«УТВЕРЖДАЮ»
Заведующий МАДОУ
детский сад № 9 «Сказка»
Коровкина Наталья Геннадьевна Н.Г.Коровкина

Модель угроз безопасности персональных данных при их обработке в информационной системы персональных данных МАДОУ детский сад №9 «Сказка»

В настоящем документе используются следующие термины и их определения:

Аутентификация отправители данных подтверждение того, что отправитель полученных данных соответствует заявленному.

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

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

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

Вредоносная программа — программа - предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

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

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

Доступ к информации возможность получения информации и 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 средств и системы обработки информации.

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

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

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

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

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 функциональнораспределенное 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.

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

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения

доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

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

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

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

Оператор (персональных данных) – муниципальный орган, юридическое лицо, организующее и осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

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.

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).

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

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

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

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

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить

информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

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

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

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

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

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

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

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

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

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

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

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

ВВЕДЕНИЕ

Работы по созданию Частной модели угроз безопасности персональных данных (Далее – Модель угроз), при их обработке в информационной системы персональных данных, (Далее – ИСПДн) проводятся в соответствии со следующими основными документами:

- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» ;
- Постановление Правительства РФ от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» ; - Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» ;
- Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» ;
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 15 февраля 2008г.);
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 14 февраля 2008г.).

Модель угроз может быть пересмотрена:

- по решению оператора на основе периодически проводимых им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;
- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

Модель угроз базируется на следующих принципах:

1) Безопасность персональных данных при их обработке в ИСПДн обеспечивается с помощью системы защиты персональных данных (СЗПДн).

2) При формировании модели угроз учитываются как угрозы, осуществление которых нарушает безопасность персональных данных (далее – прямая угроза), так и

угрозы, создающие условия для появления прямых угроз (далее – косвенные угрозы) или косвенных угроз.

3) Персональные данные обрабатываются и хранятся в информационной системе с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации.

4) Система защиты персональных данных не может обеспечить защиту информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СЗПДн не может обеспечить защиту информации от раскрытия лицами, которым предоставлено право на доступ к этой информации).

НАЗНАЧЕНИЕ, СТРУКТУРА И ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ИСПДн

ИСПДн предназначена для выполнения в электронном виде следующих основных процедур:

- прием заявлений родителей (законных представителей детей) для постановки на учет и в очередь на зачисление в дошкольное образовательное учреждение, внесение изменений в заявления, прием заявлений на перевод из одного учреждения в другое. Процедура приема заявлений родителей (законных представителей детей) реализуется в информационной системе в двух вариантах:

из регионального портала государственных услуг, единого портала государственных услуг, сайта информационной системы - Заявитель из «Личного кабинета» подает заявление и сам вводит все необходимые данные;

- формирование различных категорий получателей услуги с учетом льгот по состоянию здоровья и социальному положению детей.
- информирование законных представителей детей о ходе предоставления муниципальной услуги через «личный кабинет» регионального портала государственных услуг, единого портала государственных услуг, сайта информационной системы.

Предоставление услуги по приему заявлений и постановке на учет включает в себя следующие административные процедуры:

- предоставление заявителем заявления и документов, необходимых для постановки детей на учет для зачисления в образовательное учреждение;
- рассмотрение заявления и представленных документов заявителя;
- информирование заявителя о принятом решении: постановка ребенка на учет (с выдачей заявителю уведомления о постановки ребенка на учет) либо мотивированный отказ.

Принимая во внимание, что решение о постановке на учет и зачислении детей в образовательные учреждения, реализующие основную образовательную программу дошкольного образования не принимается на основании исключительно автоматизированной обработки персональных данных в отношении субъекта персональных данных[1], то процедура «рассмотрение заявления и представленных документов заявителя» начинается после представления Заявителем оригиналов документов (См. блок-схему предоставления муниципальной услуги).

Автоматизированный расчет производится с учетом возраста ребенка, даты подачи заявления на зачисление/перевод, льгот, предпочтений родителей в выборе дошкольного учреждения по следующему алгоритму:

Заявления, которые находятся в очереди, автоматически пересчитываются раз в сутки в 00:00 (по времени того сервера, на котором установлена Система). Результаты пересчета очереди дают Заявителю информацию для приблизительного прогноза о том, попадет ли его заявление в ближайшее распределение в детские сады.

