

Защита ПДн – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн.

ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИСПДн в незащищенное состояние.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, 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 системы защиты после восстановления ее функционирования.

5.5. СВОЕВРЕМЕННОСТЬ

Предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом и ее системы защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании информационной архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

5.6. ПРЕЕМСТВЕННОСТЬ И СОВЕРШЕНСТВОВАНИЕ

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

5.7. ПЕРСОНАЛЬНАЯ ОТВЕТСТВЕННОСТЬ

Предполагает возложение ответственности за обеспечение безопасности ПДн 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.

5.8. ПРИНЦИП МИНИМИЗАЦИИ ПОЛНОМОЧИЙ

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено».

Доступ к ПДн должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

5.9. ВЗАИМОДЕЙСТВИЕ И СОТРУДНИЧЕСТВО

Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИСПДн ГБСУ РК «Керченский МСРЦН», для снижения вероятности возникновения негативных действий связанных с человеческим фактором.

В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений технической защиты информации.

5.10. ГИБКОСТЬ СИСТЕМЫ ЗАЩИТЫ ПДн

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

5.11. 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). Однако, это не означает, что информация о конкретной системе защиты должна быть общедоступна.

5.12. ПРОСТОТА ПРИМЕНЕНИЯ СРЕДСТВ ЗАЩИТЫ

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИСПДн.

5.13. НАУЧНАЯ 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, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности ПДн.

СЗПДн должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

5.14. СПЕЦИАЛИЗИАЦИЯ И ПРОФЕССИОНАЛИЗМ

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности ПДн, 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 ГБСУ РК «Керченский МСРЦН».

5.15. ОБЯЗАТЕЛЬСНОСТЬ КОНТРОЛЯ

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДнб 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.

6. МЕРЫ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ТРЕБУЕМОГО УРОВНЯ ЗАЩИЩЕННОСТИ

Обеспечение требуемого уровня защищенности должности достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИСПДн подразделяются на:

- правовые;
- морально-этические;
- организационные (административные);
- физические;
- технические (аппаратные и программные).

Перечень выбранных мер обеспечения безопасности отражается в Плане мероприятий по обеспечению защиты персональных данных.

6.1. ПРАВОВЫЕ МЕРЫ ЗАЩИТЫ

К правовым мерам защиты относятся действующие в стране законы и иные нормативно-правовые акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности

участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

6.2. МОРАЛЬНО-ЭТИЧЕСКИЕ МЕРЫ ЗАЩИТЫ

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), 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 коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий связанных с человеческим фактором.

6.3. ОРГАНИЗАЦИОННЫЕ (АДМИНИСТРАТИВНЫЕ) МЕРЫ ЗАЩИТЫ

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

Главная цель административных мер, предпринимаемых на высшем управленческом уровне – сформировать Политику информационной безопасности ПДн (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация Политики информационной безопасности ПДн в ИСПДн состоят из мер административного уровня и организационных (процедурных) мер защиты информации.

К административному уровню относятся решения руководства учреждения, затрагивающие деятельность ИСПДн в целом. Эти решения закрепляются в Политике информационной безопасности. Примером таких решений могут быть:

- принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ПДн, определение ответственных за ее реализацию;
- формулирование целей, постановка задач, определение направлений деятельности в области безопасности ПДн;
- принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне ГБСУ РК «Керченский МСРЦН» в целом;
- обеспечение нормативно - правовой базы вопросов безопасности и т.п.

Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности ПДн, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИСПДн.

На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности ПДн. Эти правила определяют:

- какова область применения политики безопасности ПДн;
- каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности ПДн, а так же их установить ответственность;
- кто имеет права доступа к ПДн;

- какими мерами и средствами обеспечивается защита ПДн;

- какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры должны:

- предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;

- определять коалиционные и иерархические принципы и методы разграничения доступа к ПДн;

- определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов;

- организовать меры противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

Организационные меры должны состоять из:

- регламента доступа в помещения ИСПДн;

- порядка допуска сотрудников к использованию ресурсов ИСПДн ГБСУ РК «Керченский МСРЦН»;

- регламента процессов ведения баз данных и осуществления модификации информационных ресурсов;

- регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПДн;

- инструкций пользователей ИСПДн (администратора ИСПДн, администратора безопасности, оператора ИСПДн);

- инструкции пользователя при возникновении внештатных ситуаций.

6.4.ФИЗИЧЕСКИЕ МЕРЫ ЗАЩИТЫ

Физические меры защиты основаны на применении разного рода механических, электро- 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.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств (видеокамер).

