Приложение
утверждено приказом
директора
РГБУ «СШ по лёгкой атлетике
«Спартак»
от «17» 03 2020 г.
№ 2102

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных

Определения

В настоящем документе используются следующие термины и определения:

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.

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 к информации - возможность получения информации и ее использования.

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.

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

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.

Не декларированные 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.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение,

предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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.

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

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

Обозначения и сокращения

АРМ – автоматизированное рабочее место
ИСПДн – информационная система персональных данных
ИС– информационная система
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПО – программное обеспечение
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
СФ СЗПДн – среда функционирования системы (подсистемы) защиты персональных данных
УБПДн – угрозы безопасности персональных данных

Введение

Модель угроз безопасности персональных данных (далее – Модель) при их обработке в ИСПДн в государственном бюджетном учреждении социального обслуживания «Лермонтовский комплексный центр социального обслуживания населения»
строится на основании отчета о результатах проведения внутренней проверки.

В модели угроз представлено описание структуры ИСПДн, состава и режима обработки ПДн, классификация потенциальных нарушителей, оценка исходного уровня защищенности, анализ угроз безопасности персональных данных.

Анализ УБПДн включает:

- Описание угроз;
- Оценку вероятности возникновения угроз;
- Оценку реализуемости угроз;
- Оценку опасности угроз;
- Определение актуальности угроз.

Тип нарушителя

- Исходя из предположений о возможностях нарушителя его следует отнести к типу Н1.

Таким образом, для обеспечения безопасности персональных данных в ИСПДн «Региональная медицинская информационная система» необходимо использовать средства криптографической защиты информации уровня не ниже КС1.

Угроза безопасности персональных данных для информационных систем персональных

Угроза безопасности персональных данных при их обработке в информационных системах персональных данных «1С «Бухгалтерия» Зарплата и кадры», «1С Бухгалтерия» Бюджетного учреждения», « «Контур –Экстерн», строится на основании следующих документов:

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 года);
2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.).

В модели угроз представлены характеристики информационных систем персональных данных (ИСПДн) Учреждения, состав и режим обработки персональных данных (ПДн), классификация потенциальных нарушителей, оценка исходного уровня защищенности, анализ угроз безопасности персональных данных (УБПДн).

Описание информационных систем персональных данных

Описание информационной системы «1С «Бухгалтерия» Зарплата и кадры»

Информационная система развернута на четырех компьютерах. Компьютеры имеют подключения к локальной сети и выход в сеть Интернет. Обработка персональных данных осуществляется в программах «1С Бухгалтерия», «Microsoft Office». Операционная система – «Windows 7», «Windows XP».

Описание информационной системы «1С Бухгалтерия» Бюджетного учреждения»

Информационная система развернута на трех компьютерах. Компьютеры имеют подключения к локальной сети и выход в сеть Интернет. Обработка

персональных данных осуществляется в программах «Microsoft Office», «1С Бухгалтерия». Операционная система – «Windows 7».

Описание информационной системы «Контур- Экстерн »

Информационная система развернута на трех компьютерах.
Компьютеры имеют подключение к локальной сети и выход в сеть Интернет.
Обработка персональных данных осуществляется в программах «Microsoft Office»,
Операционная система – «Windows 7», «Windows XP».

Определение угроз безопасности персональных данных Классификация нарушителей

По признаку принадлежности к ИСПДн все нарушители делятся на две группы:

1. Внешние нарушители – физические лица, не имеющие права пребывания в пределах контролируемой территории, где размещается оборудование ИСПДн;
2. Внутренние нарушители – физические лица, имеющие право пребывания в пределах контролируемой территории, где размещается оборудование ИСПДн.

Внешний нарушитель

Внешние нарушители имеют возможности:

1. Воздействовать на защищаемую информацию по техническим каналам утечки информации;
2. Осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
3. Осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и сетям международного информационного обмена;
4. Осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
5. Осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;
6. Осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИСПДн.

