**Примерный перечень**

**документов по защите персональных данных**

**в образовательном учреждении**

|  |  |
| --- | --- |
| **№** | **Название документа** |
|  | Акт определения типа актуальных угроз защищенности информационных систем (далее – ИС) персональных данных |
|  | Инструкция администратора безопасности ИС персональных данных |
|  | Инструкция администратора ИС персональных данных |
|  | Инструкция должностного лица, ответственного за организацию обработки персональных данных |
|  | Инструкция по обеспечению безопасности персональных данных |
|  | Инструкция педагогическому персоналу ОО по работе с персональными данными |
|  | Модель угроз персональным данным (приложение 1 «Примерное содержание модели угроз персональным данным») |
|  | Отчет по инвентаризации ИС персональных данных |
|  | Перечень должностей сотрудников ОО, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных |
|  | Перечень должностей сотрудников ОО, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным |
|  | Перечень ИС персональных данных в ОО |
|  | Перечень персональных данных, подлежащих защите в ОО |
|  | Политика в отношении обработки персональных данных |
|  | Положение по обеспечению безопасности персональных данных |
|  | Порядок доступа в помещения ОО, в которых ведется обработка персональных данных |
|  | Правила обработки персональных данных |
|  | Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных |
|  | Правила работы с обезличенными персональными данными |
|  | Правила рассмотрения запросов субъектов персональных данных или их представителей |
|  | Приказ о вводе в действие документов, регламентирующих порядок обработки персональных данных |
|  | Приказ о назначении комиссии по уничтожению материальных носителей информации, содержащих персональные данные |
|  | Приказ о назначении ответственных за обработку персональных данных |
|  | Приказ об организации защиты персональных данных |
|  | Приказ об утверждении мест хранения материальных носителей персональных данных |
|  | Приказ об утверждении плана мероприятий по защите персональных данных, обрабатываемых в ИС |
|  | Приказ об утверждении форм журналов, используемых при обработке персональных данных, а также при эксплуатации технических средств защиты информации |
|  | Протокол экспертной оценки вероятности реализации угроз |
|  | Протокол экспертной оценки показателей опасности угроз |
|  | Рекомендации по обеспечению безопасности персональных данных, обрабатываемых в ИС ОО |

**Категории персональных данных, обрабатываемые в ИС**

|  |  |
| --- | --- |
| Категория персональных данных | Содержание информации |
| Специальные категории персональных данных | Расовая, национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья, интимная жизнь субъектов персональных данных |
| Биометрические персональные данные | Физиологические и биологические особенности человека, на основании которых можно установить его личность. Используются оператором для установления личности субъекта персональных данных (не обрабатываются сведения, относящиеся к специальным категориям персональных данных) |
| Общедоступные персональные данные | Персональные данные, полученные только из общедоступных источников персональных данных, созданных в соответствии со ст. 8 Федерального закона №  152-ФЗ |
| Иные категории персональных данных | Персональные данные, которые не относятся к специальным категориям персональных данных, биометрическим и иным категориям |
| Персональные данные сотрудников оператора | Персональные данные только указанных сотрудников (в остальных случаях ИС персональных данных является ИС, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора) |

**Требования к уровням защищенности ИС персональных данных**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Требования | Уровни защищенности | | | |
|  | 1 | 2 | 3 | 4 |
| Организация режима обеспечения безопасности помещений, в которых размещена ИС, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа |  |  |  |  |
| Обеспечение сохранности носителей персональных данных |  |  |  |  |
| Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в ИС, необходим для выполнения ими служебных (трудовых) обязанностей |  |  |  |  |
| Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз |  |  |  |  |
| Назначение должностного лица, ответственного за обеспечение безопасности персональных данных в ИС персональных данных |  |  |  | - |
| Ограничение доступа к содержанию электронного журнала сообщений |  |  | - | - |
| Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в ИС |  | - | - | - |
| Создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в ИС, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности |  | - | - | - |