6.5. АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ПДн

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн 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 ПДн в ИСПДн по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

- средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;

- средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн ГБСУ РК «Керченский МСРЦН»;

- средства обеспечения и контроля целостности программных и информационных ресурсов;

- средства оперативного контроля и регистрации событий безопасности;

- криптографические средства защиты ПДн.

Успешное применение технических средств защиты на основании принципов (раздел 5) предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонентов ИСПДн;
- каждый сотрудник (пользователь ИСПДн) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;
- в ИСПДн ГБСУ РК «Керченский МСРЦН» разработка и отладка программ осуществляется за пределами ИСПДн, на испытательных стендах;
- все изменения конфигурации технических и программных средств ИСПДн производятся строго установленным порядком (регистрируются и контролируются) только на основании распоряжений руководства ГБСУ РК «Керченский МСРЦН»;
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.). специалистами ГБСУ РК «Керченский МСРЦН» осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

7. КОНТРОЛЬ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИСПДН.

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 так прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

Контроль может проводиться как администраторами безопасности ИСПДн (оперативный контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

Контроль может осуществляться администратором 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.

8. СФЕРЫ ОТВЕТСТВЕННОСТИ ЗА БЕЗОПАСНОСТЬ ПДН

Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является директор ГБСУ РК «Керченский МСРЦН». Директор может делегировать часть полномочий по обеспечению безопасности персональных данных на заместителей директора.

Сфера ответственности включает следующие направления обеспечения безопасности ПДн:

- 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;
- обучение и информирование пользователей ИСПДн, о порядке работы с ПДн 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 (раздел 3), с этими организациями должно быть заключено «Соглашение о конфиденциальности», либо «Соглашение о соблюдении режима безопасности ПДн при выполнении работ в ИСПДн».

9. МОДЕЛЬ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ

Под нарушителем в ГБСУ РК «Керченский МСРЦН» понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты (раздел 3).

Нарушители подразделяются по признаку принадлежности к ИСПДн. Все нарушители делятся на две группы:

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

Классификация нарушителей представлена в Модели угроз безопасности персональных данных каждой ИСПДн.

10. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ

Для ИСПДн ГБСУ РК «Керченский МСРЦН» выделяются следующие основные категории угроз безопасности персональных данных:

угрозы от утечки по техническим каналам;

угрозы несанкционированного доступа к информации:

- угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн;
- 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 ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

угрозы преднамеренных действий внутренних нарушителей;

угрозы несанкционированного доступа по каналам связи.

Описание угроз, вероятность их реализации, опасность и актуальность представлены в Модели угроз безопасности персональных данных каждой ИСПДн.(Приложение.)

11. 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;
- нормативно-правовых актов Правительства Российской Федерации;
- руководящих, организационно-распорядительных и методических документов ФСТЭК России;
- потребностей ИСПДн в средствах обеспечения безопасности информации.

12. ОЖИДАЕМЫЙ ЭФФЕКТ ОТ РЕАЛИЗАЦИИ КОНЦЕПЦИИ

Реализация Концепции безопасности ПДн в ИСПДн позволит:

- оценить состояние безопасности информации ИСПДн, 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 ИСПДн;
- провести классификацию и сертификацию ИСПДн;

- провести организационно-режимные и технические мероприятия по обеспечению безопасности ПДн в ИСПДн;

- обеспечить необходимый уровень безопасности объектов защиты.

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

13. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Основными нормативно-правовыми и методическими документами, на которых базируется настоящая Концепция, являются:

1. Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.
2. «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденное Постановлением Правительства РФ от 17.11.2007 г. № 781.
3. «Порядок проведения классификации информационных систем персональных данных», утвержденный совместным Приказом ФСТЭК России № 55, ФСБ России № 86 и Мининформсвязи РФ № 20 от 13.02.2008 г.
4. «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 г. № 687.
5. «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства РФ от 06.07.2008 г. № 512.
6. Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн.
7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП).
8. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП).
9. «Положение о методах и способах защиты информации в информационных системах персональных данных», утвержденное директором ФСТЭК от 05.01.2010 г. № 58.

