

1. Состав, категории объем персональных данных, определение уровня защищенности персональных данных
   1. На основе характеристики особенностей используемых информационной системой персональных данных и обрабатываемых в них персональных данных, можно констатировать, что персональные данные субъектов персональных данных, обрабатываются в учреждении информационной системой, обрабатывающей общедоступные персональные данные. Специальные категории персональных данных и

биометрические персональные данные в информационной системе персональных данных учреждения не обрабатываются.

* 1. Для информационной системы персональных данных учреждения актуальны угрозы второго 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 информационной системы персональных данных учреждения требуется обеспечить 3-ий уровень защищенности персональных данных при их обработке в информационной системе.

В МОУ Озёрская ОШ обеспечен средний уровень защищенности.

1. Способы нарушения характеристик безопасности персональных данных
   1. Исходя из перечня персональных данных, обрабатываемых в информационной системе персональных данных, существуют следующие способы нарушения характеристик безопасности персональных данных:

* хищение персональных данных сотрудниками учреждения для использования в корыстных целях;
* передача финансовой, адресной, юридической и прочей информации о субъекте персональных данных третьим лицам;
* несанкционированное публичное разглашение персональных данных, ставших известными сотрудникам учреждения;
* 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 персональных данных;
* передача некорректной финансовой, адресной и прочей информации о субъекте персональных данных;
* искажение архивной информации по субъекту персональных данных.
* уничтожение архивной информации по субъекту персональных данных.

1. Угрозы безопасности персональных данных, при их обработке в информационных системах персональных данных
2. Под угрозами безопасности персональных данных при их обработке в информационной системы персональных данных 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 персональных данных при их обработке в информационной системе персональных данных могут быть связаны как с непреднамеренными действиями персонала

информационной системы персональных данных, 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 персональных данных.

1. В целях формирования систематизированного перечня угроз

Безопасности персональных данных при их обработке в информационной системы персональных данных и разработке на их основе частных (детализированных) моделей применительно к конкретному виду информационной системы персональных данных, угрозы безопасности персональным данным в информационной системы персональных данных можно классифицировать в соответствии со следующими признаками:

* по видам возможных источников угроз;
* по типу информационной системы персональных данных, на которые направлена реализация угроз;
* по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с персональными данными);
* по способам реализации угроз;
* по используемой уязвимости;
* по объекту воздействия.

1. Для информационной системы персональных данных существуют следующие классы угроз безопасности персональных данных:

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

–угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющими доступ к информационным ресурсам информационной системы персональных данных, включая пользователей, реализующие угрозы непосредственно в информационной системе персональных данных;

* угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к информационной системе персональных данных, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;
* угрозы, возникновение которых напрямую зависит от свойств техники, используемой в информационной системе персональных данных;
* угрозы, связанные со стихийными природными явлениями.

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

По способам реализации угроз

По способам реализации угроз выделяют следующие классы угроз:

* угрозы, связанные с несанкционированным доступом к персональным данным (в том числе угрозы внедрения вредоносных программ);
* угрозы специальных воздействий на информационную систему персональных данных.

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

**По виду несанкционированных действий, осуществляемых с персональными данными, для организации можно выделить следующие угрозы:**

* угрозы, приводящие к нарушению конфиденциальности персональных данных (копированию или несанкционированному распространению), при 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 информационной системе персональных данных, в результате которого осуществляется блокирование данных.

По используемой уязвимости для организации выделяются следующие угрозы:

* угрозы, реализуемые с использованием уязвимости системного программного обеспечения;
* угрозы, реализуемые с использованием уязвимости прикладного программного обеспечения;
* угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации технической защиты информации от несанкционированного доступа;
* угрозы, реализуемые с использованием уязвимостей средств защиты информации.

По объекту воздействия для организации выделяются следующие угрозы:

* Угрозы безопасности персональных данных, передаваемых по сетям связи;
* угрозы системному ПО, обеспечивающему функционирование информационной системы персональных данных.

1. Характеристика источников угроз безопасности персональных данных в информационной системе персональных данных

В отношении информационной системы персональных данных могут существовать три типа источников угроз безопасности персональных данных:

1. Антропогенные источники угроз безопасности персональных данных.
2. Техногенные источники угроз безопасности персональных данных.
3. Стихийные источники угроз безопасности персональных данных.

Антропогенные источники угроз безопасности персональных данных

В качестве антропогенного источника угроз для информационной системы персональных данных необходимо рассматривать субъекта (личность), имеющего санкционированный или несанкционированный доступ к работе со штатными средствами информационной системы персональных данных, действия которого могут привести к нарушению безопасности персональных данных.

