Приложение № 8 к приказу
директора М БОУ СОШ № 2 с. Арзгир
от «10» 10 2020 г. №266

Модель угроз безопасности персональных данных
МБОУ СОШ № 2 с. Арзгир

I. Перечень обозначений и сокращений

1. АРМ - автоматизированное рабочее место;
2. ИР - информационный ресурс;
3. ИСПДн - информационная система персональных данных;
4. КЗ - контролируемая зона;
5. ПДн - персональные данные;
6. ПО - программное обеспечение;
7. ПТС - программно-технические средства;
8. ПЭМИН - побочные электромагнитные излучения и наводки;
9. СЗИ - средства защиты информации;
10. СКЗИ - средства криптографической защиты информации;
11. ФСБ - Федеральная служба безопасности;
12. ФСО - Федеральная служба охраны;
13. ФСТЭК - Федеральная служба по техническому и экспертному контролю.

II. Общие положения

1. Настоящая модель угроз безопасности персональных данных (далее - Модель) содержит систематизированный перечень угроз безопасности персональных данных при их обработке (далее - Учреждение). Указанные угрозы могут исходить от источников, имеющих антропогенный, техногенный и стихийный характер и воздействующих на уязвимости ИСПДн, характерные для данной ИСПДн, реализуя тем самым угрозы информационной безопасности.

2. В Модели дается обобщенное описание ИСПДн, состав, категории и предполагаемый объем обрабатываемых ПДн с последующей классификацией ИСПДн.

3. Модель описывает потенциального нарушителя безопасности ПДн и подходы по определению актуальности угроз с учетом возможностей нарушителя и особенностей конкретной ИСПДн.

4. Настоящая Модель разработана в соответствии с требованиями Федерального законодательства и федеральных органов по защите персональных данных.

III. Характеристика объекта информатизации

В МБОУ СОШ № 2 с. Арзгир существуют следующие типы ИСПДн:

1. ИСПДн передачи информации, в том числе ПДн, в целях исполнения Федеральных законов.

3. Состав ИСПДн и обрабатываемых в них персональных данных приведен в Приложении №1 к настоящему документу.

4. В качестве объекта информатизации Школы выступают:

1. Автономные автоматизированные рабочие места (АРМ).

2. Локальные вычислительные сети.

5. В зависимости от характеристик и особенностей отдельных объектов часть вычислительных средств данных предприятий подключена к сетям связи общего пользования и (или) сетям международного информационного обмена.

6. Ввод персональных данных осуществляется как с бумажных носителей (например, документов, удостоверяющих личность субъекта ПДн), так и с электронных носителей информации.

7. ИСПДн предполагают распределенную (на АРМ) обработку и хранение ПДн.

8. Персональные данные субъектов ПДн могут выводиться из ИСПДн с целью передачи персональных данных субъектов Учреждения, как в электронном, так и в бумажном виде.

9. Контролируемой зоной (КЗ) ИСПДн являются отдельные помещения. В пределах контролируемой зоны находятся рабочие места пользователей и места хранения архивных копий данных, сетевое и телекоммуникационное оборудование ИСПДн. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

2 Состав, категории и объем персональных данных, определение уровня защищенности персональных данных

1. На основе характеристик и особенностей используемых ИСПДн и обрабатываемых в них персональных данных, можно констатировать, что персональные данные субъектов ПДн, обрабатываются в Учреждении информационной системой, обрабатывающей общедоступные персональные данные, а также системой, обрабатывающей иные категории персональных данных. Специальные категории персональных данных и биометрические персональные данные в ИСПДн Учреждения не обрабатываются.

2. Для ИСПДн МБОУ СОШ № 2 с. Арзгир актуальны угрозы 2 типа - угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе. Согласно «Требованиям к защите персональных данных при их обработке в информационных системах персональных данных» для ИСПДн Школы требуется обеспечить 4 -ий уровень защищенности персональных данных при их обработке в информационной системе.

