Перечень угроз безопасности персональных данных информационной системы МКОУ «Линёвская СШ»

ВВЕДЕНИЕ

В модели угроз представлено описание структуры ИСПДн, состава и режима обработки ПДн, классификации потенциальных нарушителей, оценку исходного уровня защищенности, анализ угроз безопасности персональных данных.

Анализ УБПДн включает:

- описание угроз;
- оценку вероятности возникновения угроз;
- оценку реализуемости угроз;
- оценку опасности угроз;
- определение актуальности угроз.

Группа	**Уровень доступа к ПДн**	**Разрешенные действия**
Администраторы ИСПДн	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение
Администратор безопасности	Обладает правами Администратора ИСПДн. Обладает полной информацией об ИСПДн.	- сбор - систематизация - накопление - хранение

	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).	- уточнение - использование - уничтожение
Операторы ИСПДн с правами записи	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение
Операторы ИСПДн с правами чтения	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к подмножеству ПДн.	- использование

1.1 Классификация нарушителей

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

– внешние нарушители – физические лица, осуществляющие целенаправленное деструктивное воздействие, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;

– внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

В качестве основных уровней знаний нарушителей об АС можно выделить следующие:

– *общая информация* – информации о назначения и общих характеристиках ИСПДн;

1.2 Исходный уровень защищенности ИСПДн

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y1).

В таблице представлены характеристики уровня исходной защищенности для ИСПДн

Исходный уровень защищенности

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

Таким образом ИСПДн имеет низкий уровень исходной защищенности.

Реализуемость УБПДн

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам		
1.1. Угрозы утечки акустической информации	0,25	низкая
1.2. Угрозы утечки видовой информации	0,25	низкая
1.3. Угрозы утечки информации по	0,25	низкая

каналам ПЭМИН		
2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа		
2.1. Кража и уничтожение носителей информации	0,25	низкая
2.2. Кража физических носителей ключей и атрибутов доступа	0,25	низкий
2.3. Утрата носителей информации	0,25	низкая
2.4. Утрата и компрометация ключей и атрибутов доступа	0,35	низкий
3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств		
3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа	0,35	низкая
3.2. Утечка информации через порты ввода/вывода	0,25	Низкий
3.3. Воздействие вредоносных программ (вирусов)	0,35	Низкий
3.4. Установка ПО, не связанного с исполнением служебных обязанностей	0,35	низкий
3.5. Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных	0,35	низкая
3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему	0,25	низкая
4. Угрозы несанкционированного доступа к информации по каналам связи		
4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны	0,25	низкая
4.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соедине-	0,25	низкая

ний и др.		
4.3. Угрозы выявления паролей по сети	0,25	низкая
4.4. Угрозы типа «Отказ в обслуживании»	0,25	низкая
4.5. Угрозы внедрения по сети вредоносных программ	0,25	низкая
4.6.Утечка информации, передаваемой с использованием протоколов беспроводного доступа	0,25	низкая
4.7. Перехват, модификация закрытого ключа ЭЦП	0,25	низкая
4.8. Угрозы удаленного запуска приложений	0,25	низкая
5. Угрозы антропогенного характера		
5.1. Разглашение информации	0,35	средняя
5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов	0,35	низкая
5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей	0,25	низкая
5.4. Угроза нарушения политики предоставления и прекращения доступа	0,25	низкая
5.5. Непреднамеренная модификация (уничтожение) информации	0,35	низкая
5.6. Непреднамеренное отключение средств защиты	0,25	низкая
6. Угрозы воздействия непреодолимых сил		
6.1. Стихийное бедствие	0,25	низкая
6.2. Выход из строя аппаратно-программных средств	0,25	низкая
6.3. Аварии (пожар, потоп, случайное отключение электричества)	0,25	низкая