Результаты пересчета очереди могут быть представлены в трех видах (с учетом специализации по здоровью и без):

- порядковый номер в очереди в рамках муниципалитета;
- порядковый номер в очереди в рамках территориальной принадлежности дошкольного учреждения;
- порядковый номер в очереди в рамках конкретного детского сада.

Автоматизированный процесс приема заявлений, постановки на учет и зачисления детей в образовательные учреждения, реализующие основную образовательную программу дошкольного образования, осуществляется при наличии следующих персональных данных:

дата рождения ребенка; данные свидетельства о рождении; желаемая дата зачисления ребенка в ДОО; адрес регистрации и фактического проживания; данные о наличии права на внеочередное или первоочередное зачисление ребенка в дошкольное образовательное учреждение; наличие потребности в специализированной группе предпочтение заявителя в выборе ДОО; адрес электронной почты; контактные телефоны.

Расчетный объем обрабатываемых персональных данных: менее 100000 субъектов персональных данных.

ИСПДн не относится к:

- информационной системе, обрабатывающей специальные категории персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.
- информационной системе, обрабатывающей биометрические персональные данные, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.
- информационной системе, обрабатывающей общедоступные персональные данные, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных».

- информационной системе, обрабатывающей персональные данные сотрудников оператора.

ИСПДн подключена к информационно-телекоммуникационной сети «Интернет».

Режим обработки персональных данных: многопользовательский.

Режим разграничения прав доступа пользователей информационной системы: с разграниченными правами доступа.

Местонахождение ИСПДн: Тверская область, Российская Федерация.

В общем виде ИСПДН представлена на рис.1

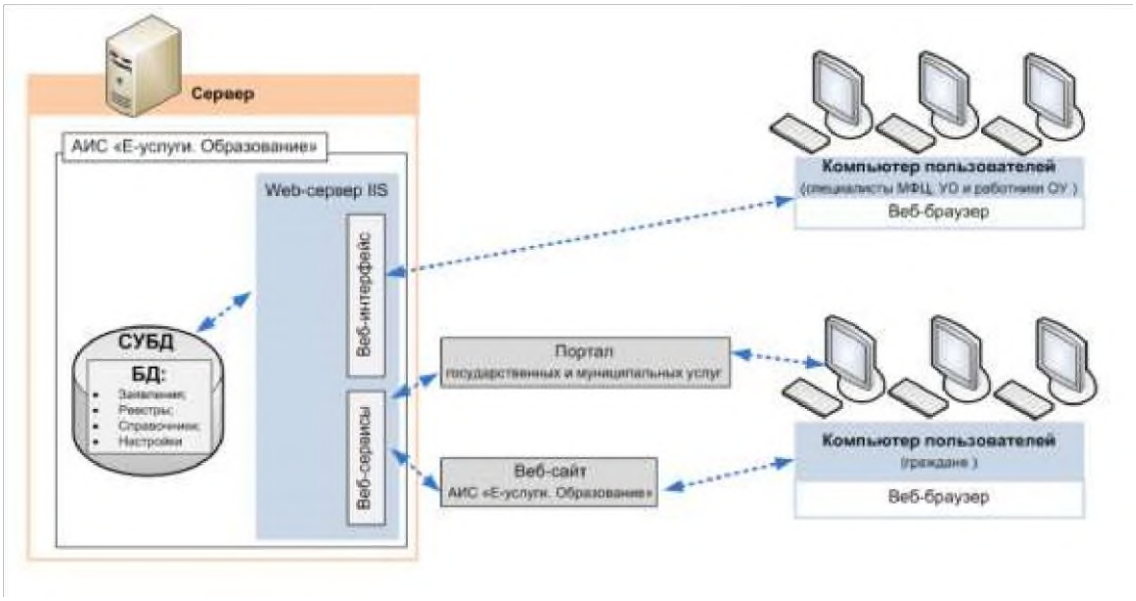

Рис.1 Общий вид технологического процесса ИСПДн.

