МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ГОРОД КРАСНОДАР ЛИЦЕЙ № 4

УТВЕРЖДАЮ

Директор МБОУ лицея № 4

Л.Б.Капустина

«01» сентября 2016 г.

Подписано цифровой подписью: Капустина Людмила Борисовна
Дата: 2021.03.01 16:44:09 +03'00'

ИНСТРУКЦИЯ
«ПЕРЕЧЕНЬ МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ ОБЕЗЛИЧЕННЫХ ДАННЫХ»

На 87 листах

Краснодар, 2013

Содержание

СПИСОК СОКРАЩЕНИЙ

АВС	-	антивирусные средства
АИС	-	автоматизированная информационная система
АРМ	-	автоматизированное рабочее место
ИНН	-	индивидуальный номер налогоплательщика
ИСПДн	-	информационная система персональных данных
ЛВС	-	локальная вычислительная сеть
ЛИС	-	локальная информационная система
МЭ	-	межсетевой экран
НСД	-	несанкционированный доступ
ОС	-	операционная система
ПДн	-	персональные данные
ПМВ	-	программно-математическое воздействие
ПО	-	программное обеспечение
ПФ	-	пенсионный фонд
ПЭМИН	-	побочные электромагнитные излучения и наводки
РИС	-	распределенная информационная система
СЗИ	-	средства защиты информации
СЗПДн	-	система (подсистема) защиты персональных данных
ТКУИ	-	технические каналы утечки информации
УБПДн	-	угрозы безопасности персональных данных
ФСТЭК России	-	Федеральный орган исполнительной власти России, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности
Хпд	-	категория обрабатываемых в информационной системе персональных данных
Хнпд	-	объем обрабатываемых в информационной системе персональных данных
МЭ	-	межсетевой экран
СКЗИ	-	средства криптографической защиты информации
VPN-соединение	-	виртуальная частная сеть

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

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

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и / или воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

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

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и / или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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

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

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

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных

действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц (ст.3 п.5 № 152-ФЗ).

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

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

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

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

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

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

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

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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

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

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

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

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

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

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

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

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

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

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

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

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы. **Специальные категории персональных данных** – персональныеданные, касающиеся расовойи национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

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

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

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства

обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

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

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

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

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

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

Учреждение – государственное образовательное учреждение города Москвы.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

1 ОБЛАСТЬ ПРИМЕНЕНИЯ ИНСТРУКЦИИ

Данная инструкция применяется для МБОУ лицея № 4» (далее – Учреждение), которые в электронном виде обрабатывает персональные данные, не позволяющие идентифицировать физическое лицо.

Согласно Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Закон), **персональные данные** (ПДн) – это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

К персональных данным относятся: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация о субъекте персональных данных.

Проекты наиболее часто встречающихся совокупностей данных, не позволяющих идентифицировать субъекта:

- Фамилия и инициалы + любые другие данные;
- Порядковый номер + любые другие данные.Общие рекомендации

Обработка обезличенных персональных данных является оптимальной, так как нарушение безопасности персональных данных не приводит к негативным последствиям для субъектов персональных данных, а требования к обеспечению защиты персональных данных в соответствии с законодательством определяет само учреждение.

Если в учреждении также производится обработка ПДн на бумажных носителях, воспользуйтесь инструкцией «Перечень мероприятия по обеспечению безопасности персональных данных при неавтоматизированной обработке».

Если в учреждении также производится автоматизированная обработка данных позволяющих идентифицировать субъекта персональных данных, воспользуйтесь инструкцией «Перечень мероприятий по обеспечению безопасности персональных данных при автоматизированной обработке данных, позволяющих идентифицировать субъекта персональных данных».

2 ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Для обеспечения соответствия законодательству в области защиты персональных данных необходимо выполнить нижеследующие шаги и разработать необходимые документы (раздел 4):

- ввести в школе режим обработки ПДн. Режим обработки вводится приказом («Приказ о введении режима обработки персональных данных»);
- инициировать внутреннюю проверку ИСПДн. Внутренняя проверка вводится приказом («Приказ о проведении внутренней проверки ИСПДн»).

В ходе внутренней проверки определяются:

- состав и структура объектов защиты;
- конфигурация и структура информационных систем персональных данных;
- информация о разграничении прав доступа к обрабатываемым персональным данным;
- режим обработки персональных данных;
- выявленные угрозы безопасности персональных данных;
- перечень мероприятий, обеспечивающих защиту персональных данных;
- перечень применяемых средств защиты информации, эксплуатационной и технической документации к ним.

Результаты внутренней проверки необходимо отразить в Отчете по результатам проведения внутренней проверки.

По результатам внутренней проверки для каждой выявленной системы должны быть составлены:

- Акт классификации «Акт классификации информационной системы, обрабатывающей персональные данные».
- Декларация соответствия требованиям законодательства «Декларация соответствия»;
- Частная модель угроз «Модель угроз ИСПДн». Для всех систем необходимо:
- обрабатываемые в системе данные указать в «Перечне ПДн, подлежащих защите в ИСПДн»;
- группы лиц, обрабатывающие персональные данные, определить и перечислить в «Положение о разграничении прав доступа к обрабатываемым ПДн»;
- все ИСПДн описать в «Отчет о результатах проведения внутренней проверки». Важно: запрещается обрабатывать персональные данные учеников и их родителей,

а так же сотрудников школы на компьютерах, не входящих в ИСПДн, личных и домашних компьютерах.

В приложениях к инструкции приведены Проекты акта классификации, отчета о результатах проведения внутренней проверки и частной модели угроз.

Подробные указания по выбору частной модели угроз в соответствии со структурой системы приведены в «Методике составления частной модели угроз (ЧМУ)». Подробная классификация системы приведена в разделе 7 Методических рекомендаций.

Ниже содержатся краткие указания по классификации ИСПДн и определения ЧМУ.

2.1 Системы бухгалтерского и кадрового учета

Если образовательное учреждение обслуживается централизованной бухгалтерией, и в самом образовательном учреждении нет функционирующих бухгалтерских программ, обрабатывающих персональные данные, то нет необходимости проводить какие-либо мероприятия по защите персональных данных данной системы, это обязанность владельца ИСПДн.

Системы бухгалтерского и кадрового учёта чаще всего обрабатывают данные, позволяющие идентифицировать субъекта персональных данных. Данная методика применима только для систем, обрабатывающих обезличенные персональные данные. Для инструкций по обеспечению безопасности при обработке персональных данных, позволяющих идентифицировать субъекта, обратитесь к инструкции «Перечень мероприятий по обеспечению безопасности персональных данных при автоматизированной обработке данных, позволяющих идентифицировать субъекта персональных данных».

Если установлена программа семейства 1С (Бухгалтерия, Налогоплательщик и т.д.), или иная программа бухгалтерского и кадрового учёта, в которой обрабатываются персональные данные, то необходимо определить:

Есть ли у данного компьютера подключение к сети Интернет?

Если компьютер подключен к сети Интернет, то частную модель угроз следует выбирать из АРМ II, АРМ IV, АРМ VI и ЛИС II (см. ЧМУ).

Если подключения нет, то частную модель угроз следует выбирать из АРМ I, АРМ III, АРМ V и ЛИС I (см. ЧМУ).

Для более точного определения модели угроз следует ответить на следующие вопросы:

Подключён ли компьютер к другим компьютерам посредством локальной сети?

Если компьютер подключен к другим компьютерам посредством локальной сети и имеет подключение к сети Интернет, то частная модель угроз системы соответствует ЛИС II, и приложение «Модель угроз ИСПДн» заполняется в соответствии с приложением 8 из «Методики составления ЧМУ». В приложение «Акт классификации информационной системы, обрабатывающей персональные данные» заносятся следующие данные о системе: многопользовательская, локальная, с разграничением прав доступа, с подключением к сетям общего пользования.

Если компьютер подключен к другим компьютерам посредством локальной сети и не имеет подключения к сети Интернет, то частная модель угроз системы соответствует ЛИС I, и приложение «Модель угроз ИСПДн» заполняется в соответствии с приложением 7 из «Методики составления ЧМУ». В приложение «Акт классификации информационной системы, обрабатывающей персональные данные» заносятся следующие данные о системе: многопользовательская, локальная, с разграничением прав доступа, без подключения к сетям общего пользования.

Если компьютер не подключен к другим компьютерам посредством локальной сети, то частная модель угроз выбирается из АРМ I-VI (см. «Методика составления ЧМУ»).

В каком режиме обрабатываются персональные данные?

Если с ИСПДн работает один человек, и она не имеет подключений к сетям связи общего пользования, то режим обработки является однопользовательским, частная модель угроз системы соответствует АРМ I, и приложение «Модель угроз ИСПДн» заполняется в соответствии с приложением 1 из «Методики составления ЧМУ». В приложение «Акт классификации информационной системы персональных данных» заносятся следующие

данные о системе: однопользовательская, АРМ, без разграничения прав доступа, без подключения к сетям связи общего пользования.

Если с системой работает один человек и она имеет подключение к сетям связи общего пользования, то режим обработки является однопользовательским, частная модель угроз системы соответствует АРМ II, и приложение «Модель угроз ИСПДн» заполняется в соответствии с приложением 2 из «Методики составления ЧМУ». В приложение «Акт классификации информационной системы, обрабатывающей персональные данные» заносятся следующие данные о системе: однопользовательская, АРМ, без разграничения прав доступа, с подключения к сетям связи общего пользования.

Если с системой работает несколько человек, то режим является многопользовательским, частная модель угроз системы соответствует АРМ III-VI.

Есть ли в системе разграничение прав пользователей?

Если с работающей системой люди имеют разные права доступа при обработке персональных данных, и она не имеет подключение к сетям связи общего пользования, частная модель угроз системы соответствует АРМ V, и приложение «Модель угроз ИСПДн» заполняется в соответствии с приложением 5 из «Методики составления ЧМУ». В приложение «Акт классификации информационной системы, обрабатывающей персональные данные» заносятся следующие данные о системе: многопользовательская, АРМ, с разграничением прав доступа, без подключения к сетям связи общего пользования.

Если с работающей системой люди имеют разные права доступа при обработке персональных данных, и она имеет подключение к сетям связи общего пользования, частная модель угроз системы соответствует АРМ VI, и приложение «Модель угроз ИСПДн» заполняется в соответствии с приложением 6 из «Методики составления ЧМУ». В приложение «Акт классификации информационной системы, обрабатывающей персональные данные» заносятся следующие данные о системе: многопользовательская, АРМ, с разграничением прав доступа, с подключением к сетям связи общего пользования.

Если с работающей системой люди имеют одинаковые права доступа при обработке персональных данных, и она имеет подключение к сетям связи общего пользования, частная модель угроз системы соответствует АРМ IV, и приложение «Модель угроз ИСПДн» заполняется в соответствии с приложением 4 из «Методики составления ЧМУ». В приложение «Акт классификации информационной системы, обрабатывающей персональные данные» заносятся следующие данные о системе: многопользовательская, АРМ, без разграничением прав доступа, с подключением к сетям связи общего пользования.

