Приложение к приказу
№160-а от 17.11.2017
УТВЕРЖДАЮ:
Директор МУ КЦСОН ЯМР
«Золотая осень»
_____ О.В.Николаева
«17» ноября 2017г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Муниципального учреждения комплексного центра социального обслуживания населения Ярославского муниципального района «Золотая осень»

2017г.

Оглавление

Определения

В настоящем документе используются следующие термины и их определения.

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

Аутентификация отправителя данных - подтверждение того, что отправитель полученных данных соответствует заявленному.

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.

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

Блокирование 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.

Вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные 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 её 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 - электрические сигналы, 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.

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.

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.

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

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

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

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.

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.

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, другая информация.

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.

Политика «чистого стола» - комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

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.

Раскрытие персональных данных - умышленное или случайное нарушение конфиденциальности персональных данных.

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.

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

Специальные категории персональных данных - персональные данные, касающиеся расовой, 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.

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.

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

1. Общие положения

Настоящая Политика информационной безопасности (далее – Политика) МУ КЦСОН ЯМР «Золотая осень» 150522, Ярославская область, Ярославский район, р.п. Красные Ткачи, ул. Первомайская, д. 14а, разработана администратором безопасности и является официальным документом.

Политика разработана в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказом ФСБ России от 10 июля 2014 г. N 378 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством РФ требований к защите ПДн для каждого из уровня защищенности».

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности.

Целью настоящей Политики является обеспечение безопасности объектов защиты МУ КЦСОН ЯМР «Золотая осень» от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности.

Защите подлежит вся циркулирующая в ИС МУ КЦСОН ЯМР «Золотая осень» информация. Защита общедоступной информации производится только в целях обеспечения ее целостности, доступности и аутентичности.

Цель защиты информации в ИС МУ КЦСОН ЯМР «Золотая осень» достигается решением следующих задач:

– реализация комплекса мер по предотвращению противоправного получения информации МУ КЦСОН ЯМР «Золотая осень» или ее несанкционированной передачи (распространения);

– своевременное обнаружение фактов несанкционированного доступа к информации и предотвращение неавторизованного (неполномочного) воздействия на информационные ресурсы;

– недопущение воздействия на технические средства обработки и хранения информации, нарушающего их функционирование;

– предупреждение неблагоприятных последствий нарушения порядка доступа к информации;

– обеспечение восстановления в приемлемые сроки информации после не предусмотренной технологией ее обработки модификации, в том числе и уничтожения.

Объекты и мероприятия защиты информации

Защите подлежат:

– техническое и программное обеспечение автоматизированной информационной системы МУ КЦСОН ЯМР «Золотая осень»

– информационно-телекоммуникационная сеть МУ КЦСОН ЯМР «Золотая осень»;

– информационные ресурсы, представленные в виде носителей на различной физической основе информационных массивов и баз данных;

– помещения, в которых размещаются носители или средства обработки защищаемой информации;

– все технические средства и системы, размещенные в помещениях, в которых обрабатывается (циркулирует) информация ограниченного доступа;

– система защиты информации.

Выполнение задач защиты информации в ИС учреждения обеспечивается организацией эффективной системы защиты информации – комплексным применением организационных и технических (программно и аппаратно реализуемых) мероприятий:

– созданием системы нормативных (руководящих) документов по организации защиты;

– четким распределением ответственности в вопросах защиты информации между сотрудниками МУ КЦСОН ЯМР «Золотая осень»;

– установлением персональной ответственности сотрудников МУ КЦСОН ЯМР «Золотая осень» за обеспечение безопасности обрабатываемой информации;

– организацией выполнения сотрудниками МУ КЦСОН ЯМР «Золотая осень» требований нормативных документов по защите информации;

– юридической защитой безопасности информации при ее предоставлении сторонним организациям;

– своевременным выявлением угроз безопасности информации и принятием соответствующих мер защиты;

– комплексным применением программно и аппаратно реализованных средств защиты информации от несанкционированного доступа к ней и от специальных воздействий на информационные ресурсы в целях их уничтожения, искажения, блокирования или фальсификации;

– содержанием актуальных резервных копий информационных ресурсов;

– систематическим анализом безопасности информации и совершенствованием системы её защиты;

– эффективной противопожарной защитой;

– глубоким знанием и пониманием сотрудниками требований безопасности информации.

Применение технических средств защиты информации в МУ КЦСОН ЯМР «Золотая осень» основано на принципах безопасности, правомочности и эффективности.