Приложение

Матрица доступа для ИСПДн

Типовая роль	Уровень доступа к ПДн	Разрешенные действия
Администратор ИСПДн	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам	- сбор - систематизация - накопление - хранение - уточнение - использование - распространение - обезличивание - блокирование

	обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	- уничтожение
Администратор безопасности	Обладает правами Администратора. Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов. Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение
Программист-разработчик ИСПДн	Обладает информацией об алгоритмах и программах обработки информации на ИСПДн. Обладает правами внесения изменений в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения. Располагает всей информаций о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн	- систематизация - накопление - хранение - уточнение - обезличивание - блокирование - уничтожение
Оператор ИСПДн первой группы	Обладает правами доступа к подмножеству ПДн. Располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системам, через которую он осуществляет доступ, и составе технических средств ИСПДн.	- сбор - систематизация - накопление - хранение
Оператор ИСПДн второй группы	Обладает правами доступа к подмножеству ПДн.	- уточнение - использование - распространение - обезличивание

Приложение 2

Министерство образования, науки и молодежи Республики Крым
Государственное бюджетное специализированное учреждение Республики Крым
«Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних»

УТВЕРЖДЕНО
Приказом директора
ГБСУ РК «Керченский
МСРЦН» №_____
«___»_____20__ года

ИНСТРУКЦИЯ
по проведению антивирусного контроля в информационной системе персональных данных ГБСУ РК «Керченский МСРЦН»

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая инструкция определяет требования к организации обеспечения безопасности персональных данных в информационной системе персональных данных (далее – ИСПДн) Государственного бюджетного специализированного учреждения Республики Крым «Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних» (далее – Учреждение) от воздействия компьютерных вирусов и другого вредоносного программного обеспечения и устанавливает ответственность сотрудников Учреждения, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

1.1. В целях обеспечения антивирусной защиты в ИСПДн производится антивирусный контроль.

1.2. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на администратора безопасности информации ИСПДн.

1.3. К применению в ИСПДн допускаются сертифицированные антивирусные средства.

1.4. В ИСПДн запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

1.5. Пользователи ИСПДн при работе со съемными носителями информации (USB флеш-накопителями) обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.

1.6. Ярлык для запуска антивирусной программы должен быть вынесен на «Рабочий стол» операционной системы.

1.7. Установка и настройка средств антивирусного контроля осуществляется администратором безопасности ИСПДн в соответствии с руководствами по применению конкретных антивирусных средств.

1.8. Администратор безопасности информации ИСПДн осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.

1.9. Администратор безопасности информации ИСПДн проводит периодическое тестирование всего установленного программного обеспечения на предмет отсутствия компьютерных вирусов.

1.10. При обнаружении компьютерного вируса пользователь ИСПДн обязан немедленно поставить в известность администратора безопасности информации ИСПДн и прекратить какие-либо действия в ИСПДн.

1.11. Администратор безопасности информации ИСПДн проводит, в случае необходимости, «лечение зараженных» файлов путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводит антивирусный контроль.

1.12. В случае обнаружения на съемных носителях информации нового вируса, «не поддающегося лечению», администратор безопасности информации ИСПДн обязан запретить использование данного съемного носителя информации.

1.13. В случае обнаружения вируса, «не поддающегося лечению», администратор безопасности информации ИСПДн обязан поставить в известность ответственного за обеспечение безопасности персональных данных в ИСПДн, запретить работу в ИСПДн и в возможно короткие сроки обновить пакет антивирусных программ.

1.14. Доведение Инструкции до сотрудников ГБСУ РК «Керченский МСРЦН» в части их касающейся осуществляется администратором безопасности информации ИСПДн под роспись в Листе ознакомления с данной инструкцией (Прилагается).

ЛИСТ ОЗНАКОМЛЕНИЯ
с инструкцией по проведению антивирусного контроля в информационной системе
персональных данных ГБСУ РК «Керченский МСРЦН»

№ п/п	Дата ознакомления	Фамилия, инициалы сотрудника	Должность сотрудника	Подпись

Приложение 3

Министерство образования, науки и молодежи Республики Крым
Государственное бюджетное специализированное учреждение Республики Крым
«Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних»

УТВЕРЖДЕНО
Приказом директора
ГБСУ РК «Керченский
МСРЦН» №_____
«___»_____20__ года

ИНСТРУКЦИЯ
о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные в ГБСУ РК «Керченский МСРЦН»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная Инструкция содержит обязательные для всех сотрудников Государственного бюджетного специализированного учреждения Республики Крым «Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних» требования по обеспечению конфиденциальности документов, содержащих персональные данные.

1.2. Персональные данные – это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

1.3. Обеспечение конфиденциальности персональных данных не требуется в случае обезличивания персональных данных или в отношении общедоступных персональных данных. В общедоступные источники персональных данных (в том числе справочники, адресные книги) в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

1.4. Конфиденциальность персональных данных предусматривает обязательное согласие субъекта персональных данных или наличие иного законного основания на их обработку. Согласие субъекта персональных данных не требуется на обработку данных:

- в целях исполнения обращения, запроса субъекта персональных данных, трудового или иного договора с ним;
- адресных данных, необходимых для доставки почтовых отправлений организациями почтовой связи;
- данных, включающих в себя только фамилии, имена и отчества;
- в целях однократного пропуска в помещение учреждения, или в иных аналогичных целях;
- персональных данных, обрабатываемых без использования средств автоматизации.