Если с работающей системой люди имеют одинаковые права доступа при обработке персональных данных, и она не имеет подключение к сетям связи общего пользования, частная модель угроз системы соответствует АРМ III, и приложение «Модель угроз ИСПДн» заполняется в соответствии с приложением 3 из «Методики составления ЧМУ». В приложение «Акт классификации информационной системы, обрабатывающей персональные данные» заносятся следующие данные о системе: многопользовательская, АРМ, без разграничения прав доступа, без подключения к сетям связи общего пользования.

На основе данных вопросов можно точно выбрать модель угроз. Для составления акта классификации необходимо добавить следующую информацию: все системы являются специальными, целиком расположены на территории Российской Федерации, объем обрабатываемых персональных данных 3 (менее 1000 субъектов ПДн). Категория обрабатываемых персональных данных 4. Бухгалтерская система 1С относится к классу

К4. На основе полученных сведений заполняется акт классификации, частная модель угроз и отчет о результатах проведения внутренней проверки.

Все системы бухгалтерского и кадрового учёта имеют схожую структуру. Поэтому вышеперечисленная методика применима к подобным системам.

Простая методика выбора частной модели угроз представлена на рисунке 1 (стр.15).

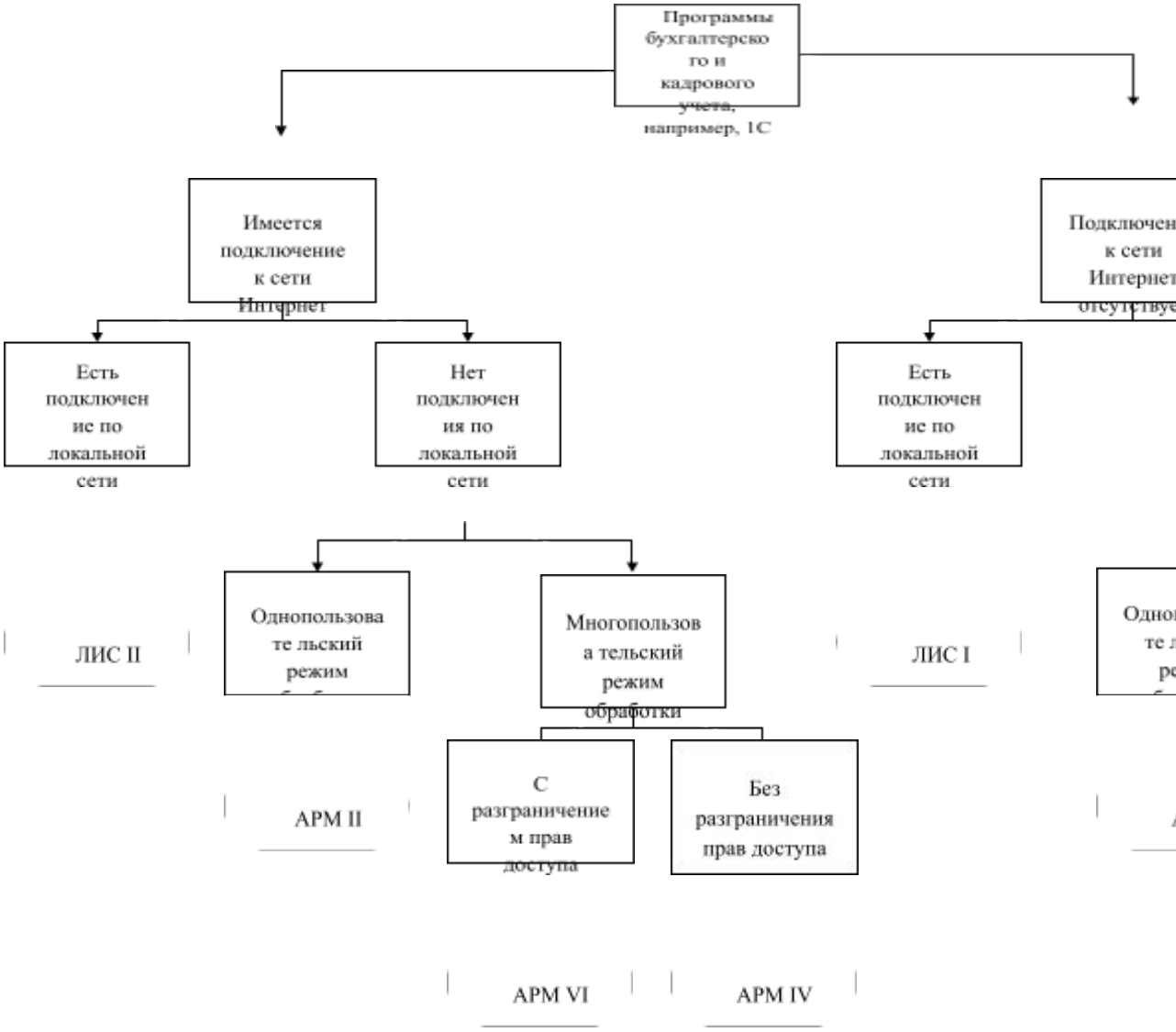

Рисунок - 1 Методика выбора частной модели угроз

Если в образовательном учреждении установлена какая либо программа, поставляемая вышестоящим органом, осуществляющим управление в области образования, в которых постоянно обрабатываются персональные данные, то необходимо определить:

- есть ли возможность удаленного доступа к системе? Если вы можете получить доступ посредством сети интернет или через локальную сеть из другого здания, то считается, что система обладает возможностью удаленного доступа. В этом случае методика классификации и определения частной модели угроз, совпадает с методикой классификации и составления частной модели угроз собственных систем, которая приведена ниже;
- если возможность удаленного доступа отсутствует, то методика классификации и составление частной модели угроз совпадает с методикой классификации и составления частной модели угроз бухгалтерского и кадрового учета (см. выше).

Если у вас создана собственная система управления учебным процессом, или используется какая либо другая система, в которой обрабатываются персональные данные, то необходимо определить:

- есть ли возможность удаленного доступа к системе? Если вы можете получить доступ посредством сети интернет или через локальную сеть из другого здания, то считается, что система обладает возможностью удаленного доступа. В этом случае частная модель угроз выбирается из РИС I-II. Если удаленного доступа нет, то частная модель угроз выбирается из АРМ I-VI, ЛИС I-II;
- есть ли у данного компьютера подключение к сети Интернет? Если компьютер подключен к сетям связи общего пользования и у него есть удаленный доступ, то частная модель угроз системы соответствует РИС II, и приложение «Модель угроз ИСПДн» заполняется в соответствии с приложением 10 из «Методики составления ЧМУ». В приложение «Акт классификации информационной системы, обрабатывающей персональные данных» заносятся следующие данные о системе: многопользовательская, распределённая, с разграничением прав доступа, с подключением к сетям связи общего пользования;
- если компьютер не подключен к сетям связи общего пользования и у него есть удаленный доступ, то частная модель угроз системы соответствует РИС I, и приложение «Модель угроз ИСПДн» заполняется в соответствии с приложением 9 из «Методики составления ЧМУ». В приложение «Акт классификации информационной системы, обрабатывающей персональные данные» заносятся следующие данные о системе: многопользовательская, распределённая, с разграничением прав доступа, без подключения к сетям связи общего пользования;
- если компьютер подключен к сети Интернет, но нет удаленного доступа, частную модель угроз следует выбирать из АРМ II, АРМ IV, АРМ VI и ЛИС II;
- если подключения и удаленного доступа нет, то частную модель угроз следует выбирать из АРМ I, АРМ III, АРМ V и ЛИС I.

Для более точного определения модели угроз следует ответить на следующие вопросы.

- подключён ли компьютер к другим компьютерам посредством локальной сети? Если компьютер подключен к другим компьютерам посредством локальной сети и имеет подключение к сети Интернет, то частная модель угроз системы соответствует ЛИС II, и приложение «Модель угроз ИСПДн» заполняется в соответствии с приложением 8 из «Методики составления ЧМУ». В приложение «Акт классификации информационной системы, обрабатывающей персональные данные» заносятся следующие данные о системе: многопользовательская, локальная, с разграничением прав доступа, с подключением к сетям общего пользования;
- если компьютер подключен к другим компьютерам посредством локальной сети и не имеет подключения к сети Интернет, то частная модель угроз системы соответствует ЛИС I, и приложение «Модель угроз ИСПДн» заполняется в соответствии с приложением 7 из «Методики составления ЧМУ». В приложение «Акт классификации информационной системы, обрабатывающей персональные данные» заносятся следующие данные о системе: многопользовательская, локальная, с разграничением прав доступа, без подключения к сетям общего пользования;
- если компьютер не подключен к другим компьютерам посредством локальной сети, то частная модель угроз выбирается из АРМ I-VI.

В каком режиме обрабатываются персональные данные?

Если с системой работает один человек и она не имеет подключений к сетям связи общего пользования, то режим обработки является однопользовательским, частная модель угроз системы соответствует АРМ I, и приложение «Модель угроз ИСПДн» заполняется в соответствии с приложением 1 из «Методики составления ЧМУ». В приложение «Акт классификации информационной системы, обрабатывающей персональные данные» заносятся следующие данные о системе: однопользовательская, АРМ, без разграничения прав доступа, без подключения к сетям связи общего пользования.

Если с системой работает один человек и она имеет подключение к сетям связи общего пользования, то режим обработки является однопользовательским, частная модель угроз системы соответствует АРМ II, и приложение «Модель угроз ИСПДн» заполняется в соответствии с приложением 2 из «Методики составления ЧМУ». В приложение «Акт классификации информационной системы, обрабатывающей персональные данные» заносятся следующие данные о системе: однопользовательская, АРМ, без разграничения прав доступа, с подключения к сетям связи общего пользования.

Если с системой работает несколько человек, то режим является многопользовательским, и частная модель угроз системы соответствует АРМ III-VI.

Есть ли в системе разграничение прав пользователей?

Если с работающей системой люди имеют разные права доступа при обработке персональных данных, и она не имеет подключение к сетям связи общего пользования, частная модель угроз системы соответствует АРМ V, и приложение «Модель угроз ИСПДн» заполняется в соответствии с приложением 5 из «Методики составления ЧМУ». В приложение «Акт классификации информационной системы, обрабатывающей персональные данные» заносятся следующие данные о системе: многопользовательская, АРМ, с разграничением прав доступа, без подключения к сетям связи общего пользования.

Если с работающей системой люди имеют разные права доступа при обработке персональных данных, и она имеет подключение к сетям связи общего пользования, частная модель угроз системы соответствует АРМ VI, и приложение «Модель угроз ИСПДн» заполняется в соответствии с приложением 6 из «Методики составления ЧМУ». В приложение «Акт классификации информационной системы, обрабатывающей

персональные данные» заносятся следующие данные о системе: многопользовательская, АРМ, с разграничением прав доступа, с подключением к сетям связи общего пользования.

Если с работающей системой люди имеют одинаковые права доступа при обработке персональных данных, и она имеет подключение к сетям связи общего пользования, частная модель угроз системы соответствует АРМ IV, и приложение «Модель угроз ИСПДн» заполняется в соответствии с приложением 4 из «Методики составления ЧМУ». В приложение «Акт классификации информационной системы, обрабатывающей персональные данные» заносятся следующие данные о системе: многопользовательская, АРМ, без разграничением прав доступа, с подключением к сетям связи общего пользования.