3 Способы нарушения характеристик безопасности персональных данных

1. Исходя из перечня персональных данных, обрабатываемых в ИСПДн, существуют следующие способы нарушения характеристик безопасности ПДн:

- хищение персональных данных сотрудниками Учреждения для использования в корыстных целях;
- передача финансовой, адресной, юридической и прочей информации о субъекте ПДн третьим лицам;
- несанкционированное публичное разглашение персональных данных, ставших известными сотрудникам МБОУ СОШ № 2 с. Арзгир;
- несанкционированное получение персональных данных третьими лицами;
- уничтожение финансовой, адресной и прочей информации о субъекте ПДн;
- модификация финансовой, адресной и прочей информации о субъекте ПДн;
- блокирование финансовой, адресной и прочей информации о субъекте ПДн;
- ввод некорректной финансовой, адресной и прочей информации о субъекте ПДн;
- передача некорректной финансовой, адресной и прочей информации о субъекте ПДн;

- искажение архивной информации по субъекту ПДн.
- уничтожение архивной информации по субъекту ПДн.

4 Угрозы безопасности персональных данных, при их обработке в информационных системах персональных данных

1. Под угрозами безопасности персональных данных при их обработке в ИСПДн понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее. Таким образом, угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн, так и со специально осуществляемыми неправомерными действиями отдельных организаций и граждан, а также иными источниками угроз. Неправомерные действия могут исходить также и от сотрудников Учреждения в случае, когда они рассматриваются в качестве потенциального нарушителя безопасности ПДн.

2. В целях формирования систематизированного перечня угроз безопасности ПДн при их обработке в ИСПДн и разработке на их основе частных (детализированных) моделей применительно к конкретному виду ИСПДн, угрозы безопасности персональным данным в ИСПДн можно классифицировать в соответствии со следующими признаками:

по видам возможных источников угроз;
по типу ИСПДн, на которые направлена реализация угроз;
по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);
по способам реализации угроз;
по используемой уязвимости;
по объекту воздействия.

3. Для ИСПДн существуют следующие классы угроз безопасности ПДн:

- **По видам возможных источников угроз безопасности персональных данных**

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющими доступ к ИР ИСПДн, включая пользователей, реализующие угрозы непосредственно в ИСПДн;

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;

- угрозы, возникновение которых напрямую зависит от свойств техники, используемой в ИСПДн;

- угрозы, связанные со стихийными природными явлениями.

Кроме этого, угрозы могут возникать в результате внедрения аппаратных закладок и вредоносных программ.

- **По типу ИСПДн, на которые направлена угроза:**

По структуре ИСПДн, на которые направлена угроза, необходимо рассматривать следующие классы угроз:

- угрозы безопасности данных, обрабатываемых в ИСПДН на базе автоматизированных рабочих мест;

- угрозы безопасности данных, обрабатываемых в ИСПДН на базе локальных информационных систем.

- **По способам реализации угроз**

По способам реализации угроз выделяют следующие классы угроз:

- угрозы, связанные с несанкционированным доступом к ПДн (в том числе угрозы внедрения вредоносных программ);

- угрозы утечки ПДн по техническим каналам утечки информации (ТКУИ);

- угрозы специальных воздействий на ИСПДн.

- **По виду нарушаемого свойства информации (несанкционированных действий, осуществляемых с персональными данными)**

По виду несанкционированных действий, осуществляемых с персональными данными, можно выделить следующий класс угроз:

- угрозы, приводящие к нарушению конфиденциальности ПДн (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;

- угрозы, приводящие к несанкционированному воздействию на содержание информации, в результате которого происходит изменение данных или их уничтожение;

- угрозы, приводящие к несанкционированному воздействию на программные или программно-аппаратные элементы ИСПДн, в результате которого осуществляется блокирование данных.

- **По используемой уязвимости выделяются следующие классы угроз:**

- угрозы, реализуемые с использованием уязвимости системного программного обеспечения (ПО);

- угрозы, реализуемые с использованием уязвимости прикладного ПО; - угрозы, возникающие в результате использования уязвимости, вызванной наличием в ИСПДн аппаратной закладки;

- угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;

- угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации технической защиты информации от несанкционированного доступа;

- угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;

- угрозы, реализуемые с использованием уязвимостей средств защиты информации.

- **По объекту воздействия выделяются следующие классы угроз:**

- угрозы безопасности ПДн, обрабатываемых на АРМ;
- угрозы безопасности ПДн, передаваемых по сетям связи;
- угрозы прикладным программам, с помощью которых обрабатываются ПДн;
- угрозы системному ПО, обеспечивающему функционирование ИСПДн.

