

**ЧАСТНАЯ МОДЕЛЬ АКТУАЛЬНЫХ УГРОЗ
И ВЕРОЯТНОГО НАРУШИТЕЛЯ
информационной системы персональных данных
«Кадры»**

Торощина Ольга Валерьевна
директор

подпись

дата

**Мартынова Маргарита
Анатольевна**
заместитель директора по учебной
работе

подпись

дата

Зуйкова Вероника Александровна
методист (руководитель МОЦ)

подпись

дата

СОДЕРЖАНИЕ

Термины и определения.....	3
Перечень сокращений.....	5
1. Общие положения.....	6
2. Общие характеристики ИСПДн	7
3. Определение актуальных угроз безопасности персональных данных в ИСПДн.....	8
4. Модель вероятного нарушителя.....	13
5. Выводы.....	17

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

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 обработки персональных данных (за исключением случаев, если обработка необходима для уточнения 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 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.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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

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.

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.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

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.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц

Программная закладка - скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

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

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц

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 становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (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 ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности ПДн.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ	– автоматизированное рабочее место;
ВТСС	– вспомогательные технические средства и системы;
ИСПДн	– информационная система персональных данных;
КЗ	– контролируемая зона;
НДВ	– недекларированные возможности;
НСД	– несанкционированный доступ;
ОБПДн	– обеспечение безопасности персональных данных;
ОС	– операционная система;
ПДн	– персональные данные;
ПМВ	– программно-математическое воздействие;
ПЭМИН	– побочные электромагнитные излучения и наводки;
СВТ	– средство вычислительной техники;
СЗИ	– средство защиты информации;
СЭУПИ	– специальные электронные устройства перехвата информации;
УБПДн	– угрозы безопасности персональных данных.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Частная модель актуальных угроз МБУДО «Новоторъяльский ЦДО» (далее Оператор) разработана в соответствии с нормативными документами ФСТЭК России:

➤ Базовая модель безопасности персональных данных при их обработке в информационных системах персональных данных, 2008г.;

➤ Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, 2008г.

Частная модель угроз содержит описание возможных угроз безопасности персональных данных и расчет актуальных угроз для ИСПДн Оператора.

Частная модель угроз направлена на определение возможных каналов утечки, путем анализа защищенности ИСПДн Оператора.

Под угрозами безопасности ПДн при их обработке в ИСПДн понимается 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.

В соответствии со статьей 19 Федерального закона №152-ФЗ от 27 июля 2006г. «О персональных данных», ПДн должны быть защищены от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий. Угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн и(или) потребителей, пользующихся услугами, предоставляемыми ИСПДн в соответствии с ее назначением, так и со специально осуществляемыми неправомерными действиями иностранных государств, криминальных сообществ, отдельных организаций и граждан, а также иными источниками угроз.

Угрозы безопасности ПДн могут быть реализованы за счет утечки ПДн по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при ее передаче по каналам связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа с использованием соответствующего программного обеспечения.

2. ОПИСАНИЕ ИСПДН

2.1. Общие характеристики ИСПДн приведены в Таблице 1

№ п/н	Характеристика	Значение характеристики
1	Состав ИСПДн	MSOffice Школьный сайт
2	Назначение	Осуществление кадрового учета
3	Категория обрабатываемых в ИСПДн персональных данных	ИСПДн «Кадры» является информационной системой, обрабатывающей иные категории персональных данных, т.е. в ней не обрабатываются специальные категории персональных данных, биометрические персональные данные, общедоступные персональные данные.
4	Объем обрабатываемых ПДн (количество субъектов персональных данных, ПДн которых обрабатываются в ИСПДн)	Объем обрабатываемых в ИСПДн «Кадры» персональных данных менее 100000 субъектов персональных данных
5	Субъекты персональных данных	ИСПДн «Кадры» является информационной системой, обрабатывающей персональные данные субъектов персональных данных, являющихся сотрудниками оператора персональных данных.
6	Структура ИСПДн	Локальная информационная система (используются комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа).
7	Подключение ИСПДн к сетям связи общего пользования и (или) сетям международного обмена	Имеет подключение к сетям международного информационного обмена.
8	Режим обработки персональных данных	Многопользовательский
9	Разграничение доступа	ИСПДн с разграничением прав доступа.
10	Местонахождение технических средств ИСПДн	Все средства находятся в пределах Российской Федерации.

3. ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИСПДН

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн.

Актуальность угрозы определяется следующими параметрами:

- уровень исходной защищенности ИСПДн;
- частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн. Характеристики ИСПДн «Кадры» приведены в таблице:

№	Параметр	Значение	Уровень защищенности
1	Территориальное размещение	локальная ИСПДн, развернутая в пределах одного здания	Высокий
2	Наличие соединений с сетями общего пользования	ИСПДн, имеющая одноточечный выход в сеть общего пользования	Средний
3	Встроенные (легальные) операции с записями баз персональных данных	Запись, удаление, сортировка	Средний
4	Разграничение доступа к персональным данным	ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн	Средний
5	Наличие соединений с другими базами ПДн иных ИСПДн	ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	Высокий
6	Уровень обобщения (обезличивания) ПДн	ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	Средний
7	Объем ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, предоставляющая часть ПДн	Средний

Соотношение характеристик ИСПДн, соответствующих разным уровням защищенности:

- 29% характеристик ИСПДн соответствуют **высокому** уровню защищенности;
- 71% характеристик ИСПДн соответствуют **среднему** уровню защищенности;
- 0% характеристик ИСПДн соответствуют **низкому** уровню защищенности.