Антропогенные источники угроз по отношению к информационной системе персональных данных 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 информационной системы персональных данных и ее элементов,

Ошибки в программном обеспечении; различного рода сбои и отказы, повреждения, проявляемые в информационной системе персональных данных. 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 учреждения из строя, искажение информации за счет проникновения в информационную систему персональных данных путем несанкционированного доступа.

К внутренним источникам можно отнести основной персонал, вспомогательный персонал.

Для внутренних источников угроз особое место занимают угрозы в виде ошибочных действий и (или) нарушений требований эксплуатационной и иной документации сотрудниками Учреждения, имеющих доступ к информационным ресурсам информационной системы персональных данных н.

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 информационной системы персональных данных, включая средства защиты информации. В частности:
* нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (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 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 информационной системы персональных данных, включая пользователей

информационной системы персональных данных и иных сотрудников Учреждения, реализующими угрозы непосредственно в информационной системе персональных данных (внутренний нарушитель);

* угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к информационной системе персональных данных и реализующими угрозы из внешних сетей связи общего пользования или сетей международного

информационного обмена (внешний нарушитель).

**Техногенные источники угроз безопасности информационной системы персональных данных**

* Техногенные источники угроз напрямую зависят от свойств техники. Данные

источники также могут быть как внешними, так и внутренними.

К внешним источникам относятся инфраструктурные элементы информационной системы персональных данных:

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 информационной системе персональных данных.

Носитель вредоносной программы

В качестве носителя вредоносной программы в информационной системе персональных данных может выступать, если вредоносная программа не ассоциируется с какой-либо прикладной программой из состава системного или общего программного обеспечения

информационной системы персональных данных, 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, сканера и т.п.).
* **Стихийные источники угроз безопасности персональных данных для организации** Стихийные источники угроз отличается большим разнообразием и непредсказуемостью и являются 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 информационной системы персональных данных и ее средств защиты, что потенциально может привести к нарушению конфиденциальности, целостности, доступности и других характеристик безопасности персональных данных.

1. 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 персональных данных в информационной системе персональных данных обеспечивается средствами защиты информации информационной системы персональных данных, а также используемыми в них информационными технологиями, техническими и программными средствами, удовлетворяющими требованиям по защите информации, устанавливаемыми в соответствии с законодательством Российской Федерации;
  + средства защиты информации штатно функционируют совместно с

техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к средствам защиты информации требований;

* + средства защиты информации не могут обеспечить защиту персональных данных от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, средство защиты информации не может обеспечить защиту персональных данных 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 объектов размещения информационной системы

персональных данных все физические лица могут быть отнесены к следующим двум категориям:

* + Категория I–лица, не имеющие права доступа в контролируемую зону информационной системы персональных данных;
  + категория II–лица, имеющие право доступа в контролируемую зону информационной системы персональных данных.

Все потенциальные нарушители подразделяются на:

* + внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны информационной системы персональных данных;
  + внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны информационной системы персональных данных.

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

В отношении информационной системы персональных данных в качестве внешних нарушителей из числа лиц категории I могут выступать:

* бывшие сотрудники учреждения;
* посторонние лица, пытающиеся получить доступ к персональных данным в инициативном порядке;
* представители преступных организаций.

Внешний нарушитель может осуществлять:

* деструктивные воздействия через элементы информационной инфраструктуры информационной системы персональных данных, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами контролируемой зоны;
* 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;

-атаки на информационную систему персональных данных путем реализации угроз удаленного доступа.

Внутренними нарушителями для организации (лица категории II) могут быть сотрудники учреждения, не являющиеся зарегистрированными пользователями и не допущенные к информационным ресурсам информационной системы персональных данных, но имеющие санкционированный доступ в контролируемую зону.

Лицо данной группы может:

* располагать именами и вести выявление паролей зарегистрированных пользователей информационной системы персональных данных;
* изменять конфигурацию технических средств обработки персональных данных, вносить программно-аппаратные закладки информационную систему персональных данных и обеспечивать съем информации, используя непосредственное подключение к техническим средствам обработки информации.

в зависимости от способа и полномочий доступа к информационным ресурсам информационной системы персональных данных.

-Актуальной для ДШИ является первая группа, к которой относятся сотрудники учреждения, не являющиеся зарегистрированными пользователями и не допущенные к информационным ресурсам информационной системы персональных данных, но имеющие санкционированный доступ в контролируемую зону.