5 Характеристика источников угроз безопасности персональных данных в ИСПДн

1. В отношении ИСПДн могут существовать три типа источников угроз безопасности ПДн:

1. Антропогенные источники угроз безопасности ПДн.
2. Техногенные источники угроз безопасности ПДн.
3. Стихийные источники угроз безопасности ПДн.

- **Антропогенные источники угроз безопасности ПДн**

В качестве антропогенного источника угроз для ИСПДн необходимо рассматривать субъекта (личность), имеющего санкционированный или несанкционированный доступ к работе со штатными средствами ИСПДн, действия которого могут привести к нарушению безопасности персональных данных. Антропогенные источники угроз по отношению к ИСПДн могут быть как внешними, так и внутренними

Среди внешних антропогенных источников можно выделить случайные и преднамеренные источники.

Случайные (непреднамеренные) источники могут использовать такие уязвимости, как ошибки, совершенные при проектировании ИСПДн и ее элементов, ошибки в программном

обеспечении; различного рода сбои и отказы, повреждения, проявляемые в ИСПДн. К таким источникам можно отнести персонал поставщиков различного рода услуг, персонал надзорных организаций и аварийных служб и т.п. Действия (угрозы), исходящие от данных источников, совершаются по незнанию, невнимательности или

халатности, из любопытства, но без злого умысла.

Преднамеренные источники проявляются в корыстных устремлениях нарушителей. Основная цель таких источников - умышленная дезорганизация работы, вывод систем Организации из строя, искажение информации за счет проникновения в ИСПДн путем несанкционированного доступа.

Внутренними источниками, как правило, являются специалисты в области программного обеспечения и технических средств, в том числе средств защиты информации, имеющие возможность использования штатного оборудования и программнотехнических средств ИСПДн. К таким источникам можно отнести основной персонал, представителей служб безопасности, вспомогательный и технический персонал.

Для внутренних источников угроз особое место занимают угрозы в виде ошибочных действия и (или) нарушений требований эксплуатационной и иной документации сотрудниками Учреждения, имеющих доступ к ИР ИСПДн. К подобным угрозам, в частности, относятся:

- непредумышленное искажение или удаление программных компонентов;
- внедрение и использование неучтенных программ;
- игнорирование организационных ограничений (установленных правил) при работе с ресурсами ИСПДн, включая средства защиты информации. В частности:
- нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (ключевой, парольной и аутентифицирующей информации);
- предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований;
- настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов;
- несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа.

Наибольшую опасность представляют преднамеренные угрозы, исходящие как от внешних, так и от внутренних антропогенных источников.

Необходимо рассматривать следующие классы таких угроз:

- угрозы, связанные с преднамеренными действиями лиц, имеющими доступ к ИСПДн, включая пользователей ИСПДн и иных сотрудников Учреждения, реализующими угрозы непосредственно в ИСПДн (внутренний нарушитель);
- угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к ИСПДн и реализующими угрозы из внешних сетей связи общего пользования или сетей международного информационного обмена (внешний нарушитель);
- угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к ИСПДн и реализующими угрозы по ТКУИ.

- **Техногенные источники угроз безопасности ПДн**

Техногенные источники угроз напрямую зависят от свойств техники. Данные источники также могут быть как внешними, так и внутренними.

К внешним источникам относятся инфраструктурные элементы ИСПДн: средства связи (телефонные линии, линии передачи данных и т.п.), сети инженерных коммуникаций (водоснабжение, канализация, отопление и пр.).

К внутренним источникам относятся некачественные технические и программные

средства обработки информации, вспомогательные средства (охраны, сигнализации, телефонии), другие технические средства, применяемые в ИСПДн, а также вредоносное программное обеспечение и аппаратные закладки.

Аппаратная закладка

Аппаратные закладки могут быть конструктивно встроенными и автономными. Аппаратные закладки могут реализовать угрозы:

- сбора и накопления ПДн, обрабатываемых и хранимых в ИСПДн;
- формирования ТКУИ.

В силу отмеченных свойств аппаратных закладок эффективная защита от них может быть обеспечена только за счет тщательного учета их специфики и соответствующей организации технической защиты информации на всех стадиях жизненного цикла ИСПДн.