Уровень исходной защищенности ИСПДн – средний ($Y_1=5$).

По каждому виду угрозы, экспертным путем (опрос специалистов) определены:

- опасность (ущерб) в соответствии с правилами, приведенными в таблице 2.

Таблица 2

Опасность (ущерб) угрозы и её характеристики

Опасность (ущерб) угрозы		
Низкая	Средняя	Высокая
Реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных	Реализация угрозы может привести к негативным последствиям для субъектов персональных данных	Реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных

- вероятность реализации угрозы (Y_2) в соответствии с правилами, приведенными в таблице 3.

Таблица 3

Вероятность угрозы и её характеристики

Вероятность	Y_2
Маловероятно	0
Низкая	2
Средняя	5
Высокая	10

С учетом полученных числовых коэффициентов Y_1 и Y_2 по каждому виду угрозы безопасности ПДн рассчитывается числовой коэффициент реализуемости угрозы Y по формуле:

$$Y = (Y_1 + Y_2)/20$$

Соответствие значения числового коэффициента реализуемости угрозы Y и его возможной реализации приведено в таблице 4.

Таблица 4

Значения реализуемости

Значение числового коэффициента реализуемости угрозы Y	Возможность реализации угрозы
$Y \in [0 ; 0.3]$	Низкая
$Y \in (0.3; 0.6]$	Средняя
$Y \in (0.6 ; 0.8]$	Высокая
$Y \in (0.8 ; 1]$	Очень высокая

Актуальность угрозы безопасности ПДн определяется на основании значения коэффициента реализуемости угрозы (Y) и показателя опасности (ущерба) угрозы по каждому ее виду. Вывод об актуальности угрозы происходит в соответствии с правилами, представленными в таблице 5.

Таблица 5

Актуальность реализации угрозы

Возможность реализации угрозы	Опасность угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Угрозы и их характеристики представлены в таблице 6.

Таблица угроз и их характеристик приведена ниже.

Наименование угрозы	Вероятность (Y2)	Реализуемость (Y)	Опасность	Актуальность
УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ				
Угрозы утечки акустической (речевой) информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы утечки видовой информации	низкая вероятность (2)	низкая (0.35)	низкая	неактуальная
Угрозы утечки информации по каналу ПЭМИН	маловероятно (0)	низкая (0.25)	низкая	неактуальная
УГРОЗЫ НСД К ПДн, ОБРАБАТЫВАЕМЫМ НА АВТОМАТИЗИРОВАННОМ РАБОЧЕМ МЕСТЕ				
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
СЕТЕВЫЕ УГРОЗЫ				
Угрозы "Анализа сетевого трафика" с перехватом	низкая вероятность	низкая (0.35)	низкая	неактуальная

передаваемой по сети информации	(2)			
Угрозы выявления паролей	низкая вероятность (2)	низкая (0.35)	средняя	неактуальная
Угрозы удаленного запуска приложений	маловероятно (0)	низкая (0.25)	средняя	неактуальная
Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
УГРОЗЫ ИЗ ВНЕШНИХ СЕТЕЙ				
Угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы выявления паролей	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы получения НСД путем подмены доверенного объекта	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы типа "Отказ в обслуживании"	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы удаленного запуска приложений	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	средняя (0.5)	средняя	актуальная

4.МОДЕЛЬ ВЕРОЯТНОГО НАРУШИТЕЛЯ

По наличию права постоянного или разового доступа в 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:

- криминальные структуры;
- 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 (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами контролируемой зоны.

Категории нарушителей

№	Описание	Нарушитель может	Возможный нарушитель
1	Лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн.	<ul style="list-style-type: none"> – 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 съём информации, используя непосредственное подключение к техническим средствам ИСПДн. 	Сотрудники, не участвующие в обработке ПДн
2	Зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.	<ul style="list-style-type: none"> – 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. 	Сотрудники, обрабатывающие ПДн
3	Зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам	<ul style="list-style-type: none"> – обладает всеми возможностями лиц первой и второй категорий; – располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системам, через которую он осуществляет доступ, и составе технических средств ИСПДн; – имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн. 	Отсутствует
4	Зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.	<ul style="list-style-type: none"> – 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 	Отсутствует

		<p>конфигурации сегмента (фрагмента) ИСПДн;</p> <ul style="list-style-type: none"> – 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. 	
5	Зарегистрированные пользователи с полномочиями системного администратора ИСПДн	<ul style="list-style-type: none"> – 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 ИСПДн
6	Зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн	<ul style="list-style-type: none"> – 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 ИСПДн
7	Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте	<ul style="list-style-type: none"> – 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. 	Отсутствует

8	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн	<ul style="list-style-type: none">– 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.	Отсутствует
---	---	--	-------------

5. ВЫВОДЫ

5.1. В результате анализа возможных угроз безопасности персональных данных выявлено 3 актуальные угрозы безопасности:

№ п/п	Угроза	Вероятность	Опасность
	Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	средняя вероятность (5)	средняя
	Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	средняя вероятность (5)	средняя
	Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	средняя

5.2 Выявленные актуальные угрозы безопасности ПДн в ИСПДн при их реализации могут привести к незначительным последствиям для субъектов ПДн. Необходимо провести мероприятия по устранению указанных угроз или снижению их уровня.