Лицо данной группы может:

* располагать именами и вести выявление паролей зарегистрированных пользователей информационной системы персональных данных;
* изменять конфигурацию технических средств обработки персональных данных, вносить программно-аппаратные закладки информационную систему персональных данных и обеспечивать съем информации, используя непосредственное подключение к техническим средствам обработки информации.

1. Актуальные угрозы безопасности персональных данных в информационных системах персональных данных
   1. Для выявления из всего перечня угроз безопасности персональных данных актуальных для информационной системы персональных данных оцениваются два показателя:

* уровень исходной защищенности информационной системы персональных данных;
* частота (вероятность) реализации рассматриваемой угрозы.
  1. Уровень исходной защищенности информационной системы персональных данных.

Под уровнем исходной защищенности информационной системы персональных данных понимается обобщенный показатель, зависящий от технических и

эксплуатационных характеристик информационной системы персональных данных. Перечень данных характеристик и показатели защищенности

информационной системы персональных данных, зависящие от них, показаны в таблице.

* 1. Показатели, относящиеся к Учреждению выделены жирным курсивом и бирюзовым цветом. МОУ Озёрская ОШ соответствует средний уровень защищенности.

Для определения исходной защищенности информационной системы персональных данных должно быть рассчитано процентное соотношение каждого уровня защищенности ко всем характеристикам, имеющим место для информационной системы персональных данных.

Таблица 9.1 – Показатели исходной защищенности информационной системы персональных данных

|  |  |  |  |
| --- | --- | --- | --- |
| **Технические и эксплуатационные характеристики ИСПДн** | **Уровень** | | |
| **Высок ий** | **Средни й** | **Низки й** |
| **По территориальному размещению** |  |  |  |
| Распределенная 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* информационная система персональных

|  |  |  |  |
| --- | --- | --- | --- |
| данных*,* развернутая в пределах одного здания 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 | |  |  |  |
| **По встроенным (легальным) операциям с записями баз ПДн** | |  |  |  |
| чтение, поиск | |  |  |  |
| ***запись, удаление, сортировка*** | |  |  |  |
| модификация,передача | |  |  |  |
| **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 с открытым доступом | |  |  |  |
| **По наличию соединений с другими базами ПДн иных ИСПДн** | |  |  |  |
| Интегрированная ИСПДн (организация использует несколько баз ПДнИСПДн, при этом организация не является владельцем всех используемых баз ПДн) | |  |  |  |
| ***ИСПДн, в которой используется одна база ПДн,***  ***принадлежащая организации –владельцу данной ИСПДн*** | |  |  |  |
| **По уровню обобщения (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 о*** | |  |  |  |
|  |
|  |
| ***безличенными***  **По объему ПДн, которые предоставляются сторонним пользователям** | |  |  |  |
| **ИС** | |  |  |  |
| **ПДн без** | |
| ИСПДн, предоставляющая всю базу данных с ПДн | |  |  |  |
| ***ИСПДн, предоставляющая часть ПДн*** | |  |  |  |
| ИСПДн, не предоставляющие никакой информации | |  |  | |

***Количество решений* 1 5 1**

***Общее количество решений***

1. Принимается, что информационная система персональных данных имеет высокий уровень исходной защищенности, если не менее 70% характеристик

информационной системы персональных данных соответствуют уровню «высокий», а остальные уровню «средний».

В случае, если не менее 70% характеристик информационной системы персональных данных относится к уровню «не ниже среднего», а остальные к уровню «низкий», то исходная защищенность информационной системы персональных данных будет среднего уровня. Во всех остальных случаях информационная система персональных данных будет иметь низкий уровень защищенности. Исходя из критериев оценки, делаем вывод, что информационная система персональных данных учреждения имеет средний уровень защищенности.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Реализуемост ь угрозы** | **Показатель опасности угрозы** | | | | | | | |
| **Низкая** | | | **Средняя** | | | **Высокая** | |
| Низкая | неактуальная | |  | неактуальная | |  | актуальная |  |
| Средняя | неактуальная | |  | актуальная |  | | актуальная |  |
| Высокая | актуальная |  | | актуальная |  | | актуальная |  |
| Очень высокая | актуальная |  | | актуальная |  | | актуальная |  |

На основании положений модели угроз, модели нарушителя, данных б исходной защищенности информационной системы персональных данных (Y1), коэффициенте реализуемости угрозы (Y),вероятности ее реализации(Y2), а также экспертной оценки опасности угрозы, определяется актуальность каждой угрозы безопасности персональных данных, обрабатываемых в информационной системы персональных данных. (Таблица 9.3)