Если с работающей системой люди имеют одинаковые права доступа при обработке персональных данных, и она не имеет подключения к сетям связи общего пользования, частная модель угроз системы соответствует АРМ III, и приложение «Модель угроз ИСПДн» заполняется в соответствии с приложением 3 из «Методики составления ЧМУ». В приложение «Акт классификации информационной системы, обрабатывающей персональные данные» заносятся следующие данные о системе: многопользовательская, АРМ, без разграничения прав доступа, без подключения к сетям связи общего пользования.

На основе данных вопросов можно точно выбрать модель угроз. Для составления акта классификации необходимо добавить следующую информацию: все системы являются специальными, целиком расположены на территории Российской Федерации, объем обрабатываемых данных 3 (меньше 1000 субъектов). Категория обрабатываемых персональных данных может принимать значения 3 (позволяющая идентифицировать субъекта ПДн) и 2 (позволяющая идентифицировать субъекта ПДн и получить о нём дополнительную информацию).

Если в системе содержатся персональные данные, по которым можно однозначно идентифицировать субъекта персональных данных, то система имеет класс К3 (наличие дополнительных сведений не изменяет класс на К2). Если в системе обрабатываются персональные данные о здоровье субъекта (диагноз, психологическое заключение и т.д.), то система имеет класс К1. **Настоятельно не рекомендуется обрабатывать в электронных системах данные о здоровье**.

Простая методика выбора частной модели угроз представлена на рисунке 2 (стр. 16) .

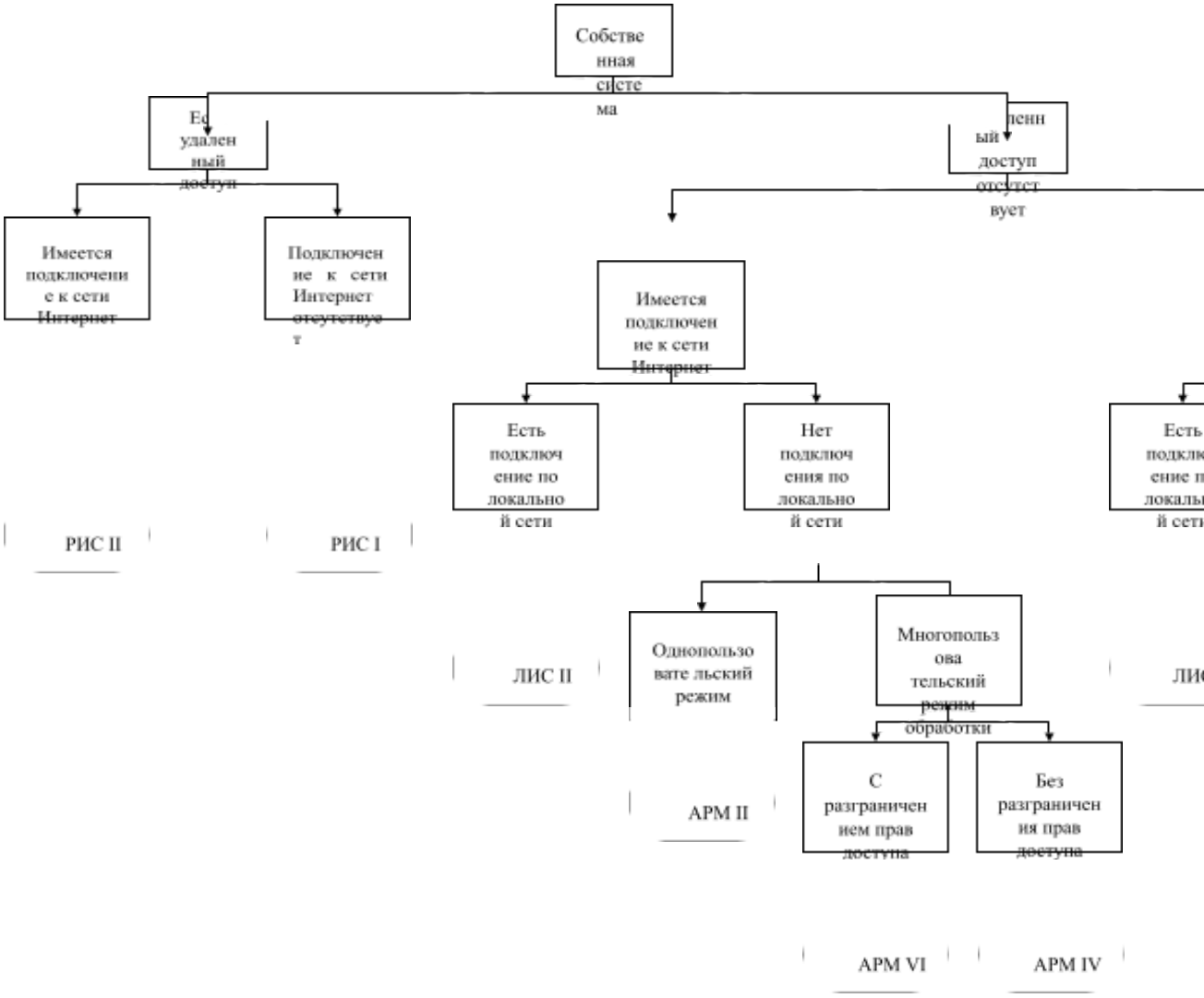

Рисунок - 2 Методика выбора частной модели угроз

3 НОРМАТИВНО-ОРГАНИЗАЦИОННАЯ ДОКУМЕНТАЦИЯ

3.1 ОРГАНИЗАЦИОННЫЕ ДОКУМЕНТЫ

Для правильного выполнения организационных мероприятий в Учреждении и разработке документов необходимо использовать шаблоны, представленные в Приложении. Данный набор документов необходим для организации защиты персональных данных в учреждении. Формы документов, на основе которых учреждение может разработать собственную нормативно-организационную базу.

Если в учреждении в электронном виде обрабатываются только обезличенные персональные данные, разработка подробной нормативной базы не является обязательной и производится на собственное усмотрение оператора.

3.2 ПРИКАЗ О ВВЕДЕНИИ РЕЖИМА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Приказ о введение режима обработки ПДн является основополагающим документом, устанавливающим, что в Учреждении ведется обработка персональных данных.

Проект приказа о введении режима обработки персональных данных. Приказ

должен:

быть оформлен в соответствии с внутренним порядком документооборота Учреждения;

быть утвержден Руководителем Учреждения.

в приказе должен быть указан сотрудник, ответственный за контроль исполнения приказа.

Ответственным сотрудником может быть Руководитель Учреждения, лицо, отвечающее за обеспечение режима безопасности, или любой другой сотрудник, на которого возложен контроль за выполнение приказа.

3.3 ПОЛОЖЕНИЕ О ПОРЯДКЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Положение вводится приказом и устанавливает нижестоящие документы по обеспечению режима обработки и защиты ПДн.

Проект приказа о введении Положения о порядке обработки персональных данных.

Положение должно:

быть оформлено в соответствии с внутренним порядком документооборота Учреждения;

быть утверждено Руководителем Учреждения.

3.4 ПРИКАЗ О ПОДРАЗДЕЛЕНИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Приказ вводит в Учреждении режим защиты персональных

данных. Проект приказа о подразделении по защите информации.

Приказ должен:

быть оформлен в соответствии с внутренним порядком документооборота Учреждения;

быть утвержден Руководителем Учреждения.

в приказе должно быть указано лицо (сотрудник) или подразделение, ответственное за обеспечение безопасности персональных данных. Если в Учреждении нет отдела или специалиста, занимающегося защитой информации, то его следует назначить из числа доверенных лиц.

Ответственным за обеспечение безопасности ПДн может быть назначен руководитель отдела информационных технологий или любой другой сотрудник.

3.5 Положение о подразделении по защите информации

Положение о подразделении по защите информации определяет лица, ответственные за обеспечение безопасности, а так же организационные и технические мероприятия по достижению безопасности. Положение вводится приказом и устанавливает нижестоящие документы по обеспечению защиты ПДн.

Проект приказа о введении Положения о подразделении по защите информации.

Положение должно:

быть оформлено в соответствии с внутренним порядком документооборота Учреждения;

быть утверждено Руководителем Учреждения.

В Положение могут быть добавлены дополнительные права и обязанности подразделения.

3.6 Положение о разграничении прав доступа к обрабатываемым персональным данным

Положение о разграничении прав доступа к обрабатываемым персональным данным определяет список лиц ответственных за обработку ПДн и уровень их доступа.

Проект Положения о разграничении прав доступа к обрабатываемым персональным данным.

Положение должно:

- быть оформлено в соответствии с внутренним порядком документооборота Учреждения;
- быть утверждено Руководителем Учреждения, на основании Отчета о результатах проведения внутренней проверки.

3.7 Приказ о проведении внутренней проверки

Приказ о проведении внутренней проверки определяет положение о проведении внутренней проверки.

Проект Приказа о проведении внутренней проверки.

Приказ должен:

быть оформлен в соответствии с внутренним порядком документооборота Учреждения;

быть утвержден Руководителем Учреждения;

в приказе должен быть установлен срок проведения проверки;

в приказе должен быть указан состав комиссии по классификации ИСПДн. В состав комиссии рекомендуется включить ответственного за обеспечение безопасности, руководителей отделов, чьи подразделения участвуют в обработке персональных данных, технических специалистов, обеспечивающих поддержку технических средств. Также к участию в комиссии в качестве консультантов можно привлекать специалистов сторонних организаций;

в приказе должен быть указан сотрудник, ответственный за контроль исполнения приказа.

Ответственным сотрудником может быть Руководитель Учреждения, лицо, отвечающее за обеспечение режима безопасности или проведение внутренней проверки, или любой другой сотрудник, на которого возложен контроль за выполнение приказа.

3.8 Перечень персональных данных, подлежащих защите

Перечень персональных данных содержит перечисление объектов защиты для каждой ИСПДн.

Проект Перечня персональных данных, подлежащих защите.

Перечень должен:

быть оформлен в соответствии с внутренним порядком документооборота Учреждения;

быть утвержден Руководителем Учреждения или комиссией на основании Отчета о результатах проведения внутренней проверки.

Дата введения Перечня должна быть последующей после проведения внутренней проверки и принятия отчета о проведении внутренней проверки.

Перечень составляется для каждой выявленной ИСПДн.

3.9 Инструкция пользователя информационной системы персональных данных.

Инструкция пользователя ИСПДн определяет должностные обязанности всех пользователей ИСПДн.

Проект Инструкции пользователя ИСПДн.

Инструкция должна:

быть утверждена Руководителем Учреждения, ответственным за обеспечение безопасности ПДн или руководителем отдела;

в случае уточнения обязанностей пользователя ИСПДн, вследствие специфических особенностей Учреждения, в Инструкцию должны быть внесены соответствующие изменения.

3.10 Инструкция администратора информационной системы персональных данных

Инструкция администратора ИСПДн определяет должностные обязанности администратора ИСПДн.

Проект Инструкции администратора ИСПДн.

Инструкция должна:

быть утверждена Руководителем Учреждения, ответственным за обеспечение безопасности ПДн или руководителем отдела;

в Инструкции должно быть указано лицо, которому непосредственно подчиняется Администратор ИСПДн.