Для реализации информационной технологии использовано лицензионное программное обеспечение: Windows Server 2012; SQL Server 2012, «Е-услуги. Образование». Веб-сервер (IIS) содержит службы Internet Information Services (IIS), которые являются унифицированной веб-платформой, объединяющей службы IIS, ASP.NET, Windows Communication Foundation и службы Windows SharePoint Services. Службы IIS позволяют организовать совместный доступ к информации обрабатываемой в ИСПДн через Интернет, интрасеть или экстрасеть. В системе SQLсервер организована двухуровневая настройка ограничения доступа к данным. На первом уровне организуется доступ к серверу посредством выданной учетной записи пользователя (login), которая позволяет ему подключиться к самому серверу, но не дает автоматического доступа к базам данных. (рис.2)

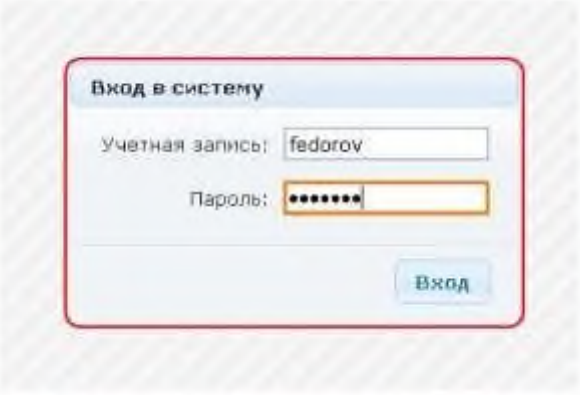

Рис.2 Интерфейс ввода учетной записи

На втором уровне для каждой базы данных SQL-сервера на основании учетной записи создается запись пользователя.

На основе прав, выданных пользователю как пользователю базы данных (user), и его регистрационного имени (login) организуется доступ к соответствующей базе данных. В разных базах данных login одного и того же пользователя может иметь одинаковые или разные имена user с разными правами доступа.

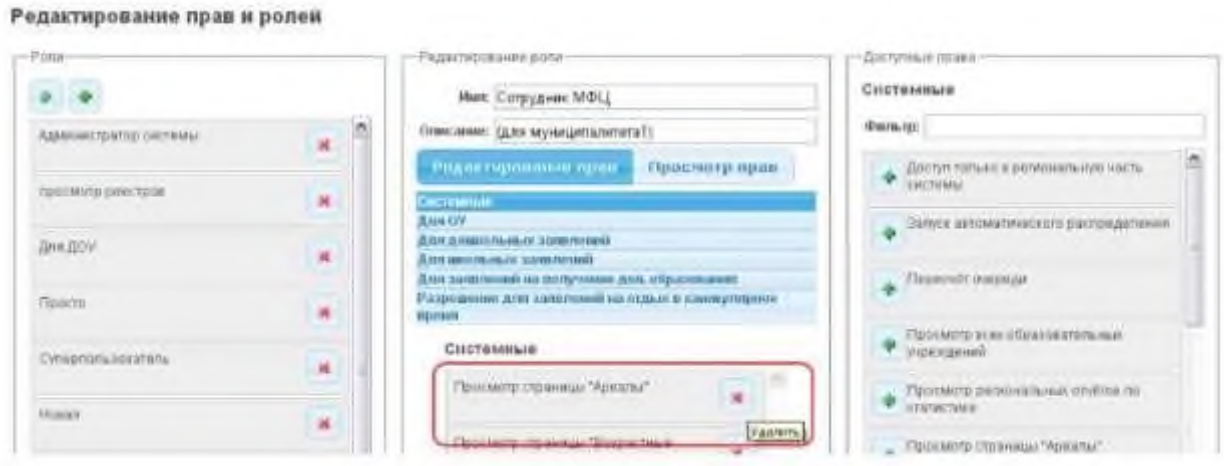

Рис.3 Интерфейс редактирования прав и ролей.

Иначе говоря, с помощью учетной записи пользователя осуществляется подключение к SQL-серверу, после чего определяются его уровни доступа для каждой базы данных в отдельности.

Для обеспечения безопасности ИСПДн используется подсистемы аудита Windows Server, настраиваемая через политики безопасности.

