**государственное бюджетное учреждение Саратовской области**

**«Центр психолого-педагогического и медико-социального сопровождения детей»**

**г. Балаково**

**ОБЕСПЕЧЕНИЕ**

**БЕЗОПАСНОСТИ ИНФОРМАЦИИ ИСПДН**

**ЕДИНОГО ОКНА ЦИФРОВОЙ ОБРАТНОЙ СВЯЗИ**

# Оглавление

|  |  |
| --- | --- |
| **Содержание раздела** | **Стр.** |
| 1. Обозначения и сокращения | 3 |
| 2. Общие положения | 4 |
| 3. Общая характеристика результатов несанкционированного или случайного доступа | 10 |
| 4. Модели угроз безопасности информации ИСПДн единого окна цифровой обратной связи (ПОС) | 12 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**1. Обозначения и сокращения**

АРМ - автоматизированное рабочее место

ВИ - видовая информация

ВТСС - вспомогательные технические средства и системы

ИСПДн - информационная система персональных данных

КЗ - контролируемая зона

МЭ - межсетевой экран

НДВ - недекларированные возможности

НСД - несанкционированный доступ

ОБПДн - обеспечение безопасности персональных данных

ОС - операционная система

ПДн - персональные данные

ПМВ - программно-математическое воздействие

ПО - программное обеспечение

РИ - речевая информация

СВТ - средство вычислительной техники

СЗИ - средство защиты информации

СПИ - стеганографическое преобразование информации

СЭУПИ - специальные электронные устройства перехвата информации

ТКУИ - технический канал утечки информации

ТСОИ - технические средства обработки информации

УБПДн - угрозы безопасности персональных данных

**2. Общие положения**

Настоящая " Базовая модель угроз и модели нарушителя безопасности информации ИСПДн единого окна цифровой обратной связи" (далее - Модель угроз) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных (ПДн), которое ведет к ущербу жизненно важных интересов личности, общества и государства.

Модель угроз содержит единые исходные данные по угрозам безопасности и модели нарушителя безопасности информации ИСПДн единого окна цифровой обратной связи, связанным:

с перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;

с несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

По наличию права постоянного или разового доступа в контролируемую зону (КЗ) ИСПДн нарушители подразделяются на два типа:

нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена, - внешние нарушители;

нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн, - внутренние нарушители.

Внешними нарушителями могут быть:

разведывательные службы государств;

криминальные структуры;

конкуренты (конкурирующие организации);

недобросовестные партнеры;

внешние субъекты (физические лица).

Внешний нарушитель имеет следующие возможности:

осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;

осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;

осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;

осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;

осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИСПДн.

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны режимных и организационно-технических мер защиты, в том числе по допуску физических лиц к ПДн и контролю порядка проведения работ.

Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к ПДн.

К первой категории относятся лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн.

Лицо этой категории может:

иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн;

располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах;

располагать именами и вести выявление паролей зарегистрированных пользователей;

изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.

Ко второй категории относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.

Лицо этой категории:

обладает всеми возможностями лиц первой категории;

знает, по меньшей мере, одно легальное имя доступа;

обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

располагает конфиденциальными данными, к которым имеет доступ.

Его доступ, аутентификация и права по доступу к некоторому подмножеству ПДн должны регламентироваться соответствующими правилами разграничения доступа.

К третьей категории относятся зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам.

Лицо этой категории:

обладает всеми возможностями лиц первой и второй категорий;

располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системы, через которую осуществляется доступ, и о составе технических средств ИСПДн;

имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.

К четвертой категории относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.

Лицо этой категории:

обладает всеми возможностями лиц предыдущих категорий;

обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн;

обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн;

имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн;

имеет доступ ко всем техническим средствам сегмента (фрагмента) ИСПДн;

обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИСПДн.

К пятой категории относятся зарегистрированные пользователи с полномочиями системного администратора ИСПДн.

Лицо этой категории:

обладает всеми возможностями лиц предыдущих категорий;

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.

Системный администратор выполняет конфигурирование и управление программным обеспечением (ПО) и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства криптографической защиты информации, мониторинга, регистрации, архивации, защиты от НСД.

К шестой категории относятся зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн.

Лицо этой категории:

обладает всеми возможностями лиц предыдущих категорий;

обладает полной информацией об ИСПДн;

имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;

не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности отвечает за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор.

К седьмой категории относятся программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте.

Лицо этой категории:

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.

К восьмой категории относятся разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн.

Лицо этой категории:

обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения;

может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.

Указанные категории нарушителей должны учитываться при оценке возможностей реализации УБПДн.

Носителем вредоносной программы может быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа не ассоциируется с какой-либо прикладной программой, то в качестве ее носителя рассматриваются:

отчуждаемый носитель, то есть дискета, оптический диск (CD-R, CD-RW), флэш-память, отчуждаемый винчестер и т.п.;

встроенные носители информации (винчестеры, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок, - видеоадаптера, сетевой платы, звуковой платы, модема, устройств ввода/вывода магнитных жестких и оптических дисков, блока питания и т.п., микросхемы прямого доступа к памяти, шин передачи данных, портов ввода/вывода);

микросхемы внешних устройств (монитора, клавиатуры, принтера, модема, сканера и т.п.).

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то ее носителями являются:

пакеты передаваемых по компьютерной сети сообщений;

файлы (текстовые, графические, исполняемые и т.д.).

**3. Общая характеристика результатов несанкционированного или случайного доступа**

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

нарушению конфиденциальности (копирование, неправомерное распространение);

нарушению целостности (уничтожение, изменение);

нарушению доступности (блокирование).