В случае уточнения обязанностей администратора ИСПДн, вследствие специфических особенностей Учреждения, в Инструкцию должны быть внесены соответствующие изменения.

3.11 Инструкция администратора безопасности информационной системы персональных данных

Инструкция администратора безопасности ИСПДн определяет должностные обязанности администратора безопасности ИСПДн.

Проект Инструкции администратора безопасности ИСПДн.

Инструкция должна:

быть утверждена руководителем подразделения ответственного за обеспечение режима безопасности или специально уполномоченным сотрудником;

в Инструкции должно быть прописано лицо, которому непосредственно подчиняется Администратор Безопасности ИСПДн.

В случае уточнения обязанностей Администратора безопасности ИСПДн, вследствие специфических особенностей Учреждения, в Инструкцию должны быть внесены соответствующие изменения.

3.12 План мероприятий по обеспечению защиты персональных данных

План мероприятий по обеспечению защиты ПДн определяет перечень мероприятий обеспечения безопасности.

Проект Плана мероприятий по обеспечению защиты ПДн.

План должен:

быть оформлен в соответствии с внутренним порядком документооборота Учреждения;

быть утвержден руководителем подразделения ответственного за обеспечение режима безопасности или специально уполномоченным сотрудником, на основании Отчета о результатах проведения внутренней проверки.

Дата введения Плана должна быть последующей после проведения внутренней проверки и принятия отчета о проведении внутренней проверки.

3.13 План внутренних проверок состояния защиты персональных данных

План внутренних проверок содержит периодичность проведения внутренних проверок.

Проект Плана внутренних проверок.

План должен быть утвержден руководителем подразделения ответственного за обеспечение режима безопасности или специально уполномоченным сотрудником.

Проверка может производиться подразделением, ответственным за обеспечение режима безопасности или с привлечением специальных организаций.

3.14 Приказ о назначении ответственных лиц за обработку

ПЕРСОНАЛЬНЫХ ДАННЫХ

Приказ о назначении ответственных лиц за обработку ПДн, определяет уровень доступа и ответственность лиц участвующих в обработке ПДн. Положение вводится приказом и устанавливает нижестоящие документы по обеспечению режима обработки ПДн.

Проект Приказа о назначении ответственных лиц за обработку ПДн.

Приказ должен:

- быть оформлен в соответствии с внутренним порядком документооборота Учреждения;
- быть утвержден Руководителем Учреждения, на основании Отчета о результатах проведения внутренней проверки;
- приказ должен быть утверждён после проведения внутренней проверки и утверждения отчёта о проведении внутренней проверки;
- в приказе должен быть указан сотрудник ответственный за контроль исполнения приказа.

Ответственным сотрудником может быть Руководитель Учреждения, лицо, отвечающее за обеспечение режима безопасности или проведение внутренней проверки, или любой другой сотрудник, на которого возложен контроль за выполнение приказа.

3.15 Приказ об утверждении мест хранения материальных носителей персональных данных

Приказ об утверждении мест хранения материальных носителей ПДн, устанавливает места хранения материальных носителей ПДн в бумажном и электронном виде (на съемных носителях).

Проект Приказа об утверждении мест хранения материальных носителей персональных данных.

Приказ должен:

- быть утвержден Руководителем Учреждения.
- назначить ответственного за хранение материальных носителей персональных данных
- в приказе отражаются все места хранения материальных носителей.

3.16 Положение об Электронном журнале обращений пользователей информационной системы к персональным данным

Положение об Электронном журнале обращений пользователей информационной системы к ПДн определяет порядок регистрации действий пользователей ИСПДн при обработке ПДн. Положение вводится приказом.

Проект Положения об Электронном журнале обращений пользователей информационной системы к ПДн.

Положение должно:

- быть оформлено в соответствии с внутренним порядком документооборота Учреждения;
- быть утверждено Руководителем Учреждения.

3.17 Концепция информационной безопасности

Концепция информационной безопасности определяет принципы обеспечения

безопасности.

Проект Концепции информационной безопасности.

Концепция должна:

- быть оформлена в соответствии с внутренним порядком документооборота Учреждения;
- быть утверждена Руководителем Учреждения.

При выявлении положений, специфичных для обработки ПДн в конкретном Учреждении, они должны быть добавлены в Концепцию.

3.18 Рекомендации по разработке Политики информационной безопасности

Политика информационной безопасности определяет категории конкретных мероприятий по обеспечению безопасности ПДн.

Проект Политики информационной безопасности.

Политика должна:

быть оформлена в соответствии с внутренним порядком документооборота Учреждения;

быть утверждена Руководителем Учреждения.

В соответствующем разделе Политики должен быть уточнен перечень групп пользователей, обрабатывающих ПДн. Группы пользователей, их права, уровень доступа и информированность должны быть отражены так, как это отражается рабочим порядком в Учреждении.

3.19 Проект договора о поручении обработки персональных данных третьим лицам

Проект договора о поручении обработки персональных данных третьим лицам, определяет обязанности сторон при передаче персональных данных Учреждением третьей стороне.

Проект Проекта договора о поручении обработки персональных данных третьим лицам.

Между сторонами может быть заключен как отдельный договор, так и внесены дополнения в уже существующие договора, так и заключено дополнительное соглашение.

3.20 Согласие субъекта на обработку персональных данных

Согласие на обработку персональных данных рекомендуется брать в явном виде всегда. Оно может быть оформлено в виде отдельного документа, или могут быть внесены разъяснения в уже имеющиеся формы бланков и договоров.

Проект Согласия субъекта на обработку персональных данных.

Согласие нужно получать от субъектов ПДн в письменной форме, с которыми заключён договор на обучение (с родителями учащегося). Если обрабатываемые персональные данные содержат только ФИО, то согласие от субъекта не требуется.

3.21 Согласие сотрудника на обработку персональных данных

От сотрудников согласие берётся при устройстве на работу, согласие за несовершеннолетних учащихся дают их родители или опекуны (согласие должно быть оговорено в договоре или в заявлении на обучение).

Проект Согласия сотрудника на обработку персональных данных.

3.22 Соглашение о неразглашении персональных данных

Соглашение подписывается с каждым сотрудником Учреждения. Проект Соглашение о неразглашении персональных данных.

3.23 Акт об уничтожении персональных данных субъекта(-ов) персональных данных

Акт об уничтожении персональных данных составляется каждый раз, когда происходит уничтожение материальных носителей персональных данных или когда данные уничтожаются по требованию субъекта или уполномоченного органа (данные должны быть отмечены в соответствующем журнале (Приложение №2))

Проект Акта об уничтожении.

Акт должен:

быть составлен для каждого случая уничтожения ПДн по запросу субъекта ПДн, уполномоченного органа, достижения целей обработки или окончания срока хранения;

Акт должен быть подписан председателем комиссии, назначенной соответствующим приказом, а так же лицами производящими уничтожение.

3.24 Рекомендации по разработке Порядка резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и систем защиты информации

Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ определяет принципы обеспечения целостности и доступности ПДн.

Проект Порядка резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ.

Документ должен:

- быть оформлено в соответствии с внутренним порядком документооборота Учреждения;
- быть утверждено руководителем подразделения ответственного за обеспечение режима безопасности или специально уполномоченным сотрудником.

В документе должны быть указаны сотрудники, ответственные за реагирование на инциденты безопасности.

Ответственным сотрудником может быть администратор ИСПДн или любой другой сотрудник.

4 РЕКОМЕНДАЦИИ ПО ВЕДЕНИЮ НЕОБХОДИМЫХ ФОРМ УЧЕТА

В данном разделе описаны действия по заполнению необходимых форм учета:

Журнал учета мероприятий по контролю над соблюдением режима защиты персональных данных (раздел 12.4.1.2. «Методические рекомендации»);

Журнал учета носителей (раздел 12.4.1.3. «Методические рекомендации»);

Журнал учета обращений субъектов ПДн (раздел 12.4.1.4 «Методические рекомендации»);

Журнал учета обращений уполномоченного органа (раздел 12.4.1.4 «Методические рекомендации»);

Журнал учета разовых пропусков (раздел 12.4.1.5 «Методические рекомендации»);

Журнал учета съемных носителей (раздел 12.4.1.3 «Методические рекомендации»);

Более подробная информация указана в разделе 12.4 «Методических рекомендаций».

4.1 НАБОР БЛАНКОВ ПРЕДОСТАВЛЕНИЯ СВЕДЕНИЙ, ОТКАЗА В ПРЕДОСТАВЛЕНИИ, УВЕДОМЛЕНИЙ, РАЗЪЯСНЕНИЙ

В приложении в папке «Набор Бланков» содержаться бланки ответов (предоставление сведений, отказы, уведомления) на запросы субъектов персональных данных, составленные в соответствии со статьей 14 главы 3 Закона, бланки общих уведомлений и разъяснений, бланк «Уведомление о завершении обработки ПДн», составленный в соответствии с пунктом 4 статьи 21 главы 4 Закона.

С помощью одного из бланков уведомления необходимо уведомить субъекта персональных данных об уничтожении его персональных данных (Бланк уведомления о завершении обработки персональных данных).

Важно: Уничтожение персональных данных, позволяющих определить субъекта персональных данных, производится по достижении целей обработки, в случае утраты необходимости в достижении целей, по письменному заявлению субъекта персональных данных или по истечению срока обработки персональных данных.

Более подробная информация указана в разделе 12.1 «Методических рекомендаций».

4.2 ОСНОВНАЯ ДОКУМЕНТАЦИЯ

Данные документы являются обязательными для прохождения проверки Роскомнадзора:

Отчет о результатах проведения внутренней проверки;

Акты классификации ИСПДн;

Модель угроз ИСПДн.

4.3 ЗАЩИТА ПРАВ СУБЪЕКТОВ

Для соответствия законодательству необходимо:

уведомить Роскомнадзор об обработке (о намерении осуществлять обработку) персональных данных. Для этого необходимо в соответствии с «Рекомендациями по заполнению уведомления об обработке» заполнить и отослать в Роскомнадзор уведомление (Приложение 25 «Уведомление в Роскомнадзор»). Это также можно сделать через официальный сайт Роскомнадзора www.rsoc.ru;

получать согласие субъекта. От сотрудников согласие берётся при устройстве на работу («Согласие сотрудника на обработку ПДн»), согласие за несовершеннолетних учащихся дают их родители или опекуны (согласие должно быть оговорено в договоре или в заявлении на обучение). Если обрабатываемые персональные данные содержат только ФИО, то согласие от субъекта не требуется. Сотрудники должны подписывать соглашение о неразглашении информации («Соглашение о неразглашении ПДн»). При необходимости, например, при размещении информации на сайте, учителя могут давать подписку о том, что часть их персональных данных (ФИО, фото и стаж) является общедоступной.

5 МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Согласия сотрудников об обработке и неразглашении должны храниться в отделе кадров. Согласия родителей или опекунов на обработку их персональных данных и персональных данных учащихся должны храниться в отделе кадров или у директора (секретаря). Их наличие необходимо при проверке Роскомнадзора.

Доступ в помещения, где производится обработка персональных данных или хранение материальных носителей персональных данных, должен быть ограничен.

