Утверждаю
Директор МБОУ
«ООШ №2 ст.Кардоникской»
_____ Л.И. Малютина
Приказ № 111 от « 01.09.2023г. »

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Информационной системы персональных данных
1.Обозначения и сокращения

АВС - антивирусные средства
АРМ - автоматизированное рабочее место
ВТСС - вспомогательные технические средства и системы
ИСПДн - информационная система персональных данных
КЗ - контролируемая зона
ЛВС - локальная вычислительная сеть
МЭ - межсетевой экран
НСД - несанкционированный доступ
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
СОВ - система обнаружения вторжений
ТКУ И - технические каналы утечки информации
УБПДн - угрозы безопасности персональных данных

2. Общие положения

2.1. Настоящая Политика информационной безопасности (далее - Политика) образовательной организации является официальным документом.
2.2. Политика разработана для достижения целей и задач обеспечения безопасности персональных данных в соответствии с требованиями Федерального закона от 27 июля 2006 г. N° 152-ФЗ «О персональных данных» и Постановления Правительства Российской Федерации от 1 ноября 2012 г. N° 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», на основании.
- Приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) 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»,
- «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. N° 149/6/6-662.

2.3. В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн образовательной организации.
2.4. Целью настоящей Политики является обеспечение безопасности объектов защиты образовательной организации от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).
2.5. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.
2.6. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.
Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.
2.7. Состав объектов защиты представлен в Перечне персональных данных, обрабатываемых в ИСПДн.

3. Область действия

Требования настоящей Политики распространяются на всех работников образовательной организации (штатных, по совместительству и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

4 Система защиты персональных данных

4.1. Система защиты персональных данных (СЗПДн), строится на основании:

- *Перечня персональных данных, обрабатываемых в ИСПДн;*
- *Акта обследования ИСПДн;*
- *Модели угроз безопасности персональных данных при их обработке в ИСПДн;*
- *Руководящих документов ФСТЭК и ФСБ России.*

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн образовательной организации. На основании анализа актуальных угроз безопасности ПДн, описанного в *Модели угроз,* делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн.
4.2. Выбранные необходимые мероприятия отражаются в *Плане мероприятий по обеспечению безопасности персональных данных в соответствии с требованиям ФЗ «О персональных данных»*.
Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а так же программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:
- АРМ пользователей;
- СУБД;

- каналы передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- антивирусные средства для рабочей станции пользователя;
- модуль доверенной загрузки;
- средства межсетевого экранирования;
- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты.

Список функций защиты может включать:

- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечивать целостность данных;
- производить обнаружения вторжений.

Список используемых технических средств отражается в *Техническом паспорте информационной системы персональных данных*. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Технический паспорт и утверждены директором образовательной организации или, ответственным за обеспечение безопасности ПДн.

5. Требования к подсистемам СЗПДн

СЗПДн включает в себя следующие меры:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

Подсистемы СЗПДн имеют различный функционал в зависимости от уровня защищенности ИСПДн, определенного в *Акте определения уровня защищенности персональных данных в ИСПДн*.

5.1 Идентификация и аутентификация субъектов доступа и объектов доступа

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

5.2 Управление доступом субъектов доступа к объектам доступа

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль над соблюдением этих правил.

5.3 Ограничение программной среды

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

5.4 Защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные

Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

5.5 Регистрация событий безопасности

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

5.6 Антивирусная защита

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

5.7 Обнаружение вторжений

Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

5.8 Контроль (анализ) защищенности персональных данных

Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

5.9 Обеспечение целостности информационной системы и персональных данных

Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

5.10 Обеспечение доступности персональных данных

Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

5.11 Защита технических средств

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы, и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

5.12 Защита информационной системы, ее средств, систем связи и передачи данных

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

5.13 Выявление инцидентов и реагирование на них

Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

5.14 Управление конфигурацией информационной системы и системы защиты персональных данных

Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

6. Пользователи ИСПДн

В ИСПДн образовательной организации можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Ответственный за обеспечение безопасности персональных данных (администратор безопасности ИСПДн);
- работники образовательной организации (разрешительная система доступа пользователей- работников к информационным ресурсам ИСПДн оформляется в виде Приказа об утверждении перечня сотрудников, допущенных к обработке персональных данных)

6.1 Ответственный за обеспечение безопасности персональных данных(администратор безопасности ИСПДн)

Ответственный за обеспечение безопасности персональных данных – сотрудник образовательной организации, ответственный за организацию работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Ответственный за обеспечение безопасности персональных данных обладает следующим уровнем доступа и знаний:

- обладает полной информацией о перечне персональных данных и технических средств, входящих в информационные системы персональных данных;
- обладает полной информацией о списке лиц, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения служебных (трудовых) обязанностей;
- обладает полной информацией о текущем состоянии защищенности ИСПДн образовательной организации;
- имеет доступ ко всем программным и аппаратным средствам обработки информации и данным ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- имеет доступ ко всем помещениям, где ведется обработка персональных данных.

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).
- осуществлять аудит средств защиты;

6.2. Работники образовательной организации

Разрешительная система доступа пользователей- работников к информационным ресурсам ИСПДн оформляется в виде Приказа об утверждении перечня сотрудников, допущенных к обработке персональных данных.

Обязанности и полномочия пользователей ИСПДн определяет инструкция пользователя ИСПДн, утвержденная директором образовательной организации.

7. Требования к работникам образовательной организации по обеспечению защиты ПДн

7.1. Все сотрудники образовательной организации, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника администратор безопасности ИСПДн обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Работник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Работники образовательной организации, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей (паролей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники образовательной организации должны следовать Инструкции по организации парольной защиты.

Сотрудники образовательной организации должны выполнять требования Инструкции пользователя ИСПДн.

При работе с ПДн в ИСПДн сотрудники образовательной организации обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ.

Сотрудники образовательной организации должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

7.2 Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:
- Инструкция ответственного за обеспечение безопасности персональных данных (администратора безопасности);
- Инструкция пользователя ИСПДн.

8. Ответственность работников ИСПДн образовательной организации

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

8.1. Ответственный за обеспечение безопасности персональных данных (администратор безопасности) несет ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

8.2. При нарушениях сотрудниками образовательной организации– пользователями ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приведенные выше требования нормативных документов по защите информации должны быть отражены в должностных инструкциях сотрудников образовательной организации.

9. Основные нормативно-правовые и методические документы, на которых базируется настоящая Политика

1 Федеральный Закон № 152-ФЗ от 27.07.2006 г. «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.

2 Постановление Правительства РФ № 1119 от 01.11.2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3 «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ № 687 от 15.09.2008 г.

4 Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:

4.1 Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

4.2 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.2008г.

4.3 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.2008 г.