Носитель вредоносной программы

В качестве носителя вредоносной программы в ИСПДн может выступать аппаратный элемент средств вычислительной техники из состава ИСПДн или ПО, выполняющее роль программного контейнера.

Если вредоносная программа не ассоциируется с какой-либо прикладной программой из состава системного или общего ПО ИСПДн, в качестве ее носителя выступают:

- внешний машинный (отчуждаемый) носитель, т.е. дискета, оптический диск, лазерный диск, флэш-память, внешний жесткий диск и т.п.;
- встроенные носители информации (жесткие диски, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок устройства - видеоадаптера, сетевой платы, устройств ввода/вывода и т. д.)
- микросхемы внешних устройств (монитора, клавиатуры, принтера, плоттера, сканера и т.п.).

В том случае, если вредоносная программа может быть проассоциирована с системным или общим ПО, с файлами различной структуры или с сообщениями, передаваемыми по сети, то ее носителем являются:

- пакеты передаваемых по сети ИСПДн сообщений;
- файлы (исполняемые, текстовые, графические и т.д.).

При возникновении угроз из данной группы появляется потенциальная возможность нарушения конфиденциальности, целостности, доступности и других характеристик безопасности ПДн.

- **Стихийные источники угроз безопасности ПДн**

Стихийные источники угроз отличается большим разнообразием и непредсказуемостью и являются, как правило, внешними по отношению к Учреждению. Под ними, прежде всего, рассматриваются различные природные катаклизмы: пожары, землетрясения, ураганы, наводнения. Возникновение этих источников трудно спрогнозировать и им тяжело противодействовать, но при наступлении подобных событий нарушается штатное функционирование самой ИСПДн и ее средств защиты, что потенциально может привести к нарушению конфиденциальности, целостности, доступности и других характеристик безопасности ПДн.

Защита от угроз, исходящих от техногенных и стихийных источников угроз безопасности ПДн, регламентируется инструкциями, разработанными и утвержденными оператором с учетом особенностей эксплуатации ИСПДн.

6. Модель нарушителя безопасности персональных данных

1. Анализ возможностей, которыми может обладать нарушитель, проводится в рамках модели нарушителя.

При разработке модели нарушителя зафиксированы следующие положения:

- Безопасность ПДн в ИСПДн обеспечивается средствами защиты информации ИСПДн, а также используемыми в них информационными технологиями, техническими и программными средствами, удовлетворяющими требованиям по защите информации, уста-

навливаемым в соответствии с законодательством Российской Федерации;

- Средства защиты информации (СЗИ) штатно функционируют совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к СЗИ требований;

- СЗИ не могут обеспечить защиту ПДн от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СЗИ не может обеспечить защиту ПДн от раскрытия лицами, которым предоставлено право на доступ к этим данным).

2 .Описание нарушителей.

С точки зрения наличия права постоянного или разового доступа в контролируемую зону (КЗ) объектов размещения ИСПДн все физические лица могут быть отнесены к следующим двум категориям:

- категория I - лица, не имеющие права доступа в контролируемую зону ИСПДн;

- категория II - лица, имеющие право доступа в контролируемую зону ИСПДн.

Все потенциальные нарушители подразделяются на:

- внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны ИСПДн;

- внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны ИСПДн.

В качестве внешнего нарушителя кроме лиц категории I должны рассматриваться также лица категории II, находящиеся за пределами КЗ.

В отношении ИСПДн в качестве внешнего нарушителями из числа лиц категории I могут выступать:

- бывшие сотрудники Учреждения;

- посторонние лица, пытающиеся получить доступ к ПДн в инициативном порядке;

- представители преступных организаций.

Внешний нарушитель может осуществлять:

- перехват обрабатываемых техническими средствами ИСПДн ПДн за счет их утечки по ТКУИ с использованием портативных, возимых, носимых, а также автономных автоматических средств разведки серийной разработки;

- деструктивные воздействия через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами КЗ;

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

- перехват информации, передаваемой по сетям связи общего пользования или каналам связи, не защищенным от несанкционированного доступа (НСД) к информации организационно- техническими мерами;

- атаки на ИСПДн путем реализации утроз удаленного доступа.