На компьютерах, являющихся частью ИСПДн, необходимо устанавливать антивирусное программное обеспечение. При наличии удалённого доступа к системе нужно применять межсетевые экраны. Требования для обеспечения защиты персональных данных при обработке обезличенных персональных данных устанавливает, в соответствии с законодательством, само учреждение, поэтому устанавливать дополнительные средства защиты рекомендуется только при наличии соответствующего финансирования.

В целях защиты элементов ИСПДн и обрабатываемой информации необходимо:

- вести резервное копирование персональных данных (не реже раза в неделю);
- ключевые элементы системы подключать к сети электропитания через источники бесперебойного питания;
- обеспечивать вентиляцию и кондиционирование помещений, содержащих элементы ИСПДн;
- иметь в наличии установочные файлы необходимого программного обеспечения.

Приложение 1

ОТЧЕТ О РЕЗУЛЬТАТАХ ПРОВЕДЕНИЯ ВНУТРЕННЕЙ ПРОВЕРКИ

На 87 листах

Краснодар, 2011

Содержание

КЛАССИФИКАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ, ОБРАБАТЫВАЮЩЕЙ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

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

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и / или воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

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

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и / или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

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 соответствующими описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

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

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 и 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.

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 и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

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

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

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства,

средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации),

программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

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

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

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

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

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

Учреждение – государственное образовательное учреждение города Москвы.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АВС	-	антивирусные средства
АИС	-	автоматизированная информационная система
АРМ	-	автоматизированное рабочее место
ИНН	-	индивидуальный номер налогоплательщика
ИСПДн	-	информационная система персональных данных
ЛВС	-	локальная вычислительная сеть
ЛИС	-	локальная информационная система
МЭ	-	межсетевой экран
НСД	-	несанкционированный доступ
ОС	-	операционная система
ПДн	-	персональные данные
ПМВ	-	программно-математическое воздействие
ПО	-	программное обеспечение
ПФ	-	пенсионный фонд
ПЭМИН	-	побочные электромагнитные излучения и наводки
РИС	-	распределенная информационная система
СЗИ	-	средства защиты информации
СЗПДн	-	система (подсистема) защиты персональных данных
ТКУИ	-	технические каналы утечки информации
УБПДн	-	угрозы безопасности персональных данных
ФСТЭК России	-	Федеральная служба по техническому и экспортному контролю – федеральный орган исполнительной власти России, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности.

ВВЕДЕНИЕ

Внутренняя проверка (далее – Проверка) произведена на основании Приказа №*(номер приказа о проведении внутренней проверки)*.

Проверка проводилась (*дата проведения проверки*) на территории Учреждения (*наименование учреждения, номер)* по адресу: *(адрес учреждения)*.

Проверка проводилась в соответствии с принципами и положениями Концепции информационной безопасности и Политики информационной безопасности.

В ходе проверки были выявлены следующие ИСПДн:

- (*список выявленных ИСПДн, например, «Школьный офис»).*

В ходе проверки для каждой ИСПДн определялось:

- состав и структура объектов защиты;
- конфигурация и структура ИСПДн;
- режим обработки ПДн;
- перечень лиц участвующих в обработке ПДн;
- права доступа лиц, допущенных к обработке ПДн;
- угрозы безопасности персональных данных. Оценивалась вероятность их реализации, реализуемость, опасность и актуальность;
- существующие меры защиты ПДн;
- список необходимых мер защиты ПДн.

Данные Проверки служат основой для других нормативно-организационных документов.

Данные о составе и структуре объектов защиты отражаются в Перечне персональных данных, подлежащих защите.

Данные о составе и структуре обрабатываемых персональных данных, конфигурации ИСПДн и режиме обработке являются основой для составления Акта классификации информационной системы, обрабатывающей персональные данные.

Данные о лицах, допущенных к обработке ПДн, и уровне их доступа отражаются в Положении о разграничении прав доступа к обрабатываемым персональным данным.

Данные об угрозах безопасности ПДн служат основной для составления Модели угроз безопасности персональных данных.

Данные о существующих и необходимых мерах защиты ПДн служат основной для составления Плана мероприятий по обеспечению защиты ПДн.

6 ИНФОРМАЦИОННАЯ СИСТЕМА, ОБРАБАТЫВАЮЩАЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ «ШКОЛЬНЫЙ ОФИС»

6.1 СТРУКТУРА ИСПДН

Таблица 1. Параметры

ИСПДн

6.2 СОСТАВ И СТРУКТУРА ПЕРСОНАЛЬНЫХ ДАННЫХ

В ИСПДн обрабатываются следующие персональные данные:

- ФИО сотрудников;
- табельный номер;
- номера домашнего и мобильного телефонов;
- ФИО учащихся;
- дата рождения.

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся к **4 категории персональных данных,** т.е. к данным, не позволяющим идентифицировать субъекта персональных данных.

Объем обрабатываемых персональных данных **не превышает 1000 записей** о субъектах персональных данных.

В соответствии с Порядком проведения классификации информационных систем персональных данных утвержденного приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20, на основании категории и объема обрабатываемых персональных данных – **ИСПДн** *«Школьный офис»* **классифицируется как специальная ИСПДн класса К4.**

Так же в ИСПДн существуют следующие объекты защиты:

- технологическая информация:
    - управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);

- технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
- информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
- информация о СЗПДн, их составе и структуре, принципах и технических решениях защиты;
- информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
- служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки обрабатываемой информации.

– технические средства обработки:
  - общее и специальное программное обеспечение, участвующее в обработке ПДн (операционные системы, СУБД, клиент-серверные приложения и другие);
  - резервные копии общесистемного программного обеспечения;
  - инструментальные средства и утилиты систем управления ресурсами ИСПДн;
  - аппаратные средства обработки ПДн (АРМ и сервера);
– сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.);
– средства защиты ПДн:
  - средства управления и разграничения доступа пользователей;
  - средства обеспечения регистрации и учета действий с информацией;
  - средства, обеспечивающие целостность данных;
  - средства антивирусной защиты;
  - средства межсетевого экранирования;
  - средства анализа защищенности;
  - средства обнаружения вторжений;
  - средства криптографической защиты ПДн, при их передачи по каналам связи сетей общего и (или) международного обмена.
– каналы информационного обмена и телекоммуникации;
– объекты и помещения, в которых размещены компоненты ИСПДн.

6.3 Структура обработки ПДн

В ИСПДн *«Школьный офис»* обработка персональных данных происходит следующим образом:

– сотрудник авторизуется на своем рабочем месте в ОС Windows XP;

- сотрудник авторизуется в ПО *«Школьный офис»;*

- сотрудник вносит персональные данные об учащихся или о сотрудниках;
- данные хранятся в БД на АРМ.

6.4 Режим обработки ПДн

В ИСПДн *«Школьный офис»* обработка персональных данных осуществляется в многопользовательском режиме с разграничением прав доступа.

Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в таблице.

Таблица 2. Матрица доступа

Группа	Уровень доступа к ПДн	Разрешенные действия	Сотрудники отдела
Администраторы ИСПДн	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Отдел информационных технологий

Администратор безопасности	Обладает правами Администратора ИСПДн. 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).	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Петров П.П.
Операторы ИСПДн с правами записи	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Отдел бухгалтерии
Операторы ИСПДн с правами чтения	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к подмножеству ПДн.	- использование	Сотрудники отдела кадров

В ИСПДн осуществляют работу следующие сотрудники.

Таблица 3. Перечень сотрудников

№	Роль	ФИО сотрудника	Подразделение
	Администратор ИСПДн	Иванов И.И.	
	Администратор ИСПДн	Петров П.П.	
	Оператор	Сидорова А.А.	

6.5 Угрозы безопасности ПДн

При обработке персональных данных в ИСПДн можно выделить следующие угрозы:

- 1. Угрозы от утечки по техническим каналам:
- 1.1. Угрозы утечки акустической информации;
- 1.2. Угрозы утечки видовой информации;
- 1.3. Угрозы утечки информации по каналам ПЭМИН.
- 2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа:
- 2.1. Кража и уничтожение носителей информации;
- 2.2. Кража физических носителей ключей и атрибутов доступа;
- 2.3. Утрата носителей информации;
- 2.4. Утрата и компрометация ключей и атрибутов доступа.
- 3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств:
- 3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа;
- 3.2. Утечка информации через порты ввода/вывода;
- 3.3. Воздействие вредоносных программ (вирусов);
- 3.4. Установка ПО, не связанного с исполнением служебных обязанностей;
- 3.5. Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных;
- 3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему.
- 4. Угрозы несанкционированного доступа к информации по каналам связи:
- 4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны;
- 4.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;
- 4.3. Угрозы выявления паролей по сети;
- 4.4. Угрозы типа «Отказ в обслуживании»;
- 4.5. Угрозы внедрения по сети вредоносных программ;
- 4.6.Утечка информации, передаваемой с использованием протоколов беспроводного доступа;
- 4.7. Перехват, модификация закрытого ключа ЭЦП;
- 4.8. Угрозы удаленного запуска приложений.

- 5. Угрозы антропогенного характера:
- 5.1. Разглашение информации;
- 5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов;
- 5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей;
- 5.4. Угроза нарушения политики предоставления и прекращения доступа;
- 5.5. Непреднамеренная модификация (уничтожение) информации;
- 5.6. Непреднамеренное отключение средств защиты.
- 6. Угрозы воздействия непреодолимых сил:
- 6.1. Стихийное бедствие;
- 6.2. Выход из строя аппаратно-программных средств;
- 6.3. Аварии (пожар, потоп, случайное отключение электричества).

Анализ вероятности реализации, реализуемости, опасности и актуальности угроз представлен в Модели угроз.

6.6 СУЩЕСТВУЮЩИЕ МЕРЫ ЗАЩИТЫ

Существующие в ИСПДн технические меры защиты представлены в таблице ниже.

Таблица 4. Меры защиты

Элемент ИСПДн	Программное средство обработки ПДн	Установленные средства защиты
АРМ пользователя	ОС Windows XP Браузер	Средства ОС: – управление и разграничение доступа пользователей; – регистрацию и учет действий с информацией. Антивирус *Касперский* – регистрацию и учет действий с информацией; – обеспечивать целостность данных; – производить обнаружений вторжений.

СУБД	1С: Бухгалтерия	Средства БД Средства ОС: − управление и разграничение доступа пользователей; − регистрацию и учет действий с информацией; − обеспечивать целостность данных; − производить обнаружений вторжений.

В ИСПДн введены следующие организационные меры защиты:

− в Учреждении осуществляется контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания;

− ведется учет носителей информации;

− носители информации хранятся в сейфе;

− в Учреждении существует отдел/ответственный сотрудник за обеспечение безопасности ПДн;

− в Учреждении проводятся периодические внутренние проверки режима безопасности ПДн;

− введена парольная политика, устанавливающая сложность ключей и атрибутов доступа (паролей), а так же их периодическую смену;

− пользователи осведомлены и проинструктированы о порядке работы и защиты персональных данных;

− осуществляется резервное копирование защищаемой информации;

− в помещениях, где расположены элементы ИСПДн, установлена пожарная сигнализация.