1.5. В учреждении формируется и ведется перечень конфиденциальных данных с указанием, мест хранения и ответственных за хранение и обработку данных по форме (Приложение №1). Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, запрещается.

1.6. Основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных установлены постановлениями Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" и от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации". Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

1.7. Общие правила хранения и передачи персональных данных.

Запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении. Все сотрудники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны быть допущены к работе с соответствующими видами персональных данных.

Сотрудникам учреждения, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. После подготовки и передачи документа в соответствии с резолюцией, файлы черновиков и вариантов документа переносятся подготовившим их сотрудником на маркированные носители, предназначенные для хранения персональных данных. Без согласования с директором учреждения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

Передача персональных данных допускается только в случаях, установленных Федеральными законами Российской Федерации «О персональных данных», «О порядке рассмотрения обращений граждан Российской Федерации», действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению (резолюции) вышестоящих должностных лиц.

Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими инструкциями по работе со служебными документами и обращениями граждан.

Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

1.8. Сотрудники учреждения, осуществляющие обработку или хранение конфиденциальных данных несут ответственность за обеспечение информационной безопасности. Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных, несут дисциплинарную, административную или уголовную ответственность в соответствии с законодательством и ведомственными нормативными актами

1.9. Сотрудники учреждения и лица, выполняющие работы по договорам и контрактам, имеющие отношение к работе с персональными данными, должны быть в обязательном порядке ознакомлены под расписку с настоящей Инструкцией.

2. ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ, И УСЛОВИЯ ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должны осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных.

2.2. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к

ним доступ. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

2.3. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

2.4. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключающее одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

2.5. Использование типовых форм документов и журналов учета (при использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Оператором способов обработки персональных данных;

- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации,

- при необходимости получения письменного согласия на обработку персональных данных;

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

2.6. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещение, на котором находится Оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

- необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом Оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных в помещение, в котором находится

Оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

- копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

- персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных в помещение, в котором находится Оператор).

2.7. Порядок уничтожения или обезличивания персональных данных (уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание). Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными).

3. ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ, ПРАВИЛА ДОСТУПА, ХРАНЕНИЯ И ПЕРЕСЫЛКИ ПЕРСОНАЛЬНЫХ ДАННЫХ:

3.1. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

3.2. Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

3.3. Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

Компьютеры и(или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

3.4. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.

3.5. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

3.6. При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

- использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

- недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

- постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

3.7. При обработке персональных данных в информационной системе разработчиками и администраторами систем должны обеспечиваться:

- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

- учет лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;

- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

- описание системы защиты персональных данных.

3.8. Специфические требования по защите персональных данных в автоматизированной информационно-аналитической системе устанавливается инструкцией по ее использованию и эксплуатации.

Приложение №1
к Инструкции о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные

Министерство образования, науки и молодежи Республики Крым
Государственное бюджетное специализированное учреждение Республики Крым
«Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних»

ПЕРЕЧЕНЬ
конфиденциальных данных, обрабатываемых в ГБСУ РК «Керченский МСРЦН»

№ п/п	Наименование конфиденциальных данных и документов с персональными данными	Наименование информационной системы/без использования средств автоматизации	Место хранения (кабинет)	ФИО ответственных за обработку и хранение
1.	Паспортные данные, телефон, ИНН, СНИЛС, медицинский полис, состав семьи, льготы, данные о состоянии здоровья, о судимости, о воинском учете сотрудников.	ИСПДн – 1	Кабинет №51	Чернявская Э.С.
2.	Паспортные данные, телефон, ИНН, СНИЛС, медицинский полис, сведения о заработной плате, состав семьи, льготы, данные о состоянии здоровья, о судимости, о воинском учете сотрудников.	ИСПДн – 2	Кабинет №48	Газиева С.Я.
3	Данные свидетельства о рождении, паспортные данные воспитанников, медицинский полис, телефон, данные о состоянии здоровья воспитанников. Паспортные данные, телефон, сведения о профессиональной деятельности и образовании, сведения о доходах и составе семьи родителей (законных представителей) воспитанников	Без использования средств автоматизации	Кабинет №34	Заведующие отделениями Болкуева Э.С., Даниленко А.Г.
4	Сведения о воинском учете сотрудников	Без использования средств автоматизации	Кабинет №53	Шестакова А.Ю.
5	Личные дела, личные карточки (форма Т-2) сотрудников	Без использования средств автоматизации	Кабинет №51	Чернявская Э.С.