**ПРИМЕРНОЕ СОДЕРЖАНИЕ**

**модели угроз персональным данным**

|  |  |
| --- | --- |
| **№** | **Название раздела** |
| 1. **Общие сведения. Назначение модели угроз** | |
| 1. **Сведения об объекте защиты** | |
| **2.1.** | Структура информационных систем (далее – ИС) персональных данных и ее основные характеристики |
| **2.1.1.** | Структура ИС персональных данных |
| **2.1.2.** | Режим разграничения прав доступа пользователей ИС персональных данных |
| **2.1.3.** | Подключение ИС персональных данных к сетям связи общего пользования и (или) сетям международного информационного обмена |
| **2.2.** | Информация, обрабатываемая в ИС персональных данных |
| **2.3.** | Контролируемая зона |
| **2.4.** | Перечень защищаемых ресурсов ИС персональных данных |
| **2.5.** | Исходный уровень защищенности ИС персональных данных |
| **2.6.** | Основные данные об ИС персональных данных |
| 1. **Модель нарушителей информационной безопасности** | |
| **3.1.** | Внешние нарушители |
| **3.2** | Внутренние нарушители |
| **3.3** | Класс средств криптографической защиты информации |
| 1. **Модель угроз информационной безопасности** | |
| **4.1.** | Источники угроз безопасности информации |
| **4.2.** | Уязвимость ИС персональных данных по отношению к деструктивным воздействиям |
| **4.3.** | Факторы, влияющие на безопасность защищаемой информации |
| **4.4.** | Угрозы техногенного характера |
| **4.4.1.** | Случайное или преднамеренное отключение электричества |
| **4.4.2.** | Аварии (пожар, потоп) |
| **4.4.3.** | Потеря доступа к внешней сети в связи с проблемами со стороны провайдера |
| **4.4.4.** | Выход из строя аппаратно-программных средств |
| **4.5.** | Стихийные бедствия |
| **4.6.** | Угрозы, реализуемые нарушителями |
| **4.6.1.** | Угрозы утечки информации по техническим каналам |
| **4.6.2.** | Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИС персональных данных, носителям данных, ключам и атрибутам доступа |
| **4.6.3.** | Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств |
| **4.6.4.** | Угрозы несанкционированного доступа к информации по каналам связи |
| **4.6.5.** | Угрозы антропогенного характера |
| **5.** **Вероятность реализации угроз безопасности** | |
| **6.** **Реализуемость угроз безопасности** | |
| **6.1.** | Оценка возможности реализации угроз безопасности |
| **6.2.** | Оценка опасности угроз |
| **7. Определение актуальности угроз** | |
| **8. Актуальные угрозы безопасности** | |
| **9. Выводы** | |

**ПРИМЕРНЫЕ ФОРМЫ**

**журналов по защите персональных данных**

Форма 1 Журнал учета передачи персональных данных

* №
* Сведения о запрашивающем лице
* Состав запрашиваемых персональных данных
* Цель получения персональных данных
* Отметка о передаче или отказе в передаче персональных данных
* Дата передачи или отказа в передаче персональных данных
* Подпись запрашивающего лица
* Подпись  ответственного сотрудника … …

Форма 2 Журнал учета обращений субъектов персональных данных о соблюдении их законных прав в области защиты персональных данных

* №
* Ф. И. О.
* Дата
* Цель … …

Форма 3 Журнал учета носителей персональных данных

* №
* Метка носителя (учетный номер)
* Фамилия исполнителя
* Получил, вернул, передал
* Дата записи информации
* Подпись исполнителя
* Примечание … …

Форма 4 Журнал уничтожения носителей персональных данных

* №
* Дата
* Вид и учетный номер уничтожаемого носителя
* Способ уничтожения
* Исполнитель … …

Форма 5 Журнал учета мероприятий по контролю состояния защиты персональных данных

* №
* Дата
* Управление / контроль прав(ами) доступа к персональным данным
* Исполнитель
* Результат … …

Форма 6 Журнал учета применяемых средств защиты информации, эксплуатационной и технической документации

* №
* Дата
* Средства защиты информации
* Эксплуатационная информация
* Техническая документация
* Подпись … …

Форма 7 Журнал учета нарушений порядка предоставления персональных данных №

* Дата, время обнаружения нарушения
* Информационная система персональных данных, в которой обнаружено нарушение
* Дата, время устранения  нарушения
* Результат
* Подпись  ответственного  сотрудника
* Примечания … …