2. Область действия

Требования настоящей Политики распространяются на всех сотрудников МУ КЦСОН ЯМР «Золотая осень» (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.). Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

3. Система защиты персональных данных

Система защиты персональных данных (СЗПДн), строится на основании:

– обследования ИС;

– перечня персональных данных, обрабатываемых в МУ КЦСОН ЯМР «Золотая осень»;

– модели угроз безопасности ИС ПДн;

– Положения о защите конфиденциальной информации в МУ КЦСОН ЯМР «Золотая осень»;

– руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн ИСПДн МУ КЦСОН ЯМР «Золотая осень». На основании анализа актуальных угроз безопасности ПДн, описанного в Модели угроз и Обследования ИС, делается заключение

о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

Для ИСПДн должен быть составлен список используемых технических средств защиты, а так же программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей;
- сервера приложений;
- граница ЛВС;
- каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз СЗПДн может включать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевого экранирования;
- средства криптографической защиты информации при передаче защищаемой информации по каналам связи.

Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн, операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечение целостности данных.

Список используемых средств должен поддерживаться в актуальном состоянии.

4. Требования к подсистемам СЗПДн

Подсистемы СЗПДн имеют различный функционал в зависимости от класса защищенности, определённого в Акте классификации для ИСПДн. ИСПДн МУ КЦСОН ЯМР «Золотая осень» имеет 4-й уровень защищенности. СЗПДн может включать в себя следующие подсистемы:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- антивирусная защита;

– защита технических средств;

– защита информационной системы, ее средств, систем связи и передачи данных.

4.1. Подсистема идентификация и аутентификация субъектов доступа и объектов доступа

Подсистема идентификация и аутентификация субъектов доступа и объектов доступа предназначена для реализации следующих функций:

– идентификация и аутентификация пользователей, являющихся сотрудниками;

– управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;

– управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;

– защита обратной связи при вводе аутентификационной информации;

– идентификация и аутентификация пользователей, не являющихся сотрудниками (внешних пользователей).

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

4.2. Подсистема управления доступом субъектов доступа к объектам доступа

Подсистема управления доступом субъектов доступа к объектам доступа предназначена для реализации следующих функций:

– управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;

– реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;

– управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;

– разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;

– назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

4.3. Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для реализации следующих функций:

– реализация антивирусной защиты;

– обновление базы данных признаков вредоносных компьютерных программ (вирусов).

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ, либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

4.4. Подсистема защиты технических средств

Подсистема защиты технических средств предназначена для реализации следующих функций:

– контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены;

– размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, обеспечивать защиту технических средств от внешних воздействий, а также

защиту персональных данных, представленных в виде информативных электрических сигналов.

4.5. Подсистема защиты информационной системы, ее средств, систем связи и передачи данных

Подсистема защиты информационной системы, ее средств, систем связи и передачи данных предназначена для реализации обеспечения защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

Для обеспечения 4-го уровня защищенности персональных данных применяются:

- средства вычислительной техники не ниже 6 класса;
- средства антивирусной защиты не ниже 5 класса;
- межсетевые экраны 5 класса.

5. Система защиты ИСПДн

Для предотвращения угроз безопасности электронной корреспонденции, содержащей информацию, составляющую конфиденциальную информацию, пользователи должны использовать средства криптографической защиты информации, включая возможность шифрования и возможность электронной подписи.

Используемые средства криптографической защиты конфиденциальной информации должны быть сертифицированы.

Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством РФ требований к защите ПДн для 4-го уровня защищенности:

Доступ в помещения:

- оснащения помещений входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода;

- оснащение помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений;

- утверждения правил доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях;

- утверждения перечня лиц, имеющих право доступа в помещения.

Сохранность носителей Пдн:

- осуществлять хранение съемных машинных носителей персональных данных в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов);

- осуществлять поэкземплярный учет машинных носителей персональных данных, который достигается путем ведения журнала учета носителей персональных данных с использованием регистрационных (заводских) номеров.

Определение перечня допущенных лиц:

- разработать и утвердить документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- поддерживать в актуальном состоянии документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей.

6. Требования к персоналу по обеспечению защиты ПДн

Все сотрудники МУ КЦСОН ЯМР «Золотая осень», являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн. При вступлении в должность нового сотрудника ответственный за безопасность сотрудник обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн. Сотрудник должен быть ознакомлен со сведениями настоящей Политики и принятыми процедурами работы с элементами ИС ПДн и СЗ ПДн.