6	Копии документов об образовании	Без использования средств автоматизации	Кабинет №51	Чернявская Э.С.
7	Трудовые книжки сотрудников	Без использования средств автоматизации	Кабинет №51	Чернявская Э.С.
8	Приказы и основания к приказам по личному составу	Без использования средств автоматизации	Кабинет №51	Чернявская Э.С.
9	Дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации	Без использования средств автоматизации	Кабинет №51	Чернявская Э.С.
10	Копии отчетов, направляемые в органы статистики	Без использования средств автоматизации	Кабинет №48	Газиева С.Я.
11	Личные дела воспитанников	Без использования средств автоматизации	Кабинет №34	Заведующие отделениями Болкуева Э.С., Даниленко А.Г.
12	Медицинские карты воспитанников	Без использования средств автоматизации	Медицинский кабинет	

Перечень может пересматриваться по мере необходимости в соответствии с установленным порядком.

Директор ГБСУ РК «Керченский МСРЦН»

Приложение 4

Министерство образования, науки и молодежи Республики Крым
Государственное бюджетное специализированное учреждение Республики Крым
«Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних»

УТВЕРЖДЕНО
Приказом директора
ГБСУ РК «Керченский
МСРЦН» №_____
«___»_____20__ года

ИНСТРУКЦИЯ
по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных, средств защиты информации и средств криптографической защиты информации в информационной системе персональных данных ГБСУ РК «Керченский МСРЦН»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция (далее – Инструкция) по резервированию и восстановлению работоспособности технических средств (далее – ТС), программного обеспечения (далее – ПО), баз данных (далее – БД), средств защиты информации (далее – СЗИ) и средств криптографической защиты информации (далее – СКЗИ) информационной системы персональных данных (далее – АИС) в Государственном бюджетном специализированном учреждении Республики Крым «Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних» (далее – ГБСУ РК «Керченский МСРЦН») определяет действия, связанные с функционированием технических и программных средств АИС и системы защиты персональных данных (далее – СЗПДн).

1.2. Настоящая инструкция разработана в соответствии с руководящими и нормативными документами регуляторов Российской Федерации в области защиты персональных данных.

1.3. Целью данной инструкции является превентивная защита элементов АИС и СЗПДн от предотвращения потери защищаемой информации.

1.4. Задачами данной инструкции являются:

- определение мер защиты от потери информации;
- определение действий восстановления технических и программных средств АИС и СЗПДн в случае потери информации.

1.5. Действие настоящей инструкции распространяется на всех пользователей, имеющих доступ к ресурсам АИС, в том числе на ответственного за обеспечение безопасности персональных данных информационных систем персональных данных ГБСУ РК «Керченский МСРЦН» и администратора АИС (далее – администратор системы), имеющих доступ к техническим и программным средствам СЗПДн в рамках своих полномочий, при возникновении аварийных ситуаций, в том числе:

- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

1.6. Пользователем АИС (далее – Пользователь) является сотрудник ГБСУ РК «Керченский МСРЦН», участвующий в рамках выполнения своих функциональных обязанностей в процессах

автоматизированной обработки персональных данных (далее – ПДн) и имеющий доступ к аппаратным средствам, программному обеспечению, данным и СЗИ АИС.

1.7. Под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов АИС или СЗПДн, предоставляемых пользователям, а также потерей защищаемой информации.

2. ПОРЯДОК РЕАГИРОВАНИЯ НА ИНЦИДЕНТ

2.1. Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств АИС и СЗПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.2. Все действия в процессе реагирования на Инцидент должны документироваться ответственным за обеспечение безопасности персональных данных информационных систем персональных данных ГБСУ РК «Керченский МСРЦН» и администратором системы в «Журнал учета событий информационной безопасности» (Приложение 1).

2.3. В кратчайшие сроки, не превышающие одного рабочего дня ответственный за обеспечение безопасности персональных данных информационных систем персональных данных ГБСУ РК «Керченский МСРЦН» и администратор системы предпринимают меры по восстановлению работоспособности.

2.4. Предпринимаемые меры, по возможности, согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена с целью получения высококвалифицированной консультации в кратчайшие сроки.