Опасность УБПДн

Тип угроз безопасности ПДн	Опасность угрозы
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	низкая
1.2. Угрозы утечки видовой информации	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	низкая
2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа	
2.1. Кража и уничтожение носителей информации	низкая
2.2. Кража физических носителей ключей и атрибутов доступа	низкий
2.3. Утрата носителей информации	низкая
2.4. Утрата и компрометация ключей и атрибутов доступа	низкий
3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств	
3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа	низкая
3.2. Утечка информации через порты ввода/вывода	Низкий
3.3. Воздействие вредоносных программ (вирусов)	Низкий
3.4. Установка ПО, не связанного с исполнением служебных обязанностей	низкий
3.5. Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных	низкая
3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему	низкая
4. Угрозы несанкционированного доступа к информации по каналам связи	
4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны	низкая
4.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	низкая

4.3. Угрозы выявления паролей по сети	низкая
4.4. Угрозы типа «Отказ в обслуживании»	низкая
4.5. Угрозы внедрения по сети вредоносных программ	низкая
4.6.Утечка информации, передаваемой с использованием протоколов беспроводного доступа	низкая
4.7. Перехват, модификация закрытого ключа ЭЦП	низкая
4.8. Угрозы удаленного запуска приложений	низкая
5. Угрозы антропогенного характера	
5.1. Разглашение информации	низкий
5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов	низкая
5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей	низкая
5.4. Угроза нарушения политики предоставления и прекращения доступа	низкая
5.5. Непреднамеренная модификация (уничтожение) информации	низкая
5.6. Непреднамеренное отключение средств защиты	низкая
6. Угрозы воздействия непреодолимых сил	
6.1. Стихийное бедствие	низкая
6.2. Выход из строя аппаратно-программных средств	низкая
6.3. Аварии (пожар, потоп, случайное отключение электричества)	низкая

Актуальность УБПДн

Тип угроз безопасности ПДн	Опасность угрозы
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	неактуальная
1.2. Угрозы утечки видовой информации	актуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	неактуальная
2. Угрозы несанкционированного доступа к информации путем физическо-	

го доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа	
2.1. Кража и уничтожение носителей информации	неактуальная
2.2. Кража физических носителей ключей и атрибутов доступа	актуальная
2.3. Утрата носителей информации	неактуальная
2.4. Утрата и компрометация ключей и атрибутов доступа	актуальная
3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств	
3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа	неактуальная
3.2. Утечка информации через порты ввода/вывода	актуальная
3.3. Воздействие вредоносных программ (вирусов)	актуальная
3.4. Установка ПО, не связанного с исполнением служебных обязанностей	актуальная
3.5. Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных	неактуальная
3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему	неактуальная
4. Угрозы несанкционированного доступа к информации по каналам связи	
4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны	неактуальная
4.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	неактуальная
4.3. Угрозы выявления паролей по сети	неактуальная
4.4. Угрозы типа «Отказ в обслуживании»	неактуальная
4.5. Угрозы внедрения по сети вредоносных программ	неактуальная
4.6.Утечка информации, передаваемой с использованием протоколов беспроводного доступа	неактуальная
4.7. Перехват, модификация закрытого ключа ЭЦП	неактуальная
4.8. Угрозы удаленного запуска приложений	неактуальная
5. Угрозы антропогенного характера	
5.1. Разглашение информации	актуальная

5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов	неактуальная
5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей	неактуальная
5.4. Угроза нарушения политики предоставления и прекращения доступа	неактуальная
5.5. Непреднамеренная модификация (уничтожение) информации	неактуальная
5.6. Непреднамеренное отключение средств защиты	неактуальная
6. Угрозы воздействия непреодолимых сил	
6.1. Стихийное бедствие	неактуальная
6.2. Выход из строя аппаратно-программных средств	неактуальная
6.3. Аварии (пожар, потоп, случайное отключение электричества)	неактуальная

Были выявлены следующие актуальные угрозы:

– кража физических носителей ключей и атрибутов доступа;

– утрата и компрометация ключей и атрибутов доступа;

– утечка информации через порты ввода/вывода;

– воздействие вредоносных программ (вирусов);

– установка ПО, не связанного с исполнением служебных обязанностей;

– разглашение информации.

Для снижения опасности реализации актуальных УБПДн рекомендуется осуществить следующие мероприятия:

– установка антивирусной защиты;

– парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

– назначить 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;

– осуществление резервирования ключевых элементов ИСПДн;

– изолирование портов ввода/вывода;

– организация разграничения прав пользователей на установку стороннего ПО, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов ИСПДн и средств защиты.