Предполагается, что выявленные внешние нарушители не могут получать доступ к защищаемой информации и воздействовать на нее по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИСПДн, является недостаточным для возможной мотивации внешних нарушителей к осуществлению указанных действий.

Таким образом, выявленные внешние нарушители могут воздействовать на защищаемую информацию всеми перечисленными выше способами, за исключением действий, направленных на утечку и искажение конфиденциальной информации по техническим каналам.

Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой

профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа к защищаемой информации.

Предположения об имеющейся у нарушителя информации об объектах реализации угроз

В качестве основных уровней знаний нарушителей об ИСПДн можно выделить следующие:

1. Общая информация – информация о назначениях и общих характеристиках ИСПДн;

2. Эксплуатационная информация – информация, полученная из эксплуатационной документации;

3. Чувствительная информация – информация, дополняющая эксплуатационную информацию об ИСПДн (например, сведения из проектной документации ИСПДн).

В частности, нарушитель может иметь:

1. Данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн;

2. Сведения об информационных ресурсах ИСПДн: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;

3. Данные об уязвимостях, включая данные о недокументированных (не декларированных) возможностях технических, программных и программно- технических средств ИСПДн;

4. Данные о реализованных в СЗИ принципах и алгоритмах; 5. Сведения о возможных каналах реализации угроз;

5. Информацию о способах реализации угроз.

Степень информированности нарушителя зависит от многих факторов, включая реализованные в Учреждения конкретные организационные меры и компетенцию нарушителей.

В связи с изложенным, предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз.

Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель имеет:

1. Аппаратные компоненты ИСПДн и СЗИ;
2. Доступные в свободной продаже технические средства и программное обеспечение;
3. Специально разработанные технические средства и программное обеспечение.
4. Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные в Учреждения конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Так как специальные средства, используемые для реализации угроз утечки информации по техническим каналам, отсутствуют в свободной продаже, предполагается, что потенциальные нарушители **не имеют**:

1. Средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ) на ИСПДн;
2. Средств воздействия на источники питания и через цепи питания;
3. Средств воздействия через цепи заземления;
4. Средств активного воздействия на технические средства (средств облучения).

Предполагается, что нарушитель обладает совершенными средствами реализации угроз.

Исходный уровень защищенности информационной системы персональных данных

Под исходным уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y1).

В Таблице 1 представлены характеристики уровня исходной защищенности для ИСПДн Учреждения.

Таблица 1

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности
По территориальному размещению Локальная ИСПДн, развернутая в пределах одного здания	Высокий
По наличию соединения с сетями общего пользования: ИСПДн, имеющая одноточечный выход в сеть общего пользования;	Средний
По встроенным (легальным) операциям с записями баз персональных данных Модификация, передача	Низкий

По разграничению доступа к персональным данным ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	Средний
По наличию соединений с другими базами ПДн иных ИСПДн ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	Высокий
По уровню обобщения (обезличивания) ПДн ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	Низкий
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки ИСПДн, предоставляющая часть ПДн;	Средний

Перечень действующих угроз на информационную систему и их актуальность

Кража ПЭВМ

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн.

Имеющиеся средства защиты

- Физическая охрана. В ночное время дежурит сторож, в дневное время специалист ; - Посетители регистрируются в журнале.
- Система видеонаблюдения.
- Кабинеты, в которых расположены элементы ИСПДн, запираются.

Опасность - Высокая Вероятность реализации - Низкая Актуальность - Актуальна

Кража носителей информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации.

Имеющиеся средства защиты

- Физическая охрана. В ночное время дежурит сторож; в дневное время назначенный специалист - Посетители регистрируются в журнале.
- Система видеонаблюдения.
- Кабинеты, в которых расположены элементы ИСПДн, запираются.
- Инструкция по работе со съемными носителями, регламентирующая правила безопасной работы с съемными носителями конфиденциальной информации.

Опасность - Высокая Вероятность реализации - Низкая Актуальность - Актуальна

Кража ключей и паролей доступа внутренними и внешними нарушителями

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн.