3. ТЕХНИЧЕСКИЕ МЕРЫ

3.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы жизнеобеспечения АИС;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

3.2. Системы жизнеобеспечения АИС включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

3.3. Все критичные помещения ГБСУ РК «Керченский МСРЦН» (помещения, в которых размещаются элементы АИС и СЗПДн) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.4. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств АИС в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

3.5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы АИС и СЗПДн, сетевое и коммуникационное оборудование, а также наиболее критичные АРМ должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

- дублированные системы электропитания в устройствах (серверы, активное сетевое оборудование и т. д.);

- резервные линии электропитания в пределах комплекса зданий;

- аварийные электрогенераторы.

3.6. Системы обеспечения отказоустойчивости:

- кластеризация;

- технология RAID.

3.7. Для обеспечения отказоустойчивости критичных компонентов АИС при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации.

3.8. Для наиболее критичных компонентов АИС должны использоваться территориально удаленные системы кластеров.

3.9. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

3.10. Система резервного копирования и хранения данных должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

4. ОРГАНИЗАЦИОННЫЕ МЕРЫ

4.1. Резервное копирование и хранение данных должно осуществляться на периодической основе:

- для обрабатываемых ПДн – согласно инструкции по обеспечению безопасности ПДн;

- для технологической информации – не реже раза в месяц;

- эталонные копии программного обеспечения (ОС, штатное и специальное ПО, программные СЗИ), с которых осуществляется их установка на элементы АИС – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

4.2. Данные о проведении процедуры резервного копирования должны отражаться в специально созданном журнале учета.

4.3. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

4.4. Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

4.5. Носители должны храниться не менее года для возможности восстановления данных.

Приложение 1
к инструкции по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных, средств защиты информации и средств криптографической защиты информации в информационной системе персональных данных

Министерство образования, науки и молодежи Республики Крым
Государственное бюджетное специализированное учреждение Республики Крым
«Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних»

ЖУРНАЛ
учета событий информационной безопасности

Начат «__» _____ 20__ г.
Окончен «__» _____ 20__ г.

№ п/п	Дата события	Основание возникновения события	Описание события (мероприятия)	Характеристика события	(ФИО, субъекта)	Должность, ФИО и подпись ответственного за ведение журнала	Примечание

Приложение 5

Министерство образования, науки и молодежи Республики Крым
Государственное бюджетное специализированное учреждение Республики Крым
«Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних»

УТВЕРЖДЕНО
Приказом директора
ГБСУ РК «Керченский
МСРЦН» №_____
«___»_____20__ года

ИНСТРУКЦИЯ
пользователя информационной системы персональных данных при возникновении нештатных ситуаций в ГБСУ РК «Керченский МСРЦН»

1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием информационных систем персональных данных ГБСУ РК «Керченский МСРЦН» (далее – ИСПДн), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

2. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания работоспособности в случае реализации рассматриваемых угроз.

3. Задачами данной Инструкции являются:

- определение мер защиты от прерывания работоспособности;
- определение действий по восстановлению в случае прерывания работоспособности.

4. Действие настоящей Инструкции распространяется на всех пользователей ИСПДн, имеющих доступ к ресурсам ИСПДн, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

5. Под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в Приложении № 1.

6. При реагировании на инцидент важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

- Уровень 1. Незначительный инцидент – локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты;
- Уровень 2. Авария – любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты;
- Уровень 3. Катастрофа – любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, к уничтожению, блокированию, неправомерной модификации или компрометации защищаемых персональных данных, а также к угрозе жизни пользователей ИСПДн.

7. При возникновении нештатной ситуации любого уровня пользователь обязан оповестить ответственного за организацию обработки персональных данных, сообщив характер аварийной ситуации, масштаб ситуации по предварительной субъективной оценке.

8. Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за организацию обработки персональных данных в Журнале учета событий информационной безопасности.

В кратчайшие сроки, не превышающие одного рабочего дня, должны быть предприняты меры по восстановлению работоспособности ИСПДн.

9. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные (программно-аппаратные) и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Все критичные помещения, в которых размещаются элементы ИСПДн и средства защиты, должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Порядок предотвращения потерь информации и организации восстановления ИСПДн описан в Инструкции по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных, средств защиты информации и средств криптографической защиты информации в информационной системе персональных данных.

10. Ответственный за организацию обработки персональных данных:

- ознакомляет всех сотрудников, находящихся в его зоне ответственности, с данной инструкцией в срок, не превышающий 3х рабочих дней с момента выхода нового сотрудника на работу;
- обучает пользователей, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций.

Пользователи ИСПДн должны получить базовые знания в следующих областях:

- оказание первой медицинской помощи;
- пожаротушение;
- эвакуация людей;
- защита материальных и информационных ресурсов;
- методы оперативной связи со службами спасения и руководителями структурных подразделений;
- выключение оборудования, электричества, водоснабжения, газоснабжения;
- по окончанию ознакомления сотрудников получает их роспись в Журнале проведения инструктажа по информационной безопасности.