Таблица 9.3 – Актуальность угроз безопасности персональных данных

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Угроза безопасности ПДн | Вероят  ность реализации  угрозы | Коэффиц  иент реализуе мости  угрозы | Оценка опасности угрозы | Оценка актуаль ности угрозы |
| 1. | Разглашение, передача или утрата  атрибутов разграничения доступа к  ИСПДн | 5 | 0,75 | средняя | актуаль  ная |
| 2. | Нарушение правил хранения  атрибутов разграничения доступа к  ИСПДн | 5 | 0,75 | низкая | актуаль  ная |
| 3. | Несообщение о фактах утраты,  компрометации атрибутов  разграничения доступа к ИСПДн | 10 | 1,0 | высокая | Актуаль  ная |
| 4. | Внедрение агентов в число персонала  системы | 0 | 0,5 | высокая | Актуаль  ная |
| 5. | Несанкционированный запуск  технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы или осуществляющих необратимые изменения в системе (форматирование или  реструктуризацию носителей  информации, удаление данных и т.п.) | 2 | 0,6 | высокая | актуаль  ная |
| 6. | Ввод ошибочных данных | 10 | 1,0 | низкая | Актуаль  ная |
| 7. | Действия сотрудников, приводящие к  частичному или полному отказу системы или нарушению работоспособности аппаратных или  программных средств | 5 | 0,75 | высокая | Актуаль  ная |
| 8. | Игнорирование организационных  ограничений (установленных правил)  при работе с ПД | 10 | 1 | средняя | Актуаль  ная |
| 9. | Физическое разрушение или вывод из | 0 | 0,5 | высокая | актуаль |
|  | строя всех или отдельных наиболее |  |  |  | ная |

10.

11.

12.

13.

14.

15.

16.

17.

18.

19.

20.

21.

22.

23.

24.

25.

26.

27.

28.

29.

важных компонентов ИСПДн

Закупки несовершенных, устаревших 0

или неперспективных средств

информатизации и информационных технологий;

Хищение носителей информации, 2

содержащих ПД

То же, внешний нарушитель 2

Незаконное получение паролей и 5

других реквизитов разграничения доступа к ИСПДн

То же, внешний нарушитель 2

Несанкционированная модификация 5

программного обеспечения

То же, внешний нарушитель 2

Перехват ПД, передаваемых по 0

каналам связи

То же, внешний нарушитель 0

Несанкционированное копирование 5

носителей информации с ПД

То же, внешний нарушитель 2

Чтение остаточной информации из 0

оперативной памяти и с внешних запоминающих устройств

То же, внешний нарушитель 0

Непреднамеренное заражение 5

компьютера вирусами

Преднамеренное заражение 10

компьютера вирусами

Вмешательство в процесс 5

функционирования ИСПДн, сетей общего пользования с целью несанкционированной модификации данных

То же, внешний нарушитель 2

Несанкционированное внедрение и 10

использование неучтенных программ, не являющихся необходимыми для выполнения сотрудниками своих служебных обязанностей

То же, внешний нарушитель 5

Неумышленное повреждения внешних 2

кабельных систем связи

0,5

0,6

0,6

0,75

0,6

0,75

0,6

0,5

0,5

0,75

0,6

0,5

0,5

0,75

1,0

0,75

0,6

1,0

0,75

0,6

низкая

высокая высокая средняя

средняя высокая высокая высокая высокая средняя средняя низкая

низкая низкая низкая высокая

высокая средняя

средняя низкая

неактуа льная

Актуаль ная

актуаль ная Актуаль ная

актуаль ная Актуаль ная

актуаль ная Актуаль ная Актуаль ная Актуаль ная Актуаль ная неактуа льная

неактуа льная актуаль ная

актуаль ная

актуаль ная

актуаль ная

актуаль ная

актуаль ная неактуа льная

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 30. | Возникновение пожаров в  непосредственной близости к помещениям, в которых обрабатываются ПД и архивам ПД результате неисправной  электропроводки, неисправных технических средств, нарушения сотрудниками правил  противопожарной безопасности. | 2 | 0,6 | высокая | актуаль  ная |
| 31. | Разрушение зданий, отдельных  помещений | 0 | 0,5 | высокая | актуаль  ная |
| 32. | Возникновение стихийных очагов  пожаров | 2 | 0,6 | низкая | неактуа  льная |
| 33. | Аварии в системах электропитания | 5 | 0,75 | низкая | актуаль  ная |
| 34. | Аварии в системах отопления и  водоснабжения в непосредственной близости к помещениям, в которых  обрабатываются ПД и архивам ПД | 2 | 0,75 | средняя | актуаль  ная |