6.7 Необходимые меры защиты

На основании анализа актуальности выявленных угроз безопасности, для достижения требуемого уровня защиты рекомендуется осуществить следующие мероприятия:

− установка антивирусной защиты;

− парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

− назначить ответственного за безопасность персональных данных из числа сотрудников учреждения;

− инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а так же с ключами и атрибутами доступа;

− осуществление резервирования ключевых элементов ИСПДн;

− изолирование портов ввода/вывода;

− организация разграничения прав пользователей на установку стороннего ПО, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов ИСПДн и средств защиты.

Приложение 2

УТВЕРЖДАЮ

Распорядительный директор
Н(Ч)ОУ СОШ «КМШ»

О.В. Агрова

« » 2011 г.

АКТ

КЛАССИФИКАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ, ОБРАБАТЫВАЮЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

«ШКОЛЬНЫЙ ОФИС»

По результатам проведенного анализа исходных данных, собранных при внутренней проверке, проведенной по приказу № *(номер приказа)* от *(дата приказа)*, утвержденному *(должность руководителя, фамилия и инициалы)*, для информационной системы персональных данных «Школьный офис» выявлены следующие характеристики:

Категория обрабатываемых персональных данных	Хпд: 4
Объем обрабатываемых персональных данных	Хпдн: 3
Заданные характеристики безопасности персональных данных	Специальная информационная система
Структура информационной системы	Автоматизированное рабочее место
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	Имеется
Режим обработки персональных данных	Многопользовательская система
Режим разграничения прав доступа пользователей	Система с разграничением доступа
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации
Дополнительная информация	К персональным данным предъявляется требование целостности и (или) доступности
Тип информационной системы персональных данных	Специальная

На основании полученных данных *и в соответствии с моделью угроз персональных данных* (для специальных информационных систем) информационной системе персональных данных «Школьный офис» присвоен класс К4.

Председатель комиссии

(ФИО) - (должность) Члены комиссии:

(ФИО) - (должность)

(ФИО) - (должность)

(ФИО) - (должность)

Приложение 3

ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ «ШКОЛЬНЫЙ ОФИС»

На 87 листах

Краснодар, 2011

СОДЕРЖАНИЕ

АКТ47

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

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

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и / или воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

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

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и / или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

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 соответствующими описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

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

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 и 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.

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 и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

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

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

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства,

средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации),

программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

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

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

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

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

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

Учреждение – образовательное учреждение города Москвы.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АВС	-	антивирусные средства
АИС	-	автоматизированная информационная система
АРМ	-	автоматизированное рабочее место
АС	-	Автоматизированная система
ИНН	-	индивидуальный номер налогоплательщика
ИСПДн	-	информационная система персональных данных
ЛВС	-	локальная вычислительная сеть
ЛИС	-	локальная информационная система
МЭ	-	межсетевой экран
НСД	-	несанкционированный доступ
ОС	-	операционная система
ПДн	-	персональные данные
ПМВ	-	программно-математическое воздействие
ПО	-	программное обеспечение
ПФ	-	пенсионный фонд
ПЭМИН	-	побочные электромагнитные излучения и наводки
РИС	-	распределенная информационная система
СЗИ	-	средства защиты информации
СЗПДн	-	система (подсистема) защиты персональных данных
ТКУИ	-	технические каналы утечки информации
УБПДн	-	угрозы безопасности персональных данных
ФСТЭК России	-	Федеральная служба по техническому и экспортному контролю – федеральный орган исполнительной власти России, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности.

ВВЕДЕНИЕ

Модель угроз безопасности персональных данных (далее – Модель) при их обработке в ИСПДн *«Школьный офис»* строится на основании Отчета о результатах проведения внутренней проверки.

В модели угроз представлено описание структуры ИСПДн, состава и режима обработки ПДн, классификации потенциальных нарушителей, оценку 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.

В заключении даны рекомендации по мерам защиты для уменьшения опасности актуальных угроз.

7 ИСПДН «ШКОЛЬНЫЙ ОФИС»

7.1 Структура ИСПДн

Таблица 5 – Параметры ИСПДн

Заданные характеристики безопасности персональных данных	Специальная информационная система
Структура информационной системы	Автоматизированное рабочее место
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	Имеется
Режим обработки персональных данных	Многопользовательская
Режим разграничения прав доступа пользователей	Система с разграничением доступа
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации
Дополнительные информация	К персональным данным предъявляется требование целостности и (или) доступности

7.2 Состав и структура персональных данных

В ИСПДн обрабатываются следующие персональные данные:

- ФИО сотрудников;
- табельный номер;
- номера домашнего и мобильного телефонов;
- ФИО учащихся;
- дата рождения.

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся к **4 категории персональных данных,** т.е. к данным, позволяющим идентифицировать субъекта персональных данных.

Объем обрабатываемых персональных данных, **не превышает 1000 записей** о субъектах персональных данных.

7.3 Структура обработки ПДн

В ИСПДн *«Школьный офис»* обработка персональных данных происходит следующим образом:

- сотрудник авторизуется на своем рабочем месте в ОС Microsoft Windows XP;
- сотрудник авторизуется в ПО *«Школьный офис»;*
- сотрудник вносит персональные данные об учащихся или о сотрудниках;

- данные хранятся в БД на АРМ.

7.4 РЕЖИМ ОБРАБОТКИ ПДН

В ИСПДн *«Школьный офис»* обработка персональных данных осуществляется в однопользовательском режиме без разграничения прав доступа.

Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в таблице.

Таблица 6. Матрица доступа

Группа	Уровень доступа к ПДн	Разрешенные действия
Администраторы ИСПДн	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение
Администратор безопасности	Обладает правами Администратора ИСПДн. 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).	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение

Операторы ИСПДн с правами записи	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение
Операторы ИСПДн с правами чтения	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к подмножеству ПДн.	- использование

7.5 КЛАССИФИКАЦИЯ НАРУШИТЕЛЕЙ

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

− внешние нарушители – физические лица, осуществляющие целенаправленное деструктивное воздействие, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;

− внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

7.5.1 Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИСПДн, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных утечку информации по техническим каналам утечки.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи.

7.5.2 Внутренний нарушитель

К такому виду нарушителя могут относиться (список лиц должен быть уточнен в соответствии с группами пользователей описанных в Политике информационной безопасности):

− пользователи ИСПДн, т.е. сотрудники, имеющие право доступа к ИСПДн (категория I);

− сотрудники, не имеющие права доступа к ИСПДн (категория II);

− администраторы ИСПДн (категория III);

− разработчики и поставщики программно-технических средств, расходных материалов, услуг (категория IV).

Возможности нарушителей 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.

Лица категорий I и III (пользователи и администраторы ИСПДн) хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также с применяемыми принципами и концепциями безопасности.

Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Кроме того, предполагается, что эти лица могли бы располагать специализированным оборудованием.

К лицам данных категорий ввиду их исключительной роли в ИСПДн должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

7.5.3 Предположения об имеющейся у нарушителя информации об объектах реализации угроз

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

- *общая информация* – информации о назначения и общих характеристиках ИСПДн;
- *эксплуатационная информация* – информация, полученная из эксплуатационной документации;
- *чувствительная информация* – информация, дополняющая эксплуатационную информацию об ИСПДн (например, сведения из проектной документации ИСПДн).

В частности, нарушитель может иметь:

- данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн;
- сведения об информационных ресурсах ИСПДн: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;
- данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИСПДн;
- данные о реализованных в ПСЗИ принципах и алгоритмах;
- исходные тексты программного обеспечения ИСПДн;
- сведения о возможных каналах реализации угроз;
- информацию о способах реализации угроз.

Предполагается, что лица категории I (пользователи ИСПДн) владеют только эксплуатационной информацией, что обеспечивается организационными мерами.

Предполагается, что лица категории III (администраторы ИСПДн) обладают чувствительной информацией об ИСПДн и функционально ориентированных АИС, включая информацию об уязвимостях технических и программных средств ИСПДн.

Степень информированности нарушителя зависит от многих факторов, включая

реализованные конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, с целью создания определенного запаса прочности предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

7.5.4 Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель имеет:

- аппаратные компоненты СЗПДн и СФ СЗПДн;
- доступные в свободной продаже технические средства и программное обеспечение;
- специально разработанные технические средства и программное обеспечение.

Для создания устойчивой СЗПДн предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

- средств перехвата в технических каналах утечки;
- средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);
- средств воздействия на источники и через цепи питания;
- средств воздействия через цепи заземления;
- средств активного воздействия на технические средства (средств облучения).

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории III и лица категории IV (администраторы и разработчики ИСПДн).

Необходимо определить всех потенциальных нарушителей, не имеющих доступа в ИСПДн, всех пользователей ИСПДн и определить их категорию.

7.6 Исходный уровень защищенности ИСПДн

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

В таблице представлены характеристики уровня исходной защищенности для ИСПДн «Школьный офис».

Таблица 7. Исходный уровень защищенности

Позиция	Технические и эксплуатационные характеристики	Уровень защищенности
1	По территориальному размещению	высокий
2	По наличию соединения с сетями общего пользования	высокий

3	По встроенным (легальным) операциям с записями баз персональных данных	средний
4	По разграничению доступа к персональным данным	средний
5	По наличию соединений с другими базами ПДн иных ИСПДн	высокий
6	По уровню (обезличивания) ПДн	средний
7	По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	средний

7.7 Вероятность реализации УБПДн

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

− **маловероятно -** отсутствуют объективные предпосылки для осуществления угрозы ($Y_2 = 0$);

− **низкая вероятность** - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию ($Y_2 = 2$);

− **средняя вероятность** - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны ($Y_2 = 5$);

− **высокая вероятность** - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты ($Y_2 = 10$).

При обработке персональных данных в ИСПДн можно выделить следующие угрозы.

7.7.1 Угрозы утечки информации по техническим каналам

7.7.1.1 Угрозы утечки акустической (речевой) информации

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

В ИСПДн Учреждений функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют. Поэтому для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

7.7.1.2 Угрозы утечки видовой информации

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

Если в Учреждении введен контроль доступа в контролируемую зону, АРМ пользователей расположены так, что практически исключен визуальный доступ к

мониторам, а на окнах установлены жалюзи, то для всех типов ИСПДн вероятность реализации угрозы – является маловероятной.

Если в Учреждении отсутствуют вышеперечисленные меры защиты, то их необходимо внедрить.

7.7.1.3 Угрозы утечки информации по каналам ПЭМИН

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия паразитных электромагнитных излучений у элементов ИСПДн.

Угрозы данного класса маловероятны для всех видов ИСПДн, т.к. размер контролируемой зоны большой, и элементы ИСПДн зачастую находятся в самом центре здания и экранируются несколькими несущими стенами, а паразитный сигнал маскируется со множеством других паразитных сигналов элементов, не входящих в ИСПДн.

7.7.2 Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам 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).

7.7.2.1 Кража и уничтожение носителей информации

Угроза осуществляется всеми видами нарушителей.

Если в Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, ведется учет и хранение носителей в сейфе, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

При наличии свободного доступа в контролируемую зону посторонних лиц вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры по пресечению НСД посторонних лиц к носителям информации.

7.7.2.2 Кража физических носителей ключей и атрибутов доступа

Угроза осуществляется всеми видами нарушителей.