11. Навыки и знания пользователей ИСПДн по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение пользователей ИСПДн порядку действий при возникновении аварийной ситуации.

Ответственность за организацию обучения пользователей ИСПДн несет ответственный за организацию обработки персональных данных. Директор ГБСУ РК «Керченский МСРЦН» согласовывает сроки и порядок их обучения.

Приложение 1
к инструкции пользователя ИСПДн
при возникновении нештатной ситуации

Источники угроз безопасности персональных данных

Технологические угрозы:
- Пожар в здании;
- Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения);
- Взрыв (бытового газа, взрывчатых веществ или приборов, работающих под давлением);
- Химический выброс в атмосферу.

Внешние угрозы:
- Массовые беспорядки;
- Сбои общественного транспорта;
- Эпидемия;
- Массовое отравление персонала;
- Теракт.

Стихийные бедствия:
- Удар молнии;
- Сильный снегопад;
- Сильные морозы;
- Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания;
- Затопление водой в период паводка;
- Наводнение, вызванное проливным дождем;
- Торнадо;
- Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод).

ИТ-угрозы:
- Сбой системы кондиционирования в серверном помещении;
- Выход из строя файлового сервера;
- Частичная потеря информации на сервере без потери его работоспособности;
- Выход из строя локальной сети;
- Выход из строя рабочей станции;
- Частичная потеря информации на рабочей станции без потери её работоспособности.

Угроза, связанная с человеческим фактором:
- Ошибка персонала, имеющего доступ к элементам ИСПДн;
- Нарушение конфиденциальности, целостности и доступности конфиденциальной информации, а также несанкционированные действия, заблокированные средствами защиты и зафиксированные средствами регистрации.

Угрозы, связанные с внешними поставщиками:
- Отключение электроэнергии;
- Сбой в работе интернет-провайдера;
- Физический разрыв внешних каналов связи.

Приложение 6

Министерство образования, науки и молодежи Республики Крым
Государственное бюджетное специализированное учреждение Республики Крым
«Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних»

УТВЕРЖДЕНО
Приказом директора
ГБСУ РК «Керченский
МСРЦН» №_____
«___»_____20__ года

ИНСТРУКЦИЯ
по проведению инструктажа лиц, допущенных к работе с информационной системой персональных данных ГБСУ РК «Керченский МСРЦН»

1. Настоящая инструкция разработана с целью обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных Государственного бюджетного специализированного учреждения Республики Крым «Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних» (далее - ИСПДн).

2. При поступлении на работу сотрудника, которому для выполнения своих трудовых обязанностей необходим доступ к ИСПДн (далее - новый сотрудник), ответственный за организацию обработки персональных данных:

- в соответствии с п.6 ч.1 ст.18.1 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» проводит ознакомление нового сотрудника с положениями законодательства Российской Федерации о персональных данных и локальными актами учреждения в отношении обработки персональных данных (Приложение 1).
- знакомит нового сотрудника с ответственностью за неисполнение требований по обеспечению безопасности персональных данных в ИСПДн, предусмотренной действующим законодательством Российской Федерации;
- отмечает в Журнале учета проведения инструктажей по информационной безопасности и персональным данным данные о проведении первичного инструктажа.

3. Новый сотрудник может приступить к исполнению своих непосредственных трудовых обязанностей, связанных с обработкой персональных данных, только после успешного прохождения инструктажа.

Приложение 1
к инструкции по проведению инструктажа
лиц, допущенных к работе с информационной
системой персональных данных

Перечень законодательных актов Российской Федерации о персональных данных, документов, определяющих требования к защите персональных данных, внутренних локальных актов, определяющих политику учреждения в отношении обработки персональных данных, с которыми необходимо ознакомить нового сотрудника при проведении инструктажа.

Законодательные акты Российской Федерации о персональных данных:

1) Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (ред. от 21.07.2014).

2) Постановление Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3) Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (для сотрудников, обрабатывающих персональные данные в том числе без использования средств автоматизации).

