МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ "НОВОТОРЪЯЛЬСКИЙ ЦЕНТР ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ"

Приложение № 5 к приказу
№ 273 от 08.09.2023г.

Техническое задание на создание системы защиты для информационных систем персональных данных «Кадры», «Ученики»

пгт. Новый Торъял
2023 г.

СПИСОК СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

АВС – антивирусные средства
АРМ – автоматизированное рабочее место
АС – автоматизированная система
АСЗИ – автоматизированная система в защищенном исполнении
ИСПДн – информационная система персональных данных
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
ОС – операционная система
ПДн – персональные данные
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
СКЗИ – средства криптографической защиты информации
СОВ – система обнаружения вторжений
ТС – техническое средство
УБПДн – угрозы безопасности персональных данных

НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Настоящий документ составлен в соответствии со следующими действующими нормативно-методическими документами в области защиты персональных данных:

[1] – Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

[2] – Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

[3] – Постановление Правительства Российской Федерации об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных от 1 ноября 2012 г.№1119;

[4] –Приказ ФСТЭК от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

[5] – Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 14 февраля 2008г. заместителем директора ФСТЭК России);

[6] – Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 15 февраля 2008г. заместителем директора ФСТЭК России).

ОБОСНОВАНИЕ РАЗРАБОТКИ СИСТЕМЫ ЗАЩИТЫ

В информационных системах «Кадры», «Ученики», предполагается обработка персональных данных. Информационные системы «Кадры», «Ученики»,попадают под действие закона [2]. В соответствии с [3] требуется обеспечить безопасность персональных данных. Безопасность персональных данных обеспечивается выполнением комплекса организационных и технических мер защиты, которые определяются в соответствии с нормативно-методическими документами ФСТЭК России и ФСБ России.

Система защиты должна разрабатываться с целью предотвращения ущерба от возможной реализации нарушений характеристик безопасности. Угрозы безопасности определены в «Модели угроз информационной системы…» (далее Модель угроз).

Настоящий документ разработан для решения следующих задач:

- разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;
- создание регламента проведения мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
- создание регламента мероприятий, обеспечивающих контроль за обеспечением уровня защищенности персональных данных.

ИСХОДНЫЕ ДАННЫЕ

Описание информационных систем персональных данных «Кадры», «Ученики», приведено в Модели угроз.

Для информационных систем «Кадры», «Ученики» определен предполагаемый уровень защищенности ИСПДн – 4. По заданным характеристикам безопасности (заданы в Модели угроз), информационная система является специальной, и требования для нее формируются на основании модели угроз.

Перечень требований безопасности персональных данных, предусмотренный нормативно-методическими документами для ИСПДн с заданными параметрами (классом, режимом обработки данных) представлен в таблице.

Защита информации от выявленных угроз сводится к принятию организационных и технических мер, которые позволяют избавиться от тех или иных компонентов угроз.

В таблице представлен список требований, которые нужно выполнить для нейтрализации угроз ИСПДн «Кадры», «Ученики».

№ п/п	Требование
1	**2**
1	фильтрация на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов)
2	идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия
3	регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана)
4	контроль целостности программной и информационной части межсетевого экрана
5	фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств
6	восстановление свойств межсетевого экрана после сбоев и отказов оборудования
7	регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления
8	использование средств антивирусной защиты
9	использование в составе информационной системы программных или программно-аппаратных средств (систем) анализа защищенности. Средства (системы) анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему
10	использование в составе информационной системы программных или программно-аппаратных средств (систем) обнаружения вторжений
11	Для выбора и реализации методов и способов защиты информации в информационной системе оператором или уполномоченным лицом требуется назначить структурное подразделение или должностное лицо (работника), ответственные за обеспечение безопасности персональных данных
12	обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними
13	учет лиц, допущенных к работе с персональными данными в информационной системе; лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к 14 соответствующим персональным данным на основании списка, утвержденного оператором или уполномоченным лицом
14	разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие

№ п/п	Требование
1	**2**
	мер по предотвращению возможных опасных последствий подобных нарушений
15	регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы
16	при регистрации входа (выхода) пользователя в систему (из системы) либо регистрации загрузки и инициализации операционной системы и ее программного останова в параметрах регистрации дополнительно указывается результат попытки входа (успешная или неуспешная)
17	при регистрации входа (выхода) пользователя в систему (из системы) либо регистрации загрузки и инициализации операционной системы и ее программного останова в параметрах регистрации дополнительно указывается идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа
18	учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме)
19	размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные
20	идентификация и проверка подлинности пользователя при входе в систему информационной системы по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов
21	при идентификации и проверке подлинности пользователя при входе в систему должен дополнительно использоваться идентификатор (код)
22	физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации
23	периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа
24	наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности
25	обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации
26	физическая охрана технических средств информационных систем (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания

ПЕРЕЧЕНЬ ПРЕДЛАГАЕМЫХ К ИСПОЛЬЗОВАНИЮ СЕРТИФИЦИРОВАННЫХСРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

В данном разделе представлены средства защиты информации для реализации технических мер защиты. Специалисты оператора оставляют за собой право выбора тех или иных средств защиты, исходя из особенностей работы информационной системы.

№ п/п	Тип СЗИ	СЗИ	Описание СЗИ	Сертификат
1.	сертифицированные средства защиты информации от несанкционированного доступа	Блокхост-Сеть	Средство защиты информации от несанкционированного доступа; производитель: ООО «Газинформсервис»	ФСТЭК, №1517, от 30.11.2007
2.	сертифицированные средства защиты информации от несанкционированного доступа	Secret Net 5.1	Средство защиты информации от несанкционированного доступа; производитель: ООО «Код Безопасности»	ФСТЭК, №1912, от 17.09.2009
3.	сертифицированные средства защиты информации от несанкционированного доступа	Dallas Lock 7.5	Средство защиты информации от несанкционированного доступа; производитель ООО «Конфидент»	ФСТЭК, №1685, от 18.09.2008
4.	сертифицированные средства защиты информации от несанкционированного доступа	Страж NT 3.0	Средство защиты информации от несанкционированного доступа; производитель: ЗАО «НПЦ «Модуль»	ФСТЭК, №2145, от 30.07.2010
5.	сертифицированные средства защиты информации от несанкционированного доступа	Dr.Web Enterprise Security Suite	Средство защиты информации от несанкционированного доступа; производитель: «Доктор Веб»	ФСТЭК, №2446, от 20.09.2011
6.	сертифицированные средства защиты информации от несанкционированного доступа	Security Studio	Средство защиты информации от несанкционированного доступа; производитель: ООО «Код Безопасности»	ФСТЭК, №1597, от 24.04.2008

Допускается применение прочих сертифицированных средств защиты информации, если это требуется исходя из особенностей функционирования системы. Полный реестр сертифицированных средств защиты информации представлен на сайте ФСТЭК России.