Форма 8 Журнал учета выдачи ключей доступа к информационным системам персональных данных

* Дата и время получения
* Номер кабинета
* Фамилия, инициалы сотрудника
* Подпись сотрудника о получении
* Дата и время возврата
* Подпись сотрудника о сдаче под охрану … …

**ПРИМЕРНЫЙ ПЕРЕЧЕНЬ**

**угроз безопасности для информационных систем**

**персональных данных**

|  |  |
| --- | --- |
| **№** | Наименование угрозы |
| **1** | Угрозы техногенного характера |
| **1.1.** | Угрозы техногенного характера |
| **1.2.** | Аварии (пожар, потоп) |
| **1.3** | Потеря доступа к внешней сети в связи с проблемами со стороны провайдера |
| **1.4.** | Выход из строя аппаратно-программных средств |
| **2.** | Стихийные бедствия |
| **3.** | Угрозы (атаки), реализуемые нарушителями |
| **3.1.** | Угрозы утечки информации по техническим каналам |
| **3.1.1.** | Угрозы утечки акустической (речевой) информации |
| **3.1.2.** | Угрозы утечки видовой информации |
| **3.1.3.** | Угрозы утечки информации по каналам побочных электромагнитных излучений и наводки |
| **3.2.** | Угрозы несанкционированного доступа к информации путем физического доступа к элементам информационных систем (далее – ИС) персональных данных, носителям данных, ключам и атрибутам доступа |
| **3.2.1.** | Кража персонального компьютера |
| **3.2.2.** | Кража серверного оборудования |
| **3.2.3.** | Кража и уничтожение носителей информации |
| **3.2.4.** | Кража (утрата) физических носителей ключей (например, электронных USB-ключей и смарт-карт и проч.) и атрибутов доступа |
| **3.2.5.** | Утрата носителей информации |
| **3.2.6.** | Вывод из строя узлов персонального компьютера, телекоммуникационных каналов связи |
| **3.2.7** | Несанкционированное отключение средств защиты |
| **3.2.8.** | Кража/модификация/уничтожение информации сотрудниками |
| **3.2.9.** | Утрата и компрометация ключей и атрибутов доступа |
| **3.3.** | Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств |
| **3.3.1.** | Утечка информации через порты ввода/вывода |
| **3.3.2.** | Воздействие вредоносных программ (вирусов) |
| **3.3.3.** | Установка программного обеспечения (далее – ПО), не связанного с исполнением служебных обязанностей |
| **3.3.4.** | Внедрение или сокрытие недекларированных возможностей системного и прикладного ПО ИС персональных данных |
| **3.3.5.** | Создание учетных записей теневых пользователей и неучтенных точек доступа в систему |
| **3.3.6.** | Угрозы, реализуемые в ходе загрузки операционной системы |
| **3.4.** | Угрозы несанкционированного доступа к информации по каналам связи |
| **3.4.1.** | Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны |
| **3.4.2.** | Угрозы сканирования сети |
| **3.4.3.** | Угроза выявления паролей по сети |
| **3.4.4.** | Подмена доверенного объекта |
| **3.4.5.** | Навязывание ложного маршрута сети |
| **3.4.6.** | Внедрение ложного объекта сети |
| **3.4.7.** | Угрозы типа «Отказ в обслуживании» |
| **3.4.8.** | Угрозы внедрения по сети вредоносных программ/скриптов |
| **3.4.9.** | Утечка информации, передаваемой с использованием протоколов беспроводного доступа |
| **3.4.10.** | Угрозы удаленного запуска приложений |
| **3.4.11.** | Угрозы при использовании уязвимостей веб-сервисов или ошибок программирования |
| **3.5.** | Угрозы антропогенного характера |
| **3.5.1.** | Разглашение информации, модификация, уничтожение работниками, допущенными к ее обработке |
| **3.5.2.** | Сокрытие ошибок и неправомерных действий пользователей и администраторов |
| **3.5.3.** | Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей |
| **3.5.4.** | Угроза нарушения политики предоставления и прекращения доступа |
| **3.5.5.** | Непреднамеренная модификация (уничтожение) информации |
| **3.5.6.** | Непреднамеренное отключение средств защиты |
| **3.5.7.** | Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке |