



УТВЕРЖДАЮ
Директор МБОУ «СОШ
«Технический лицей»

И.А.Стрובה

Приказ № 134 от 02.09.2024

**МОДЕЛЬ УГРОЗ
БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ ИНФОРМАЦИОННЫХ
СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ
В МУНИЦИПАЛЬНОМ БЮДЖЕТНОМ ОБЩЕОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ
"СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА «ТЕХНИЧЕСКИЙ ЛИЦЕЙ»
ГОРОДА ОБНИНСКА
(сокращенно - МБОУ «СОШ «Технический лицей»)**

г. Обнинск, 2024

Перечень обозначений и сокращений

АРМ – автоматизированное рабочее место;

ИР - информационный ресурс;

ИСПДн - информационная система персональных данных;

ПДн - персональные данные;

ПО - программное обеспечение;

ПТС - программно-технические средства;

СЗИ - средства защиты информации;

СКЗИ - средства криптографической защиты информации;

1. Общие положения

Настоящая модель угроз безопасности персональных данных (далее – Модель) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в ИСПДн МБОУ «СОШ «Технический лицей».

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.

В Модели дается обобщенное описание ИСПДн, состав, категории обрабатываемых ПДн с последующей классификацией ИСПДн.

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

Настоящий документ составлен в соответствии со следующими действующими нормативно-методическими документами по защите персональных данных:

1. - Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
2. — Постановление Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
3. - Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (ФСБ России, № 149/5- 144, 2008);
4. - Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 14 февраля 2008г. заместителем директора ФСТЭК России);
5. Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 15 февраля 2008г. заместителем директора ФСТЭК России);
6. Приказ Министерства просвещения Российской Федерации от 21.07.2022 года № 576 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Министерством просвещения Российской Федерации»

ИСПДн МБОУ «СОШ «Технический лицей» поддерживает технологические процессы деятельности образовательной организации. Рассматриваемая ИСПДн имеет подключение к сетям общего пользования.

Обработка персональных данных в ИСПДн ведется в автономном режиме с разграничением прав доступа. Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Информационные системы персональных данных

Исходные данные **информационного ресурса Электронный журнал/дневник «Моя школа»** в МБОУ «СОШ «Технический лицей» г. Обнинска развернута на 44 компьютерах, которые имеют выход в сеть Интернет. Обработка персональных данных осуществляется в программах «Microsoft Office». Операционная система – «Windows 7, 10»,

Информационная система «Кадры» развернута на одном компьютере. Компьютер имеет выход в сеть Интернет. Обработка персональных данных осуществляется в программах «Microsoft Office». Операционная система – «Windows 10». Имеются СКЗИ.

Информационная система VipNetClient4 «Деловая почта» установлена на одном рабочем компьютере с доступом одного должностного лица.

Все перечисленные информационные системы относятся к следующим типам:

- ИСПДн ведения бухгалтерского учета, управления персоналом, расчета заработной платы;
- ИСПДн учета и передачи информации, в том числе ПДн, в целях исполнения Федеральных законов.

2. Характеристика объекта информатизации

В качестве объекта информатизации Школы выступают:

1. Автономные автоматизированные рабочие места (АРМ).
2. Локальные вычислительные сети.

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

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

ИСПДн предполагают как распределенную (на АРМ), так и централизованную (на выделенных файловых серверах сети) обработку и хранение ПДн.

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

3. Состав, категории и объем персональных данных, определение уровня защищенности персональных данных

На основе характеристик и особенностей используемых ИСПДн и обрабатываемых в них персональных данных, можно констатировать, что персональные данные субъектов ПДн, обрабатываются в МБОУ «СОШ «Технический лицей» информационной системой, обрабатывающей общедоступные персональные данные, а также системой, обрабатывающей иные категории персональных данных. Специальные категории персональных данных и биометрические персональные данные в ИСПДн МБОУ «СОШ «Технический лицей» не обрабатываются.

Для ИСПДн МБОУ «СОШ «Технический лицей» актуальны угрозы 2 типа - угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе. Согласно подпункту «б» пункта 11 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» для ИСПДн МБОУ «СОШ «Технический лицей» требуется обеспечить 3-ий уровень защищенности персональных данных при их обработке в информационной системе.

4. Способы нарушения характеристик безопасности персональных данных

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

- Хищение персональных данных работниками школы 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 предприятия;
- несанкционированное получение персональных данных третьими лицами;
- уничтожение информации о субъекте ПДн;
- модификация информации о субъекте ПДн;
- блокирование информации о субъекте ПДн;
- передача некорректной информации о субъекте ПДн;
- искажение архивной информации по субъекту ПДн.
- уничтожение архивной информации по субъекту ПДн.

5. Угрозы безопасности персональных данных, при их обработке в информационных системах персональных данных

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 предприятия в случае, когда они рассматриваются в качестве потенциального нарушителя безопасности ПДн.