Имеющиеся средства защиты

- Инструкция пользователя ИСПДн, запрещающая хранение паролей доступа на бумажных или электронных носителях без соответствующей защиты от несанкционированного доступа к ним.

Опасность - Средняя Вероятность реализации - Низкая Актуальность - Актуальна

Кража, модификация, уничтожение информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

Имеющиеся средства защиты

- Разрешительная система доступа (организационная мера) к информационным ресурсам.

Опасность - Высокая Вероятность реализации - Низкая Актуальность - Актуальна

Несанкционированное отключение средств защиты

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты всех ИСПДн.

Имеющиеся средства защиты

- Инструкция пользователя ИСПДн;
- Инструкция по антивирусной защите;
- Блокировка отключения антивирусной защиты системой централизованного управления средствами антивирусной защиты на компьютерах пользователей.

Опасность - Средняя
Вероятность реализации - Маловероятно
Актуальность - Неактуальна

Действия вредоносных программ (вирусов)

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

- скрывать признаки своего присутствия в программной среде компьютера;

-обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти; разрушать (искажать произвольным образом) код программ в оперативной памяти;

-выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.); □ сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

-искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Имеющиеся средства защиты - Антивирус Касперского.

Опасность - Средняя Вероятность реализации - Низкая Актуальность – Актуальна

Установка ПО не связанного с исполнением служебных обязанностей

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов.

Имеющиеся средства защиты

- Инструкция пользователя ИСПДн, запрещающая пользователям самостоятельную установку стороннего программного обеспечения.

Опасность - Низкая

Вероятность реализации - Средняя
Актуальность – Неактуальна

Утрата паролей доступа к ИСПДн

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политики в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

Имеющиеся средства защиты

- Инструкция по парольной защите, устанавливающая правила использования и хранения паролей.

Опасность - Средняя Вероятность реализации - Средняя Актуальность – Актуальна

Непреднамеренное отключение средств защиты

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и средствами защиты или не осведомлены о них. Имеющиеся средства защиты

- Инструкция пользователя ИСПДн.
- Блокировка отключения антивирусной защиты системой централизованного управления средствами антивирусной защиты на компьютерах пользователей

Опасность - Средняя Вероятность реализации - Низкая Актуальность - Неактуальна

Разглашение, модификация, уничтожение информации сотрудниками, допущенными к ее обработке

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн.

Имеющиеся средства защиты

- Инструкция пользователя ИСПДн, регламентирующая работу с персональными данными.

Опасность - Высокая Вероятность реализации - Средняя Актуальность – Актуальна

Перехват информации за пределами контролируемой зоны

Угроза осуществляется путем перехвата и анализа трафика проходящего по каналам связи принадлежащим сторонним организациям. Угроза может быть реализована при передаче отчетности, в контролирующие органы, через сеть Интернет.

Имеющиеся средства защиты

- Криптографические средства защиты информации (КриптоПро, ViPNET).

Опасность - Высокая
Вероятность реализации - Маловероятно
Актуальность – Актуальна

Удаленный запуск приложений

Угроза заключается в стремлении запустить на узле ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой узла. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др. Выделяют три подкласса данных угроз:

- распространение файлов, содержащих несанкционированный исполняемый код;
- удаленный запуск приложения путем переполнения буфера приложений-серверов;
- удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java- апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы. При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса». При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back.Orifice, NetBus), либо штатными средствами управления и
администрирования компьютерных сетей (LandeskManagementSuite, Managewise, BackOrifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

Имеющиеся средства защиты

- Антивирус Касперского;
- Межсетевой экран Windows.

Опасность - Средняя Вероятность реализации - Низкая Актуальность – Актуальна

Сканирование сети

Сущность процесса реализации угрозы заключается в передачи запросов сетевым службам хостов ИСПДн и анализе ответов от них.

Цель - выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений,

определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

Имеющиеся средства защиты

- Антивирус Касперского;
- Межсетевой экран Windows.

Опасность - Средняя Вероятность реализации - Низкая Актуальность – Актуальна