Сотрудники МУ КЦСОН ЯМР «Золотая осень», использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов

(электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники МУ КЦСОН ЯМР «Золотая осень» должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники МУ КЦСОН ЯМР «Золотая осень» должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать и использовать потенциально – опасное программное обеспечение (Torrent – клиенты, Skype), подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами МУ КЦСОН ЯМР «Золотая осень» третьим лицам.

При работе с ПДн в ИСПДн сотрудники МУ КЦСОН ЯМР «Золотая осень», обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ.

При завершении работы с ИСПДн сотрудники обязаны защитить АРМ с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники МУ КЦСОН ЯМР «Золотая осень» должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, которые могут повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, директору или ответственному за безопасность сотруднику.

7. Рекомендации к помещениям, в которых обрабатываются ПДн

Доступ в помещения, в которых располагаются средства обработки ПДн, должен контролироваться. Не допускается бесконтрольное пребывание не допущенных к работе с ПДн лиц в данных помещениях.

Сетевое оборудование следует располагать в местах, недоступных для посторонних лиц (в специальных помещениях, шкафах, коробах).

Уборка помещений и обслуживание технических средств ИСПДн должна осуществляться только авторизованным персоналом с соблюдением мер, исключающих несанкционированный доступ к ПДн, носителям информации, программным и техническим средствам обработки, передачи и защиты информации ИСПД.

Помещения, в которых располагаются технические средства ИСПДн, должны быть подключены к системе гарантированного энергоснабжения с целью обеспечения высококачественного бесперебойного электропитания ИСПД.

7.1.Системы безопасности зданий (помещений)

В целях защиты от несанкционированного доступа к информации в МУ КЦСОН ЯМР «Золотая осень» создается контролируемая зона.

Охрана контролируемой зоны организуется в целях предотвращения доступа в нее посторонних лиц, а также создания надежных препятствий для несанкционированного проникновения в помещения МУ КЦСОН ЯМР «Золотая осень».

Помещения имеют прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. Окна оборудованы металлическими решетками, охранной сигнализацией, жалюзи, препятствующими неконтролируемому проникновению в помещения, а также просмотра посторонними лицами ведущихся там работ.

В целях повышения эффективности охраны помещения МУ КЦСОН ЯМР «Золотая осень» оборудуются системами безопасности:

- системой пожарной сигнализации;
- системой охранной и тревожной сигнализации;

7.1.1. Охранная сигнализация.

Охранная сигнализация предназначается для обеспечения своевременного выявления попыток несанкционированного проникновения в помещения и выдачи сигнала тревоги в случае несанкционированного проникновения в помещение, находящееся под охраной.

Охранная сигнализация должна обеспечить надежное и быстрое срабатывание извещателей с достаточной для принятия немедленных мер локализацией места проникновения, самодиагностику и возможность работы от автономного источника электроэнергии.

Системой охранной сигнализации оборудуются все помещения МУ КЦСОН ЯМР «Золотая осень».

7.1.2. Пожарная сигнализация.

Помещения МУ КЦСОН ЯМР «Золотая осень» оборудуются системами пожарной сигнализации в целях своевременного обнаружения очага возгорания и своевременного принятия мер по тушению пожара.

Пожарная сигнализация должна обеспечить надежное и быстрое срабатывание извещателей с достаточной для принятия немедленных мер локализацией места возникновения пожара, самодиагностику и возможность работы от автономного источника электроэнергии.

При повседневном режиме электроснабжения системы охранной и пожарной сигнализации должны функционировать круглосуточно (непрерывно).

Устанавливаемое оборудование и сети систем должны быть безопасны при эксплуатации для лиц, соблюдающих правила обращения с ними.

8. Должностные обязанности пользователей ИСПДн

Сотрудники, допущенные к работе с ИСПДн, обязаны выполнять требования инструкций, принятых и утвержденных в МУ КЦСОН ЯМР «Золотая осень»:

- Политика обработки персональных данных;
- Положение об обработке ПДн;
- Перечень ПДН, обрабатываемых в учреждении;
- Перечень целей и сроков обработки ПДн в учреждении;
- Инструкция пользователя информационной системы Пдн;
- Инструкция пользователя автоматизированной системы;
- Инструкция по проведению антивирусного контроля в автоматизированной системе;
- Порядок обращения с идентификационной и аутентификационной информацией;
- Инструкция по работе со съемными носителями, содержащими конфиденциальную информацию, в том числе и персональные данные.

9. Ответственность сотрудников

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

Сотрудники МУ КЦСОН ЯМР «Золотая осень» несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками МУ КЦСОН ЯМР «Золотая осень» – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.