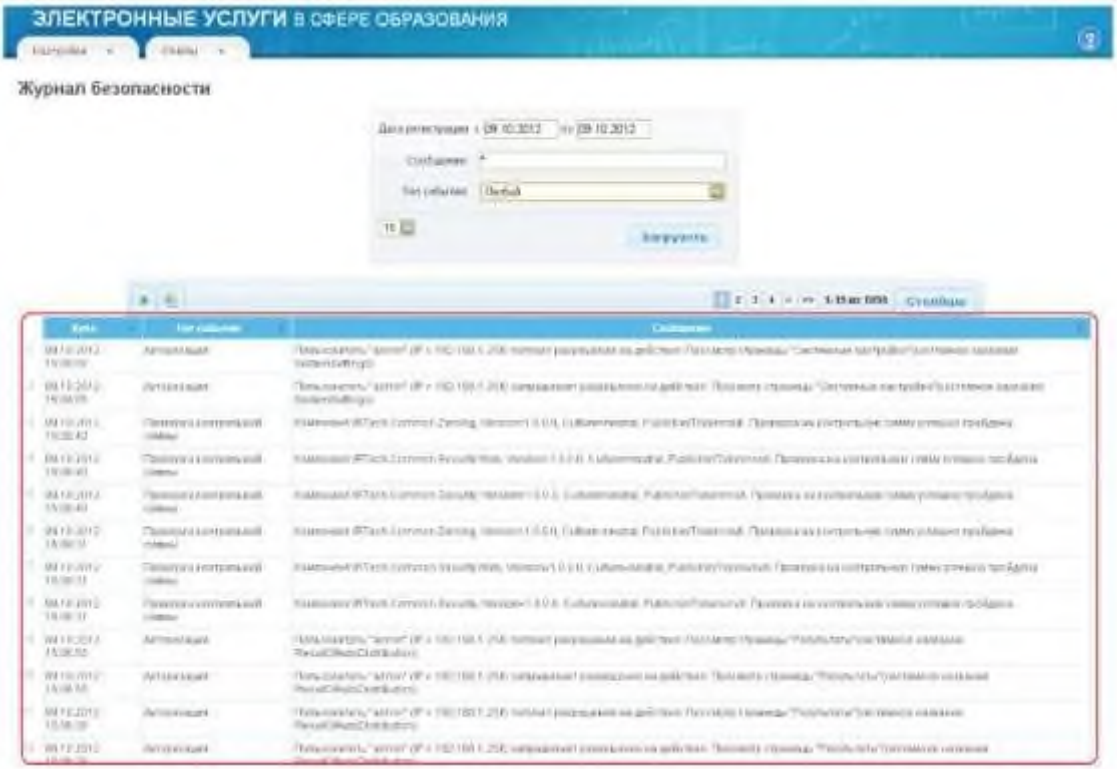

Рис.4 Журнал безопасности ИСПДн

ОПИСАНИЕ ФОРМ ПРЕДСТАВЛЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Персональные данные имеют различные формы представления (носители ПДн) с учетом используемых в информационной системе информационных технологий и технических средств.

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

Носители ПДн содержат информацию, в следующих видах:

- видовая информация, представленная в виде текста и изображений различных устройств отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средства обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн;
- информация, обрабатываемая (циркулирующая) в ИСПДн, в виде

электрических, электромагнитных, оптических сигналов;

- информация, обрабатываемая в ИСПДн, представленная в виде бит, байт, IPпротоколов, файлов и других логических структур.

ОПРЕДЕЛЕНИЕ ХРАКТЕРИСТИК БЕЗОПАСНОСТИ

Основными характеристиками безопасности являются конфиденциальность, целостность и доступность.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

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

Доступность информации – состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно.

Принимая во внимание, что решение о постановке на учет и зачислении детей в образовательные учреждения, реализующие основную образовательную программу дошкольного образования не принимается на основании исключительно автоматизированной обработки персональных данных в отношении субъекта персональных данных, соответственно при обработке персональных данных в ИСПДн необходимо обеспечить следующие характеристики безопасности – конфиденциальность, доступность.

МАТРИЦА ДОСТУПА

Матрица доступа отражает права всех групп субъектов доступа ИСПДн на действия с персональными данными. Действия (операции) с персональными данными, включают сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных).

При описании матрицы доступа использованы следующие основные группы субъектов доступа ИСПДн:

- Администраторы ИСПДн, осуществляющие настройку и установку технических средств ИСПДн и обеспечивающие ее бесперебойную работу;
- Разработчики ИСПДн, осуществляющие разработку и поддержку программного обеспечения собственной разработки или стандартных программ, специально доработанных под нужды организации;
- Операторы ИСПДн, осуществляющие текущую работу с персональными данными:
- Заявители ИСПДн, родители (законные представители) детей осуществляющие подачу заявления из «Личного кабинета» и получение информации через региональный портал государственных услуг, единый портал государственных услуг, сайт информационной системы «Е-услуги. Образование». Типовая матрица доступа для ИСПДн представлена в таблице 1

Таблица 1

Типовая роль	Уровень доступа к ПДн	Разрешенные действия

Администратор ИСПДн	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем	сбор систематизация накопление хранение уточнение использование распространение обезличивание блокирование
	техническим средствам обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	уничтожение
Разработчик ИСПДн	Обладает информацией об алгоритмах и программах обработки информации на ИСПДн. Обладает правами внесения изменений в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения. Располагает всей информаций о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн	систематизация блокирование уничтожение
Оператор ИСПДн	Обладает правами доступа к подмножеству ПДн. Располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системам, через которую он осуществляет доступ, и составе технических средств ИСПДн.	сбор систематизация накопление хранение уточнение использование распространение обезличивание

Заявители ИСПДн	Обладает правами доступа к подмножеству ПДн.	уточнение использование распространение

УРОВЕНЬ ИСХОДНОЙ ЗАЩИЩЕННОСТИ

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y_1), приведенных в таблице 1.