Внутренний нарушитель (лица категории II) подразделяется на восемь групп в зависимости от способа и полномочий доступа к информационным ресурсам (ИР) ИСПДн.

-К первой группе относятся сотрудники Учреждения, не являющиеся зарегистрированными пользователями и не допущенные к ИР ИСПДн, но имеющие санкционированный доступ в КЗ.

Лицо данной группы может:

- располагать именами и вести выявление паролей зарегистрированных пользователей ИСПДн;

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

- Ко второй группе относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ИР ИСПДн с рабочего места. К этой категории относятся сотрудники Учреждения, имеющие право доступа к локальным ИР ИСПДн для выполнения своих должностных обязанностей.

Лицо данной группы:

- обладает всеми возможностями лиц первой категории;

- знает, по меньшей мере, одно легальное имя доступа;

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающим доступ к ИР ИСПДн;

- располагает ПДн, к которым имеет доступ.

- К третьей группе относятся зарегистрированные пользователи подсистем ИСПДн, осуществляющие удаленный доступ к ПДн по локальной сети Учреждения.

Лицо данной группы:

- обладает всеми возможностями лиц второй категории;

- располагает информацией о топологии сети ИСПДн и составе технических средств ИСПДн;

- имеет возможность прямого (физического) доступа к отдельным техническим средствам (ТС) ИСПДн.

- К четвертой группе относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности ИСПДн.

Лицо данной группы:

- обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте ИСПДн;

- обладает полной информацией о технических средствах и конфигурации сегмента ИСПДн;

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

- имеет доступ ко всем техническим средствам сегмента ИСПДн;

- обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента ИСПДн.

- К пятой группе относятся зарегистрированные пользователи с полномочиями системного администратора, выполняющего конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства мониторинга, резервного копирования, антивирусного контроля, защиты от несанкционированного доступа.

Лицо данной группы:

- обладает полной информацией о системном, специальном и прикладном ПО, используемом в ИСПДн;

- обладает полной информацией о ТС и конфигурации ИСПДн

- имеет доступ ко всем ТС ИСПДн и данным;

- обладает правами конфигурирования и административной настройки ТС ИСПДн.

- К шестой группе относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности Учреждения, отвечающего за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей, криптографическую защиту информации. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор.

Лицо данной группы:

- обладает полной информацией об ИСПДн;

- имеет доступ к средствам защиты информации и протоколирования и к части ключе-

вых элементов ИСПДн;

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

- К седьмой группе относятся лица из числа программистов - разработчиков сторонней организации, являющихся поставщиками ПО и лица, обеспечивающие его сопровождение на объекте размещения ИСПДн.

Лицо данной группы:

- обладает информацией об алгоритмах и программах обработки информации в ИСПДн;

- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в ПО ИСПДн на стадии его разработки, внедрения и сопровождения;

- может располагать любыми фрагментами информации о ТС обработки и защиты информации в ИСПДн.

- К восьмой группе относятся персонал, обслуживающий ТС ИСПДн, а также лица, обеспечивающие поставку, сопровождение и ремонт ТС ИСПДн.

Лицо данной группы:

- обладает возможностями внесения закладок в ТС ИСПДн на стадии их разработки, внедрения и сопровождения;

- может располагать фрагментами информации о топологии ИСПДн, автоматизированных рабочих местах, серверах и коммуникационном оборудовании, а также о ТС защиты информации в ИСПДн.

3. Предположения о возможностях нарушителя.

Для получения исходных данных о ИСПДн нарушитель (как I категории, так и II категории) может осуществлять перехват зашифрованной информации и иных данных, передаваемых по каналам связи сетям общего пользования и (или) сетям международного информационного обмена, а также по локальным сетям ИСПДн.

Любой внутренний нарушитель может иметь физический доступ к линиям связи, системам электропитания и заземления.

Предполагается, что возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны объектов размещения ИСПДн ограничительных факторов, из которых основными являются режимные мероприятия и организационно-технические меры, направленные на:

- предотвращение и пресечение несанкционированных действий;
- подбор и расстановку кадров;
- допуск физических лиц в контролируемую зону и к средства вычислительной техники;
- контроль за порядком проведения работ.