Вероятность реализации угрозы повышается при наличии свободного доступа в контролируемую зону посторонних лиц.

Если в Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, ведется учет и хранение носителей в сейфе, то для всех видов ИСПДн вероятность реализации угрозы – является низкой.

При отсутствии парольной политики или контроля за ее исполнением, вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры по организации парольной политики.

7.7.2.3 Утрата носителей информации

Угроза осуществляется внутренними нарушителями, являющимися пользователями ИСПДн, вследствие человеческого фактора.

Если в Учреждении осуществляется учет носителей информации и пользователи проинструктированы о действиях в случаях утраты носителей, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

7.7.2.4 Утрата и компрометация ключей и атрибутов доступа

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политики в части их создания (создают простые 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.

Если в Учреждении введена парольная политика, предусматривающая требуемую сложность пароля и периодическую его смену, введена политика «чистого стола», осуществляется контроль за выполнением правил политик, пользователи проинструктированы о парольной политике и о действиях в случаях утраты или компрометации паролей, то для всех видов ИСПДн вероятность реализации угрозы – является низкой.

При отсутствии парольной политики или контроля за ее исполнением, вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры по организации парольной политики.

7.7.3 Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств

7.7.3.1 Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа

Угроза осуществляется внешними нарушителями и внутренними нарушителями категорий II и IV там, где расположены элементы ИСПДн и средства защиты, а так же происходит работа пользователей.

Если в Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

При наличии свободного доступа в контролируемую зону посторонних лиц, вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры по пресечению НСД в контролируемую зону.

7.7.3.2 Утечка информации через порты ввода/вывода

Угроза осуществляется внутренними нарушителями категорий I и IV (пользователи и разработчики ИСПДн).

Угроза реализуется путем подключения съемных носителей к компьютеру и несанкционированного копирования на них информации.

Если в Учреждении порты ввода/вывода изолированы, пользователи ознакомлены с политикой безопасности, то для всех видов ИСПДн вероятность реализации угрозы – является низкой.

Вероятность реализации угрозы может быть пересмотрена при отсутствии ограничений использования съемных носителей информации.

7.7.3.3 Воздействие 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.

Если в Учреждении на всех элементах ИСПДн установлена антивирусная защита, пользователи проинструктированы о мерах предотвращения вирусного заражения, то для всех видов ИСПДн вероятность реализации угрозы – является низкой.

При отсутствии установленной антивирусной защиты, вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры по предотвращению угроз вирусного заражения.

7.7.3.4 Установка ПО, не связанного с исполнением служебных обязанностей

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями категорий I и IV (пользователи и разработчики ИСПДн).

Если в Учреждении введено разграничение прав пользователей на установку ПО и осуществляется контроль, пользователи проинструктированы о политике установки ПО, то для всех видов ИСПДн вероятность реализации угрозы – является низкой.

При отсутствии разграничения прав на установку ПО, вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры по организации разграничения прав пользователей.

7.7.3.5 Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных

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.

Если в Учреждении осуществляется контроль действий пользователей и разработчиков, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

При увеличении элементов, в том числе программного обеспечения, ИСПДн, числа функциональных связей между элементами и при наличии подключения к сетям общего доступа и (или) международного обмена вероятность реализации данной угрозы должна быть пересмотрена.

Для снижения вероятности реализации угрозы необходимо сертифицировать ПО

собственной разработки или стандартное ПО, доработанное под нужды учреждения.

7.7.3.6 Создание учетных записей теневых пользователей и неучтенных точек доступа в систему

Угроза осуществляется внутренними нарушителями категорий I и IV (пользователи и разработчики ИСПДн).

Угроза реализуется путем несанкционированного создания неучтенных точек доступа в систему (например, несанкционированное подключение нового компьютера к локальной сети), а также создание нерабочих учетных записей (тестовых, временных и т.д.).

Вероятность реализации угрозы повышается при отсутствии контроля действий пользователей и разработчиков.

Вероятность реализации угрозы – является маловероятной.

7.7.4 Угрозы несанкционированного доступа к информации по каналам связи

7.7.4.1 Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль. В ходе реализации угрозы нарушитель:

− изучает логику работы ИСПДн - то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней;

− перехватывает поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TELNET, не предусматривающих шифрование), ее подмены, модификации и т.п.

Вероятность реализации угрозы для всех видов ИСПДн – является маловероятной.

7.7.4.2 Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.

Сущность процесса реализации угрозы заключается в передаче 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.

Вероятность реализации угрозы для всех видов ИСПДн – является маловероятной.

7.7.4.3 Угроза выявления паролей по сети

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов,

таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

Вероятность реализации угрозы – является маловероятной.

7.7.4.4 Угрозы типа «Отказ в обслуживании»

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Могут быть выделены несколько разновидностей таких угроз:

- скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;
- явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);
- явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;
- явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, которое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИСПДн из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – является маловероятной.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

7.7.4.5 Угрозы внедрения по сети вредоносных программ

К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию.

«Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

- программы подбора и вскрытия паролей;
- программы, реализующие угрозы;
- программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИСПДн;
- программы-генераторы компьютерных вирусов;
- программы, демонстрирующие уязвимости средств защиты информации и др.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, установлена антивирусная защита, то вероятность реализации угрозы – является маловероятной.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

7.7.4.6 Утечка информации, передаваемой с использованием протоколов беспроводного доступа

Угроза реализуется путем перехвата информации, передаваемой по беспроводным сетям.

Если в Учреждении производится контроль трафика, проходящего по беспроводным сетям, то вероятность реализации угрозы – является маловероятной.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

7.7.4.7 Перехват, модификация закрытого ключа ЭЦП

Угроза реализуется путем получения доступа к закрытому ключу ЭЦП либо путем перехвата закрытого ключа ЭЦП.

Вероятность реализации угрозы – является маловероятной.

7.7.4.8 Угрозы удаленного запуска приложений

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы,

«сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. 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, Net Bus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, установлена антивирусная защита, то вероятность реализации угрозы – является маловероятной.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

7.7.5 Угрозы антропогенного характера

7.7.5.1 Разглашение информации

Угроза осуществляется внутренними нарушителями категорий I и III (пользователи и администраторы ИСПДн).

Угроза реализуется путем несанкционированной передачи информации третьим лицам.

Если в Учреждении пользователи осведомлены о порядке работы с персональными данными, а так же подписали Договор о неразглашении, то для всех видов ИСПДн вероятность реализации угрозы – является низкой.

При неосведомленности пользователей и не заключении Договора о неразглашении, вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры снижению вероятности реализации угрозы.

7.7.5.2 Сокрытие ошибок и неправомерных действий пользователей и администраторов

Угроза реализуется внутренними нарушителями категорий I и III (пользователи и администраторы ИСПДн).

Если в Учреждении осуществляется контроль действий пользователей, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

При отсутствии контроля действий пользователей вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры по установлению контроля.

7.7.5.3 Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей

Угроза реализуется внутренними нарушителями категории III (администраторы ИСПДн).

Угроза реализуется вследствие халатного отношения ответственного лица к своим должностным обязанностям.

Если в Учреждении осуществляется контроль действий ответственных лиц, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

При отсутствии контроля действий ответственных лиц вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры по установлению контроля.

7.7.6 Угроза нарушения политики предоставления и прекращения доступа

Угроза реализуется внутренними нарушителями категории III (администраторы ИСПДн).

Угроза реализуется при отсутствии процедуры удаления устаревших, неучтенных или недействующих учетных записей пользователей или несанкционированного предоставления прав доступа.

Вероятность реализации угрозы повышается при отсутствии контроля действий администраторов.

Вероятность реализации угрозы – является маловероятной.

7.7.6.1 Непреднамеренная модификация (уничтожение) информации

Угроза реализуется внутренними нарушителями категорий I и III (пользователи и администраторы ИСПДн).

Угроза реализуется путем непреднамеренного воздействия на элементы ИСПДн или содержащуюся в ней информацию.

Если в Учреждении осуществляется резервное копирование обрабатываемых ПДн, пользователи проинструктированы о работе с ИСПДн, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

При отсутствии резервного копирования и неосведомленности пользователей о работе с ИСПДн, вероятность реализации угрозы должна быть пересмотрена , и необходимо принять меры снижению вероятности реализации угрозы.

7.7.6.2 Непреднамеренное отключение средств защиты

Угроза реализуется внутренними нарушителями категорий I и III (пользователи и администраторы ИСПДн).

Угроза реализуется путем случайного отключения средств защиты (антивирусного ПО, межсетевых экранов и т.д.).

Вероятность реализации угрозы повышается при отсутствии контроля доступа в контролируемую зону и к настройкам режимов средств защиты, а так же неосведомленности пользователей о работе с ИСПДн.

Вероятность реализации угрозы для всех видов ИСПДн – является маловероятной.

7.7.7 Угрозы воздействия непреодолимых сил

7.7.7.1 Стихийное бедствие

Угроза осуществляется вследствие возникновения различного рода природных

катаклизмов (землетрясение, затопление и прочее).

Если в Учреждении сотрудники проинструктированы о действиях в случае возникновения внештатных ситуаций, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

При отсутствии пожарной сигнализации и неосведомленности пользователей о действиях в случае возникновения внештатных ситуаций, вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры снижению вероятности реализации угрозы.

7.7.7.2 Выход из строя аппаратно-программных средств

Угроза реализуется вследствие окончания срока эксплуатации аппаратно-программных средств, нерегулярных проверок данных средств и перебоев в электропитании.

Если в Учреждении производится своевременная замена устаревших аппаратно-программных средств, регулярные проверки аппаратно-программных средств и установлены элементы бесперебойного питания, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

В противном случае вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры снижению вероятности реализации угрозы.

7.7.7.3 Аварии (пожар, потоп, случайное отключение электричества)

Угроза осуществляется вследствие возникновения различного рода аварий в пределах контролируемой зоны.

Если в Учреждении производится своевременная замена устаревшего оборудования, коммуникаций и т.д., проводятся их регулярные проверки, установлены элементы бесперебойного питания, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

В противном случае вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры снижению вероятности реализации угрозы.

7.8 РЕАЛИЗУЕМОСТЬ УГРОЗ

По итогам оценки уровня защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением Y = (Y1 + Y2)/20.

Оценка реализуемости УБПДн представлена в таблице.