Таблица 1

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению:			
распределённая ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;			+
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);			+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;		+	
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;		+	
локальная ИСПДн, развернутая в пределах одного здания.	+		
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;			+
ИСПДн, имеющая одноточечный выход в сеть общего пользования;		+	
ИСПДн, физически отделенная от сети общего пользования.	+		
3. По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;	+		
запись, удаление, сортировка;		+	
модификация, передача.			+
4. По разграничению доступа к персональным данным:			

ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн;		+	
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;			+
ИСПДн с открытым доступом.			+
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);			+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации-владельцу данной ИСПДн.	+		
6. По уровню (обезличивания) ПДн:			
ИСПДн в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+		
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;		+	
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн).			+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая всю БД с ПДн;			+
ИСПДн, предоставляющая часть ПДн;		+	
ИСПДн, не предоставляющие никакой информации.	+		

Исходная степень защищенности определяется следующим образом:

1) ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню "высокий" (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу) ($Y_1 = 0$).

2) ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже "средний" (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные - низкому уровню защищенности ($Y_1 = 5$).

3) ИСПДн имеет низкую степень исходной защищенности, если не выполняется условия по пунктам 1 и 2 ($Y_1 = 10$).

Технические и эксплуатационные характеристики	ИСПДн
По территориальному размещению	средний
По наличию соединения с сетями общего пользования	средний
По встроенным (легальным) операциям с записями баз персональных данных	низкий
По разграничению доступа к персональным данным	средний
По наличию соединений с другими базами ПДн иных ИСПДн	высокий
По уровню (обезличивания) ПДн	средний
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	средний
Уровень защищенности	средний
Значение Y_1	5

ВЕРОЯТНОСТЬ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ
КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ

Состав и содержание УБПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн обрабатываемым в ИСПДн.

Основными элементами ИСПДн являются:

- персональные данные, обрабатываемые в ИСПДн;
- информационные технологии, как совокупность приемов, способов и методов применения средств вычислительной техники при обработке ПДн;
- технические средства ИСПДн, осуществляющие обработку ПДн (средства вычислительной техники (СВТ), информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн;
- программные средства (операционные системы, системы управления базами данных и т.п.);
- средства защиты информации (СЗИ), включая СКЗИ;
- вспомогательные технические средства и системы (технические средства и системы, их коммуникации, не предназначенные для обработки ПДн, но размещенные в помещениях, в которых расположены ИСПДн, такие как средства вычислительной техники, средства и системы охранной и пожарной сигнализации, средства и системы кондиционирования, средства электронной оргтехники и т.п.) (далее - ВТСС);
- документация на СКЗИ и на технические и программные компоненты ИСПДн;
- ключевая, аутентифицирующая и парольная информация; - помещения, в которых находятся защищаемые ресурсы.

Возможности источников УБПДн обусловлены совокупностью методов и способов несанкционированного и (или) случайного доступа к ПДн, в результате

которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн.

Угроза безопасности ПДн реализуется в результате образования канала реализации УБПДн между источником угрозы и носителем (источником) ПДн, что создает необходимые условия для нарушения безопасности ПДн (несанкционированный или случайный доступ).

Основными элементами канала реализации УБПДн являются:

- источник УБПДн – субъект, материальный объект или физическое явление, создающие УБПДн;
- среда (путь) распространения ПДн или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) ПДн;
- носитель ПДн – физическое лицо или материальный объект, в том числе физическое поле, в котором ПДн находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Источниками угроз НСД в ИСПДн могут быть:

- нарушитель;
- носитель вредоносной программы.

КЛАССИФИКАЦИЯ НАРУШИТЕЛЕЙ

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

- внешние нарушители – физические лица, не имеющие права пребыва-ния на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;
- внутренние нарушители – физические лица, имеющие право пребыва-ния на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

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.