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 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.

по типу ИСПДн, на которые направлена реализация угроз:

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 виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);

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 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 используемой уязвимости:

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, обуславливающих наличие технических каналов утечки информации;
- угрозы, реализуемые с использованием уязвимостей средств защиты информации.

по объекту воздействия:

по объекту воздействия выделяются следующие классы угроз:

- угрозы безопасности ПДн, обрабатываемых на АРМ;
- угрозы безопасности ПДн, обрабатываемых в выделенных средствах обработки (принтерах, плоттерах, графопостроителях, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.); угрозы безопасности ПДн, передаваемых по сетям связи;
- угрозы прикладным программам, с помощью которых обрабатываются ПДн;
- угрозы системному ПО, обеспечивающему функционирование ИСПДн.

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

6. Характеристика источников угроз безопасности персональных данных в ИСПДн

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 программно-технических 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 работниками Школы, 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 предприятия, 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 МБОУ «СОШ «Технический лицей».

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.

7. Модель нарушителя безопасности персональных данных

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

При разработке модели нарушителя зафиксированы следующие положения:

1. 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, устанавливаемым в соответствии с законодательством Российской Федерации;

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

3. 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).

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 внешних нарушителями из числа лиц категории I могут выступать:

- бывшие сотрудники Школы;
- 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 угроз удаленного доступа.

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

1. К первой группе относятся сотрудники предприятий, не являющиеся зарегистрированными пользователями и не допущенные к ИР ИСПДн, но имеющие санкционированный доступ в КЗ. К этой категории нарушителей относятся сотрудники различных структурных подразделений предприятий: энергетики, сантехники, уборщицы, сотрудники охраны и другие лица, обеспечивающие нормальное функционирование объекта информатизации.

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.

2. Ко второй группе относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ИР ИСПДн с рабочего места. К этой категории относятся сотрудники предприятий, 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.

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

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.

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

5. 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.

6. К шестой группе относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности Организации, 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 ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

7. 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, недеklarированных 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.

8. 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.

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.

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 организационно-технических и режимных мер.

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.

Тип нарушителя при использовании в ИСПДн криптографических средств защиты информации

При обмене информацией между ИСПДн и внешними по отношению к МБОУ «СОШ «Технический лицей» 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».

8. Актуальные угрозы безопасности персональных данных в информационных системах персональных данных

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

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

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн.

Следующим параметром, необходимым для определения актуальности угроз безопасности ПДн, является частота (или вероятность) реализации угрозы, под которой понимается определенный экспертным путем показатель, характеризующий вероятность реализации конкретной угрозы безопасности ПДн для ИСПДн в реальных условиях ее функционирования.

Вводится четыре значения этого показателя, обозначаемого как Y2:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

Далее дается оценка опасности каждой угрозы ПДн для ИСПДн. Данная оценка носит экспертный характер и получается путем опроса экспертов в области безопасности информации.

Данная оценка имеет три значения:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов ПДн;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов ПДн;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов ПДн.

После просчета всех показателей производится оценка актуальности каждой угрозы

безопасности ПДн при их обработке в ИСПДн исходя из матрицы, приведенная в таблице:

Таблица: Матрица расчета актуальности угроз безопасности ПДн

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

Делаем вывод о наличии актуальных угроз и мер защиты, направленных на снижения риска возникновения и последствий актуальных угроз.

Тип угроз безопасности ПДн	Возможность реализации
1. Угрозы от утечки по техническим каналам.	Неактуальная
2. Угрозы несанкционированного доступа к информации.	
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 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	
2.2.1. Утрата ключей и атрибутов доступа	Актуальная
2.2.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Неактуальная
2.2.3. Непреднамеренное отключение средств защиты	Неактуальная
2.2.4. Выход из строя аппаратно-программных средств	Неактуальная
2.2.5. Сбой системы электроснабжения	Неактуальная
2.2.6. Стихийное бедствие	Неактуальная
2.3. Угрозы преднамеренных действий внутренних нарушителей	
2.3.1. Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке	Неактуальная
2.3.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Неактуальная

Актуальными угрозами безопасности ПДн в МБОУ «СОШ «Технический лицей» г. Обнинска являются:

- угрозы от действий вредоносных программ (вирусов);
- угрозы утраты ключей и атрибутов доступа.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;
- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;
- назначение ответственного за безопасность персональных данных из числа сотрудников учреждения;
- инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а так же с ключами и атрибутами доступа.

Контрольными мерами по эффективности системы защиты являются:

- анализ и оценка исходных данных и документации по защите информации на объекте информатизации;
- проверка состава средств защиты информации, их состояния;
- изучение процесса обработки и хранения информации, анализ информационных потоков на объекте информатизации;
- проверка состояния организации работ и выполнения организационно-технических требований по защите информации на объекте информатизации.