Нарушение конфиденциальности может быть осуществлено в случае утечки информации:

копирования ее на отчуждаемые носители информации;

передачи ее по каналам передачи данных;

при просмотре или копировании ее в ходе ремонта, модификации и утилизации программно-аппаратных средств;

при "сборке мусора" нарушителем в процессе эксплуатации ИСПДн.

Нарушение целостности информации осуществляется за счет воздействия (модификации) на программы и данные пользователя, а также технологическую (системную) информацию, включающую:

микропрограммы, данные и драйвера устройств вычислительной системы;

программы, данные и драйвера устройств, обеспечивающих загрузку операционной системы;

программы и данные (дескрипторы, описатели, структуры, таблицы и т.д.) операционной системы;

программы и данные прикладного программного обеспечения;

программы и данные специального программного обеспечения;

промежуточные (оперативные) значения программ и данных в процессе их обработки (чтения/записи, приема/передачи) средствами и устройствами вычислительной техники.

Нарушение целостности информации в ИСПДн может также быть вызвано внедрением в нее вредоносной программы программно-аппаратной закладки или воздействием на систему защиты информации или ее элементы.

Кроме этого, в ИСПДн возможно воздействие на технологическую сетевую информацию, которая может обеспечивать функционирование различных средств управления вычислительной сетью:

конфигурацией сети;

адресами и маршрутизацией передачи данных в сети;

функциональным контролем сети;

безопасностью информации в сети.

Нарушение доступности информации обеспечивается путем формирования (модификации) исходных данных, которые при обработке вызывают неправильное функционирование, отказы аппаратуры или захват (загрузку) вычислительных ресурсов системы, которые необходимы для выполнения программ и работы аппаратуры.

Указанные действия могут привести к нарушению или отказу функционирования практически любых технических средств ИСПДн:

средств обработки информации;

средств ввода/вывода информации;

средств хранения информации;

аппаратуры и каналов передачи;

средств защиты информации.

**4. Модели угроз безопасности информации ИСПДн единого окна цифровой обратной связи (ПОС)**

В зависимости от целей и содержания обработки ПДн оператор может осуществлять обработку ПДн в ИСПДн различных типов.

По структуре информационные системы подразделяются на автоматизированные рабочие места, локальные информационные системы и распределенные информационные системы.

По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы, имеющие подключения, и системы, не имеющие подключений.

По режиму обработки персональных данных в информационной системе информационные системы подразделяются на однопользовательские и многопользовательские.

По разграничению прав доступа пользователей информационные системы подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

Информационные системы в зависимости от местонахождения их технических средств подразделяются на системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

В зависимости от технологий, состава и характеристик технических средств ИСПДн, а также опасности реализации УБПДн и наступления последствий в результате несанкционированного или случайного доступа можно выделит следующие типы ИСПДн:

автоматизированные рабочие места, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

автоматизированные рабочие места, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

локальные ИСПДн, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

локальные ИСПДн, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

распределенные ИСПДн, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

распределенные ИСПДн, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

Применительно к основным типам ИСПДн составляются типовые модели угроз безопасности ПДн, характеризующие наступление различных видов последствий в результате несанкционированного или случайного доступа и реализации УБПДн.

Частные модели угроз безопасности ПДн применительно к конкретным ИСПДн составляются операторами, заказчиками и разработчиками ИСПДн на этапах их создания и (или) эксплуатации.

При обработке ПДн на автоматизированном рабочем месте, не имеющем подключения к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих УБПДн:

угроз утечки информации по техническим каналам;

угроз НСД к ПДн, обрабатываемым в автоматизированном рабочем месте.

Угрозы утечки информации по техническим каналам включают в себя:

угрозы утечки акустической (речевой) информации;

угрозы утечки видовой информации;

угрозы утечки информации по каналу ПЭМИН.

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, возможно при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средства обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

Угрозы утечки информации по каналу ПЭМИН возможны из-за наличия электромагнитных излучений, в основном, монитора и системного блока компьютера. Основную опасность представляют угрозы утечки из-за наличия электромагнитных излучений монитора.

Угрозы НСД в автономном АРМ связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн. Кроме этого, источниками угроз НСД к информации в АРМ могут быть аппаратные закладки и отчуждаемые носители вредоносных программ.

В ИСПДн на базе автономного АРМ возможны все виды уязвимостей ИСПДн, за исключением уязвимостей, связанных с реализацией протоколов сетевого взаимодействия и каналов передачи данных. В таких ИСПДн возможны:

угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;

угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.);

угрозы внедрения вредоносных программ.

При обработке ПДн на автоматизированном рабочем месте, имеющем подключения к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих УБПДн:

угрозы утечки информации по техническим каналам;

угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте.

Угрозы утечки информации по техническим каналам включают в себя:

угрозы утечки акустической (речевой) информации;

угрозы утечки видовой информации;

угрозы утечки информации по каналу ПЭМИН.

Возникновение УБПДн в рассматриваемых ИСПДн по техническим каналам характеризуется теми же условиями и факторами, что и для автоматизированного рабочего места, не имеющего подключения к сетям общего пользования и (или) сетям международного информационного обмена.

Угрозы НСД в ИСПДн связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Угрозы НСД в ИСПДн, связанные с действиями нарушителей, имеющих доступ к ИСПДн, аналогичны тем, которые имеют место для отдельного АРМ, не подключенного к сетям связи общего пользования. Угрозы из внешних сетей включают в себя:

угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;

угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.;

угрозы выявления паролей;

угрозы получения НСД путем подмены доверенного объекта;

угрозы типа "Отказ в обслуживании";

угрозы удаленного запуска приложений;

угрозы внедрения по сети вредоносных программ.