ВНУТРЕННИЙ НАРУШИТЕЛЬ

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа.

Система разграничения доступа ИСПДн обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

- администратор базы данных ИСПДн (категория I);
- администраторы оператора ИСПДн (категория II);
- сотрудники оператор ИСПДн (категория III);
- заявители ИСПДн (категория IV);
- лица, обладающие возможностью доступа к системе передачи данных (категория V);
- сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы ИСПДн, но не имеющие права доступа к ним (категория VI);
- обслуживающий персонал (охрана, работники инженерно–технических служб

и т.д.) (категория VII);

- уполномоченный персонал разработчиков ИСПДн, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн (категория VIII).

На лиц категорий I и II возложены задачи по администрированию программно-аппаратных средств и баз данных ИСПДн для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИСПДн. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИСПДн, а также к техническим и программным средствам ИСПДн в соответствии с установленными для них административными полномочиями.

Эти лица 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 категорий I и II 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. Предполагается, что в число лиц категорий I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-VIII относятся к вероятным нарушителям.

Предполагается, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

ПРЕДПОЛОЖЕНИЯ ОБ ИМЕЮЩЕЙСЯ У НАРУШИТЕЛЯ ИНФОРМАЦИИ ОБ ОБЪЕКТАХ РЕАЛИЗАЦИИ УГРОЗ

В качестве основных уровней знаний нарушителей об ИСПДн 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 программнотехнических 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 III и категории IV владеют только эксплуатационной информацией, что обеспечивается организационными мерами. При этом лица категории IV не владеют парольной, аутентифицирующей и ключевой информацией, используемой в ИСПДн, к которым они не имеют санкционированного доступа.

Предполагается, что лица категории V владеют в той или иной части чувствительной и эксплуатационной информацией о системе передачи информации и общей информацией об ИСПДн, использующих эту систему передачи информации, что обеспечивается организационными мерами. При этом лица категории V не владеют парольной и аутентифицирующей информацией, используемой в ИСПДн.

Предполагается, что лица категории VI и лица категории VII по уровню знаний не превосходят лица категории V.

Предполагается, что лица категории VIII обладают чувствительной информацией об ИСПДн, включая информацию об уязвимостях технических и программных средств ИСПДн. Организационными мерами предполагается исключить доступ лиц категории VIII к техническим и программным средствам ИСПДн в момент обработки с использованием этих средств защищаемой информации.

Таким образом, наиболее информированными об ИСПДн являются лица категории III и лица категории VIII.

Степень информированности нарушителя зависит от многих факторов, включая 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.

ПРЕДПОЛОЖЕНИЯ ОБ ИМЕЮЩИХСЯ У НАРУШИТЕЛЯ СРЕДСТВ 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.

Внутренний нарушитель может использовать штатные средства.

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

Поэтому, 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 технических средств входящих в состав ИСПДн);
- 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 VIII.

КЛАССИФИКАЦИЯ УЯЗВИМОСТЕЙ ИСПДн

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности персональных данным.

Причинами возникновения уязвимостей являются:

- ошибки при проектировании и разработке программного (программноаппаратного) обеспечения;
- преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения;
- неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;
- несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;
- несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;
- сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

Различают следующие группы основных уязвимостей:

- уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);
- уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

ПЕРЕЧЕНЬ ВОЗМОЖНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Для 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.

2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн.

2.1.1.Кража технических средств входящих в состав ИСПДн;

2.1.2.Кража носителей информации;

2.1.3.Кража ключей и атрибутов доступа;

2.1.4.Кражи, модификации, уничтожения информации;

2.1.5.Вывод из строя узлов технических средств входящих в состав ИСПДн, каналов связи;

2.1.6.Несанкционированное отключение средств защиты.

2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программноматематических воздействий).

2.2.1.Действия вредоносных программ (вирусов);

2.2.2.Недекларированные возможности системного ПО и ПО для обработки персональных данных;

2.2.3.Установка ПО не связанного с исполнением служебных обязанностей.

2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры изза ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

2.3.1.Утрата ключей и атрибутов доступа;

2.3.2.Непреднамеренная модификация (уничтожение) информации сотрудниками;

2.3.3.Непреднамеренное отключение средств защиты;

2.3.4.Выход из строя аппаратно-программных средств; 2.3.5. Сбой системы электроснабжения;

2.3.6. Стихийное бедствие.

2.4. Угрозы преднамеренных действий внутренних нарушителей.