В силу этого внутренний нарушитель не имеет возможности получения специальных знаний о ИСПДн в объеме, необходимом для решения вопросов создания и преодоления средств защиты ПДн, и исключается его возможность по созданию и применению специальных программно-технических средств реализации целенаправленных воздействий данного нарушителя на подлежащие защите объекты и он может осуществлять попытки несанкционированного доступа к ИР с использованием только штатных программно-технических средств ИСПДн без нарушения их целостности.

Возможность сговора внутренних нарушителей между собой, сговора внутреннего нарушителя с персоналом организаций-разработчиков подсистем ИСПДн, а также сговора внутреннего и внешнего нарушителей должна быть исключена применением организационно-технических и кадрово-режимных мер, действующих на объектах размещения ИСПДн.

4. Предположения об имеющихся у нарушителя средствах атак

Предполагается, что нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства.

Внешний нарушитель (лица категории I, а также лица категории II при нахождении за пределами КЗ) может использовать следующие средства доступа к защищаемой информации:

- доступные в свободной продаже аппаратные средства и программное обеспечение, в том числе программные и аппаратные компоненты криптосредств;
- специально разработанные технические средства и программное обеспечение;
- средства перехвата и анализа информационных потоков в каналах связи;
- специальные технические средства перехвата информации по ТКУИ;
- штатные средства ИСПДн (только в случае их расположения за пределами КЗ).

Внутренний нарушитель для доступа к защищаемой информации, содержащей ПДн, может использовать только штатные средства ИСПДн. При этом его возможности по использованию штатных средств зависят от реализованных в ИСПДн организационнотехнических и режимных мер.

5. Описание каналов атак.

Возможными каналами атак, которые может использовать нарушитель для доступа к защищаемой информации в ИСПДн, являются:

- каналы непосредственного доступа к объекту (визуально-оптический, акустический, физический);
- электронные носители информации, в том числе съемные, сданные в ремонт и вышедшие из употребления;
- бумажные носители информации;
- штатные программно-аппаратные средства ИСПДн;
- кабельные системы и коммутационное оборудование, расположенные в пределах контролируемой зоны и не защищенные от НСД к информации организационно-техническими мерами;
- незащищенные каналы связи; ТКУИ.

6. Тип нарушителя при использовании в ИСПДн криптографических средств защиты информации

При обмене информацией между ИСПДн и внешними по отношению к предприятию информационными системами необходимо использование средств криптографической защиты информации (СКЗИ).

Уровень криптографической защиты персональных данных, обеспечиваемой СКЗИ, определяется путем отнесения нарушителя, действиям которого должно противостоять СКЗИ, к конкретному типу, и базируется на подходах, описанных в «Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации».

Тип нарушителя и класс СКЗИ должен определяться в соответствии с таблицей Таблица - Соответствие типов нарушителя и класса СКЗИ

Группа внутреннего нарушителя	Тип нарушителя	Класс СКЗИ
Группа 1	Н2	КС2
Г руппа 2	Н3	КС3
Г руппа 3	Н3	КС3
Г руппа 4	Н3	КС3
Г руппа 5	Н3	КС3
Г руппа 6	Н3	КС3
Г руппа 7	Н5	КВ2
Г руппа 8	Н4	КВ1

Внешний нарушитель относится к типу Н1. При этом, если он обладает возможностями по созданию способов и подготовки атак, аналогичными соответствующим возможностям внутреннего нарушителя типа Hi (за исключением возможностей, предоставляемых пребыванием в момент атаки в контролируемой зоне), то этот нарушитель также будет обозначаться как нарушитель типа Hi.

7 Актуальные угрозы безопасности персональных данных в информационных системах персональных данных

1. Для выявления из всего перечня угроз безопасности ПДн актуальных для ИСПДн оцениваются два показателя:

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

2. Уровень исходной защищенности информационной системы персональных данных

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн. Перечень данных характеристик и показатели защищенности ИСПДн, зависящие от них, показаны в таблице.

3. Показатели, относящиеся к Учреждению выделены жирным курсивом.

Для определения исходной защищенности ИСПДн должно быть рассчитано процентное соотношение каждого уровня защищенности ко всем характеристикам, имеющим место для ИСПДн.