Таблица 8. Реализуемость УБПДн

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам		
1.1. Угрозы утечки акустической информации	0,25	низкая
1.2. Угрозы утечки видовой информации	0,25	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	0,25	низкая

2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа		
2.1. Кража и уничтожение носителей информации	0,25	низкая
2.2. Кража физических носителей ключей и атрибутов доступа	0,25	средняя
2.3. Утрата носителей информации	0,25	низкая
2.4. Утрата и компрометация ключей и атрибутов доступа	0,35	средняя
3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств		
3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа	0,35	низкая
3.2. Утечка информации через порты ввода/вывода	0,25	средняя
3.3. Воздействие вредоносных программ (вирусов)	0,35	средняя
3.4. Установка ПО, не связанного с исполнением служебных обязанностей	0,35	средняя
3.5. Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных	0,35	низкая
3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему	0,25	низкая
4. Угрозы несанкционированного доступа к информации по каналам связи		
4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны	0,25	низкая
4.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	0,25	низкая
4.3. Угрозы выявления паролей по сети	0,25	низкая
4.4. Угрозы типа «Отказ в обслуживании»	0,25	низкая
4.5. Угрозы внедрения по сети вредоносных программ	0,25	низкая
4.6.Утечка информации, передаваемой с использованием протоколов беспроводного доступа	0,25	низкая

4.7. Перехват, модификация закрытого ключа ЭЦП	0,25	низкая
4.8. Угрозы удаленного запуска приложений	0,25	низкая
5. Угрозы антропогенного характера		
5.1. Разглашение информации	0,35	средняя
5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов	0,35	низкая
5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей	0,25	низкая
5.4. Угроза нарушения политики предоставления и прекращения доступа	0,25	низкая
5.5. Непреднамеренная модификация (уничтожение) информации	0,35	низкая
5.6. Непреднамеренное отключение средств защиты	0,25	низкая
6. Угрозы воздействия непреодолимых сил		
6.1. Стихийное бедствие	0,25	низкая
6.2. Выход из строя аппаратно-программных средств	0,25	низкая
6.3. Аварии (пожар, потоп, случайное отключение электричества)	0,25	низкая

7.9 ОЦЕНКА ОПАСНОСТИ УГРОЗ

Оценка опасности УБПДн производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

- низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
- средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
- высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Оценка опасности УБПДн представлена таблице.

Таблица 9. Опасность УБПДн

Тип угроз безопасности ПДн	Опасность угрозы
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	низкая
1.2. Угрозы утечки видовой информации	низкая

1.3. Угрозы утечки информации по каналам ПЭМИН	низкая
2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа	
2.1. Кража и уничтожение носителей информации	низкая
2.2. Кража физических носителей ключей и атрибутов доступа	средняя
2.3. Утрата носителей информации	низкая
2.4. Утрата и компрометация ключей и атрибутов доступа	средняя
3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств	
3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа	низкая
3.2. Утечка информации через порты ввода/вывода	средняя
3.3. Воздействие вредоносных программ (вирусов)	средняя
3.4. Установка ПО, не связанного с исполнением служебных обязанностей	средняя
3.5. Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных	низкая
3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему	низкая
4. Угрозы несанкционированного доступа к информации по каналам связи	
4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны	низкая
4.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	низкая
4.3. Угрозы выявления паролей по сети	низкая
4.4. Угрозы типа «Отказ в обслуживании»	низкая
4.5. Угрозы внедрения по сети вредоносных программ	низкая
4.6.Утечка информации, передаваемой с использованием протоколов беспроводного доступа	низкая
4.7. Перехват, модификация закрытого ключа ЭЦП	низкая
4.8. Угрозы удаленного запуска приложений	низкая
5. Угрозы антропогенного характера	
5.1. Разглашение информации	средняя
5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов	низкая
5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей	низкая
5.4. Угроза нарушения политики предоставления и прекращения доступа	низкая

5.5. Непреднамеренная модификация (уничтожение) информации	низкая
5.6. Непреднамеренное отключение средств защиты	низкая
6. Угрозы воздействия непреодолимых сил	
6.1. Стихийное бедствие	низкая
6.2. Выход из строя аппаратно-программных средств	низкая
6.3. Аварии (пожар, потоп, случайное отключение электричества)	низкая

7.10 Определение актуальности угроз в ИСПДн

В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИСПДн определяются актуальные и неактуальные угрозы.

Таблица 10. Правила определения актуальности УБПДн

Возможность реализации угрозы	**Показатель опасности угрозы**		
	Низкая	Средняя	Высокая
	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Оценка актуальности угроз безопасности представлена в таблице.

Таблица 11. Актуальность УБПДн

Тип угроз безопасности ПДн	**Опасность угрозы**
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	неактуальная
1.2. Угрозы утечки видовой информации	неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	неактуальная
2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа	
2.1. Кража и уничтожение носителей информации	неактуальная
2.2. Кража физических носителей ключей и атрибутов доступа	актуальная
2.3. Утрата носителей информации	неактуальная

2.4. Утрата и компрометация ключей и атрибутов доступа	актуальная
3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств	
3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа	неактуальная
3.2. Утечка информации через порты ввода/вывода	актуальная
3.3. Воздействие вредоносных программ (вирусов)	актуальная
3.4. Установка ПО, не связанного с исполнением служебных обязанностей	актуальная
3.5. Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных	неактуальная
3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему	неактуальная
4. Угрозы несанкционированного доступа к информации по каналам связи	
4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны	неактуальная
4.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	неактуальная
4.3. Угрозы выявления паролей по сети	неактуальная
4.4. Угрозы типа «Отказ в обслуживании»	неактуальная
4.5. Угрозы внедрения по сети вредоносных программ	неактуальная
4.6.Утечка информации, передаваемой с использованием протоколов беспроводного доступа	неактуальная
4.7. Перехват, модификация закрытого ключа ЭЦП	неактуальная
4.8. Угрозы удаленного запуска приложений	неактуальная
5. Угрозы антропогенного характера	
5.1. Разглашение информации	актуальная
5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов	неактуальная
5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей	неактуальная
5.4. Угроза нарушения политики предоставления и прекращения доступа	неактуальная
5.5. Непреднамеренная модификация (уничтожение) информации	неактуальная
5.6. Непреднамеренное отключение средств защиты	неактуальная
6. Угрозы воздействия непреодолимых сил	
6.1. Стихийное бедствие	неактуальная
6.2. Выход из строя аппаратно-программных средств	неактуальная

6.3. Аварии (пожар, потоп, случайное отключение электричества)	неактуальная

Были выявлены следующие актуальные угрозы:

- кража физических носителей ключей и атрибутов доступа;
- утрата и компрометация ключей и атрибутов доступа;
- утечка информации через порты ввода/вывода;
- воздействие вредоносных программ (вирусов);
- установка ПО, не связанного с исполнением служебных обязанностей;
- разглашение информации.

Для снижения опасности реализации актуальных УБПДн рекомендуется осуществить следующие мероприятия:

- установка антивирусной защиты;
- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;
- назначить ответственного за безопасность персональных данных из числа сотрудников учреждения;
- инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а так же с ключами и атрибутами доступа;
- осуществление резервирования ключевых элементов ИСПДн;
- изолирование портов ввода/вывода;
- организация разграничения прав пользователей на установку стороннего ПО, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов ИСПДн и средств защиты.

7.11 М

О
Д
Е
Л
Ь
У
Г
Р
О
З
Б
Е
З
О
П
А
С
Н
О
С
Т
И
И
с
х
о
д
н
ы
й
к
л
а
с
с
з
а
щ
и

щ
е
н
н
о
с
т
и
–
с
р
е
д
н
и
й

Т
а
б
л
и
ц
а
1
2
.
У
г
р
о
з
ы
б
е
з
о
п

а
с
н
о
с
т
и

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	
					Т
1. Угрозы от утечки по техническим каналам					
1.1. Угрозы утечки акустической информации	Маловероятно	Низкая	Низкая	Неактуальная	Виброг генера звукои
1.2. Угрозы утечки видовой информации	Маловероятно	Низкая	Низкая	Неактуальная	Жалюз
1.3. Угрозы утечки информации по каналам ПЭМИН	Маловероятно	Низкая	Низкая	Неактуальная	Генера простр зашум
					Генера цепи э
2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ключам и атрибутам доступа					
2.1. Кража и уничтожение носителей информации	Маловероятно	Низкая	Низкая	Неактуальная	Охран
					Хране
					Шифр

2.2. Кража физических носителей ключей и атрибутов доступа	Низкая	Средняя	Средняя	Актуальная	Хране
2.3. Утрата носителей информации	Маловероятно	Низкая	Низкая	Неактуальная	
2.4. Утрата и компрометация ключей и атрибутов доступа	Низкая	Средняя	Средняя	Актуальная	
3. Угрозы несанкционированного доступа к информации с использованием программно-аппарат					
3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа	Маловероятно	Низкая	Низкая	Неактуальная	Систем НСД
3.2. Утечка информации через порты ввода/вывода	Низкая	Средняя	Средняя	Актуальная	Изолир ввода/
3.3. Воздействие вредоносных программ (вирусов)	Низкая	Средняя	Средняя	Актуальная	Антив

3.4. Установка ПО не связанного с исполнением служебных обязанностей	Низкая	Средняя	Средняя	Актуальная	
3.5. Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных	Маловероятно	Низкая	Низкая	Неактуальная	
3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему	Маловероятно	Низкая	Низкая	Неактуальная	Систем доступ
4. Угрозы несанкционированного доступа к информации по каналам связи					
4.1. Угроза «Анализ сетевого трафика» с перехватом информации за	Маловероятно	Низкая	Низкая	Неактуальная	Межсе

пределами контролируемой зоны					
4.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	Маловероятно	Низкая	Низкая	Неактуальная	Межсе
4.3. Угрозы выявления паролей по сети	Маловероятно	Низкая	Низкая	Неактуальная	Межсе
4.4. Угрозы типа «Отказ в обслуживании»	Маловероятно	Низкая	Низкая	Неактуальная	Межсе Антив
4.5. Угрозы	Маловероятно	Низкая	Низкая	Неактуальная	Антив

внедрения по сети вредоносных программ					
4.6. Утечка информации, передаваемой с использованием протоколов беспроводного доступа	Маловероятно	Низкая	Низкая	Неактуальная	Шифр инфор
4.7. Перехват, модификация закрытого ключа ЭЦП	Маловероятно	Низкая	Низкая	Неактуальная	Межсе Антив
4.8. Угрозы удаленного запуска приложений	Маловероятно	Низкая	Низкая	Неактуальная	Межсе Антив
5. Угрозы антропогенного характера					
5.1. Разглашение	Низкая	Средняя	Средняя	Актуальная	

информации					
5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов	Маловероятно	Низкая	Низкая	Неактуальная	
5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей	Маловероятно	Низкая	Низкая	Неактуальная	
5.4. Угроза нарушения политики предоставления и прекращения доступа	Маловероятно	Низкая	Низкая	Неактуальная	
5.5. Непреднамеренная модификация (уничтожение) информации	Маловероятно	Низкая	Низкая	Неактуальная	Настро защит
5.6.	Маловероятно	Низкая	Низкая	Неактуальная	Доступ

Непреднамеренное отключение средств защиты					режим средст предос админ безопа
6. Угрозы воздействия непреодолимых сил					
6.1. Стихийное бедствие	Маловероятно	Низкая	Низкая	Неактуальная	Пожар сигнал
6.2. Выход из строя аппаратно-программных средств	Маловероятно	Низкая	Низкая	Неактуальная	Устрой беспер питани
6.3. Аварии (пожар, потоп, случайное отключение электричества)	Маловероятно	Низкая	Низкая	Неактуальная	Пожар сигнал

8 ЗАКЛЮЧЕНИЕ

В соответствии с Порядком проведения классификации информационных систем персональных данных утвержденного приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20, на основании категории и объема обрабатываемых персональных данных – ИСПДн *«Школьный офис»* классифицируется как специальная ИСПДн класса К4.

Аттестация ИСПДн *«Школьный офис»* не требуется.