2.4.1.Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке;

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

2.5. Угрозы несанкционированного доступа по каналам связи.

2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:

2.5.1.1. Перехват за переделами с контролируемой зоны;

2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;

2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.

2.5.2. 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.

2.5.3. Угрозы выявления паролей по сети.

2.5.4. Угрозы навязывание ложного маршрута сети.

2.5.5. Угрозы подмены доверенного объекта в сети.

2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.

2.5.7. Угрозы типа «Отказ в обслуживании».

2.5.8. Угрозы удаленного запуска приложений. 2.5.9. Угрозы внедрения по сети вредоносных программ.

ОПРЕДЕЛЕНИЕ ВЕРОЯТНОСТИ РЕАЛИЗАЦИИ УГОРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

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 (Y_2) 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 ($Y_2 = 10$).

Определение вероятности реализации угрозы, должно быть проведено для всех выявленных угроз. Ниже приведено описание каждой угрозы и даны обобщенные вероятности реализации угроз для каждого типа ИСПДн.

Угрозы утечки информации по техническим каналам

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 функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют. Поэтому для всех типов ИСПДн вероятность реализации угрозы – **являются маловероятными.**

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.

При условии что в здании Оператора где размещена ИСПДн введен контроль доступа в контролируемую зону, а рабочие места пользователей расположены так, что практически исключен визуальный доступ к мониторам, а на окнах установлены жалюзи, то для ИСПДн вероятность реализации рассматриваемой угрозы – **является маловероятной.**

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 ИСПДн, т.к. размер контролируемой зоны большой, и элементы ИСПДн, находятся в самом центре здания и экранируются несколькими несущими стенами, и паразитный сигнал маскируется со множеством других паразитных сигналов элементов не входящих в ИСПДн.

Угрозы несанкционированного доступа к информации

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).

Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн

Кража технических средств входящих в состав ИСПДн.

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

Принимая во внимание, что у Оператора введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на

замок, установлены решетки на первых и последних этажах здания, то вероятность реализации данной угрозы – **является маловероятной.**

Кража носителей информации

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

Принимая во внимание, что у Оператора 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, то вероятность реализации данной угрозы – **является маловероятной**.

Кража ключей и атрибутов доступа

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.

Принимая во внимание, что у Оператора введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, организовано хранение ключей и введена политика «чистого стола», то вероятность реализации данной угрозы – **является маловероятной.**

Кражи, модификации, уничтожения информации

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

Принимая во внимание, что у Оператора введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, то вероятность реализации данной угрозы – **является маловероятной.**

Вывод из строя узлов технических средств входящих в состав ИСПДн, каналов связи

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

Принимая во внимание, что у Оператора введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, то вероятность реализации данной угрозы – **является маловероятной.**

Несанкционированное отключение средств защиты

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

Принимая во внимание, что у Оператора введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, пользователи

ИСПДн проинструктированы о работе с персональными данными, то вероятность реализации данной угрозы – **является маловероятной**.

Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).

Действия вредоносных программ (вирусов).

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

- скрывать признаки своего присутствия в программной среде компьютера;
- обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать произвольным образом) код программ в оперативной памяти;
- выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);
- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
- искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

У Оператора на всех элементах ИСПДн установлена антивирусная защита, пользователи проинструктированы о мерах предотвращения вирусного заражения, таким образом вероятность реализации угрозы – **является низкой.**

Недекларированные возможности 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.

Вероятность реализации угрозы повышается:

- при увеличении элементов, в том числе программного обеспечения, ИСПДн;
- при увеличении числа функциональных связей между элементами;

- наличии подключения к сетям общего доступа и (или) международного обмена.

Для рассматриваемой ИСПДн вероятность реализации угрозы – **низкая.**

Установка ПО, не связанного с исполнением служебных обязанностей

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

У Оператора введено разграничение правами пользователей на установку ПО и осуществляется контроль, пользователи проинструктированы о политике установки ПО, таким образом для рассматриваемой ИСПДн вероятность реализации угрозы – **является маловероятной**.

Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

Утрата ключей и атрибутов доступа

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

У Оператора введена парольная политика, предусматривающая требуемую сложность пароля и периодическую его смену, введена политика «чистого стола», осуществляется контроль за их выполнением, пользователи проинструктированы о парольной политике и о действиях в случаях утраты или компрометации паролей, таким образом для рассматриваемой ИСПДн вероятность реализации угрозы – **является низкой**.