Внутренние локальные акты:

1) Политика обработки персональных данных.
2) Концепция информационной безопасности информационных систем персональных данных.
3) Положение об организации защиты персональных данных.
4) Положение об информационной безопасности.
5) Положение об использовании сети интернет.
6) Положение о защите детей от информации, причиняющей вред их здоровью и развитию.
7) Положение о комиссии по классификации информационных систем персональных данных.
8) Положение о порядке хранения и уничтожения носителей персональных данных.
9) Правила использования сети Интернет.
10) Положение об официальном сайте.
11) Приказ «О назначении лица, ответственного за организацию обработки персональных данных».
12) Инструкция администратора точки доступа к сети Интернет.
13) Инструкция пользователя, ответственного за использование криптосредств.
14) Инструкция по обеспечению безопасности эксплуатации средств криптографической защиты информации.
15) Инструкция администратора безопасности информационной системы персональных данных.
16) Инструкция пользователя информационной системы персональных данных.
17) Инструкция пользователя по обеспечению безопасности персональных данных.
18) Инструкция по организации парольной защиты в информационных системах.
19) Инструкция пользователя средств криптографической защиты информации в Организации.
20) Инструкция по организации антивирусной защиты информационных систем.
21) Инструкция специалиста по правилам обработки, хранения и передачи персональных данных.

22) Инструкция по проведению антивирусного контроля в информационной системе персональных данных.

23) Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные.

24) Инструкция по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных, средств защиты информации и средств криптографической защиты информации в информационной системе персональных данных.

25) Инструкция пользователя информационной системы персональных данных при возникновении нештатных ситуаций.

26) Инструкция по проведению инструктажа лиц, допущенных к работе с информационной системой персональных данных.

27) Перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним.

28) Типовые формы согласия на обработку персональных данных.

29) Перечень персональных данных, обрабатываемых в ГБСУ РК «Керченский МСРЦН».

30) Журнал поэкземплярного учета средств криптографической защиты информации (СКИЗ).

31) Журнал ежедневной выдачи средств криптографической защиты информации (СКИЗ)

32) Журнал проведения инструктажей по информационной безопасности и защите персональных данных.

33) Журнал учета событий информационной безопасности.

Настоящий перечень может дополняться и корректироваться в зависимости от принятых законодательных актов Российской Федерации и утвержденных в учреждении новых локальных актов по информационной безопасности и защите персональных данных.

Приложение 7

Министерство образования, науки и молодежи Республики Крым
Государственное бюджетное специализированное учреждение Республики Крым
«Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних»

УТВЕРЖДЕНО
Приказом директора
ГБСУ РК «Керченский
МСРЦН» №_____
«___»_____20__ года

ПЕРЕЧЕНЬ
по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним в ГБСУ РК «Керченский МСРЦН»

Перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним, составляется на основании Отчета о результата проведения внутренней проверки обеспечения защиты персональных данных.

Требования к техническим средствам защиты описаны в Положении об информационной безопасности, раздел 5.

В Перечне должна содержаться следующая информация:
- название средства защиты.
- эксплуатационная информация.
- техническая документация.

Перечень по учету технических средств защиты информации, эксплуатационной и технической документации к ним, составляется для каждой ИСПДн (Приложение №1).

Перечень должен поддерживаться в актуальном состоянии

Приложение №1 ИСПДн <u>АИС «1С: Предприятие: Бухгалтерия, Зарплата + Кадры»</u>

Перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации

Техническое средство	Эксплуатационная информация	Техническая документация
Средство защиты СЗИ от НДС «Secret Net Studio»	Средство защиты настроено на: - защиту входа в систему; - защиту информации от несанкционированного доступа; - контроль утечек и каналов распространения защищаемой информации; - антивирусную защиту; - межсетевое экранирование; - защиту от сетевых атак	Журнал настроек Межсетевого экрана хранится 52 каб.
Антивирусная защита «Kaspersky Endpoint Security для Windows (версия 11.0.0.6499)	Антивирус настроен на: - резидентный антивирусный мониторинг; - ежедневное антивирусное сканирование;	

	- скрипт-блокирование;	
Межсетевой экран СКЗИ ПК «ViPNet Client 4»	Межсетевой экран настроен на: - фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов; - блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату. - «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации» - по 3 классу защищенности; - «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» - по 4 уровню контроля; - «Требования к системам обнаружения вторжений» – по 4 классу защиты.	Инструкция по установке и настройке от производителя. Руководство администратора Журнал настроек Межсетевого экрана хранится 52 каб.

Приложение 8

Министерство образования, науки и молодежи Республики Крым
Государственное бюджетное специализированное учреждение Республики Крым
«Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних»

УТВЕРЖДЕНО
Приказом директора
ГБСУ РК «Керченский
МСРЦН» №_____
«___»_____20__ года

ЖУРНАЛ
проведения инструктажей
по информационной безопасности и защите персональных данных

Начат:_____
Окончен:_____

№ п/п	Дата проведения инструктажа	Вид инструктажа	Ф.И.О. инструктируемого работника	ФИО должностного лица, проводившего инструктаж	Подпись	
					инструктирующего	инструктируемого