Непреднамеренная модификация (уничтожение) информации сотрудниками

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

Принимая во внимание, что в ИСПДн осуществляется резервное копирование обрабатываемых ПДн, пользователи проинструктированы о работе с ИСПДн, то для рассматриваемой ИСПДн вероятность реализации угрозы – **является маловероятной**.

Непреднамеренное отключение средств защиты

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

Принимая во внимание, что у Оператора введен контроль доступа в контролируемую зону, двери закрываются на замок, осуществляется разграничение доступа к настройкам режимов средств защиты, пользователи проинструктированы о работе с ИСПДн, то вероятность реализации угрозы – **является маловероятной.**

Выход из строя аппаратно-программных средств

Угроза осуществляется вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации.

У Оператора осуществляет резервирование ключевых элементов ИСПДн, таким образом для рассматриваемой ИСПДн вероятность реализации угрозы – **является маловероятной.**

Сбой системы электроснабжения

Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации.

У Оператора ко всем ключевым элементам ИСПДн подключены источники бесперебойного питания и осуществляет резервное копирование информации, таким образом для рассматриваемой ИСПДн вероятность реализации угрозы – **является маловероятной.**

Стихийное бедствие

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

У Оператора установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций, таким образом для рассматриваемой ИСПДн вероятность реализации угрозы – **является маловероятной.**

Угрозы преднамеренных действий внутренних нарушителей

Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке

Угроза осуществляется путем НСД внешних нарушителей в помещения, где расположены элементы ИСПДн и средства защиты, а так же происходит работа пользователей.

У Оператора введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания. При наличии вышеперечисленных мер вероятность реализации угрозы – **является маловероятной.**

Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них.

У Оператора пользователи осведомлены о порядке работы с персональными данными, а так же подписали Договор о неразглашении, то для рассматриваемой ИСПДн вероятность реализации угрозы – **является низкой.**

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

Угрозы несанкционированного доступа по каналам связи

В соответствии с «Типовой моделью угроз безопасности персональных данных, обрабатываемых в распределенных ИСПДн, имеющих подключение к сетям общего пользования и (или) международного информационного обмена» (п. 6.6. Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 г.), для ИСПДн можно рассматривать следующие угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:

- угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;
- 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.;
- угрозы выявления паролей по сети;
- угрозы навязывание ложного маршрута сети;
- угрозы подмены доверенного объекта в сети;
- угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

Принимая во внимание, что решение о постановке на учет и зачислении детей в образовательные учреждения, реализующие основную образовательную программу дошкольного образования не принимается на основании исключительно автоматизированной обработки персональных данных в отношении субъекта персональных данных, то для рассматриваемой ИСПДн вероятность реализации вышеперечисленных угроз – **является маловероятной.**

Реализуемость угроз

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.	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
2.1.1. Кража ПЭВМ	неактуальная
2.1.2. Кража носителей информации	неактуальная
2.1.3. Кража ключей и атрибутов доступа	неактуальная
2.1.4. Кражи, модификации, уничтожения информации	неактуальная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	неактуальная
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	неактуальная
2.1.7. Несанкционированное отключение средств защиты	неактуальная
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программноматематических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	актуальная
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	неактуальная
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	неактуальная
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.	
2.3.1. Утрата ключей и атрибутов доступа	актуальная
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	неактуальная
2.3.3. Непреднамеренное отключение средств защиты	неактуальная
2.3.4. Выход из строя аппаратно-программных средств	неактуальная
2.3.5. Сбой системы электроснабжения	неактуальная
2.3.6. Стихийное бедствие	неактуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей	

2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	неактуальная
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	неактуальная
2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	
2.5.1.1. Перехват за переделами с контролируемой зоны	неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	неактуальная
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	неактуальная
2.5.2.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
2.5.3.Угрозы выявления паролей по сети	неактуальная
2.5.4.Угрозы навязывание ложного маршрута сети	неактуальная
2.5.5.Угрозы подмены доверенного объекта в сети	актуальная
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	актуальная
2.5.7.Угрозы типа «Отказ в обслуживании»	неактуальная
2.5.8.Угрозы удаленного запуска приложений	неактуальная
2.5.9.Угрозы внедрения по сети вредоносных программ	актуальная

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;
- использование протокола защищенного соединение (HTTPS);
- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;
- назначение ответственного за обработку персональных данных из числа сотрудников Оператора;
- инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а так же с ключами и атрибутами доступа;
- осуществление резервирования ключевых элементов ИСПДн;
- 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.