

УТВЕРЖДАЮ

Директор
МБОУ СОШ г. Пионерского

Т.В. Леткова

«20» февраля 2019 г.

м.п.



ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Настоящая Политика информационной безопасности (далее – Политика) **Муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа города Пионерский»** (далее – Учреждение) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных и является официальным документом.

Политика разработана в соответствии с требованиями:

- Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказа 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»;
- приказа ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости».
- постановления Правительства Российской Федерации от 10 июля 2013 г. № 582 «Об утверждении правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации».

В Политике определены требования к работникам Учреждения, допущенным для работы в информационных системах персональных данных (далее – ИСПДн), степень ответственности таких работников, структура и необходимый уровень защищённости ИСПДн Учреждения, статус и обязанности работников, ответственных за обеспечение безопасности персональных данных (далее – ПДн) в ИСПДн Учреждения.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Целью настоящей Политики является:

- а) обеспечение безопасности объектов защиты Учреждения от всех видов угроз (внешних, внутренних; умышленных, непреднамеренных);
- б) минимизация ущерба от возможной реализации угроз безопасности персональных данных (далее - УБПДн).

Безопасность ПДн, обрабатываемых в Учреждении, достигается путем исключения несанкционированного, в том числе случайного доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей Учреждения (работников, допущенных для выполнения своих должностных обязанностей в информационных системах персональных данных).

Информация, размещаемая на официальном сайте Учреждения в информационно-телекоммуникационной сети «Интернет» без согласия субъекта персональных данных, не превышает перечня персональных данных, разрешенного для открытого опубликования, установленного нормативными правовыми актами Российской Федерации. Размещение дополнительной информации о субъектах персональных данных, выходящей за рамки перечня информации, разрешенной для открытого опубликования, производится только при письменном согласии субъекта персональных данных.

В Учреждении осуществляется своевременное обнаружение и реагирование на УБПДн и предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты Учреждения утвержден приказами руководителя:

- «Об утверждении перечня информационных систем персональных данных, перечня персональных данных, подлежащих защите, контролируемой зоны помещений, о назначении администратора информационной безопасности»;

- «Об утверждении комиссий, мест хранения материальных носителей персональных данных, допуске лиц к работе со средствами криптографической защиты информации, общей документации, назначении ответственных».

Состав ПДн, обрабатываемых в ИСПДн Учреждения и подлежащих защите, утвержден приказом по Учреждению:

- «Об утверждении перечня информационных систем персональных данных, перечня персональных данных, подлежащих защите, контролируемой зоны помещений, о назначении администратора информационной безопасности».

Настоящая Политика утверждена руководителем Учреждения.

Требования настоящей Политики распространяются на всех работников Учреждения, а также иных лиц, взаимодействующих с Учреждением.

2. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Система защиты персональных данных (далее - СЗПДн) Учреждения строится на основании:

- аналитических отчетов по результатам обследования информационных систем персональных данных (далее – Аналитический отчет);
- частных моделей угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- перечня персональных данных, подлежащих защите;
- актов определения уровня защищенности персональных данных при их обработке в информационных системах персональных данных;
- локальных актов (приказов, распоряжений) по Учреждению;
- организационно-распорядительной документации, относящейся к системе защиты информации и персональных данных Учреждения;
- руководящих и нормативных документов Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязи России);
- руководящих и нормативных документов Управления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Управление Роскомнадзора Российской Федерации);
- руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Учреждения.

На основании анализа актуальных угроз безопасности ПДн, описанных в частных моделях угроз безопасности персональных данных, технических заданиях на разработку СЗПДн, делается заключение о необходимости использования технических средств и проведения организационных мероприятий для обеспечения безопасности ПДн Учреждения.

Избранные необходимые мероприятия отражаются в **Плане мероприятий по обеспечению безопасности персональных данных Учреждения.**

План мероприятий по обеспечению безопасности персональных данных утверждается приказом руководителя Учреждения.

В Учреждении для ИСПДн, относящимся к государственным или региональным системам, проводятся мероприятия по аттестации ИСПДн требованиям безопасности информации.

При проведении работ в Аналитических отчетах составляется перечень используемых технических средств, программного обеспечения, участвующего в обработке ПДн на всех элементах ИСПДн, включающих в себя:

- а) перечень основных технических средств и систем (далее – ОТСС);
- б) перечень вспомогательных технических средств, располагаемых совместно с ОТСС;
- в) перечень программного обеспечения, используемого в ИСПДн;
- г) перечень работников Учреждения, допущенных для работы в соответствующей ИСПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз СЗПДн может включать следующие технические средства защиты информации (далее – ТСЗИ):

- а) антивирусные средства для рабочих мест пользователей и серверов;
- б) средства защиты информации от несанкционированного доступа;
- в) средства межсетевое экранирования;
- г) средства криптографической защиты информации, используемые при передаче защищаемой информации по открытым каналам связи.

Список используемых технических средств защиты отражается в «Журнале учета средств защиты».

Список используемых технических средств защиты информации должен поддерживаться в актуальном состоянии. При изменении состава ТСЗИ соответствующие изменения должны быть внесены в «Журнал учета средств защиты».

Список используемых криптографических средств защиты отражается в «Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов».

Список используемых криптографических средств защиты информации должен поддерживаться в актуальном состоянии.

При изменении состава СКЗИ соответствующие изменения должны быть внесены в «Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов».

3. ТРЕБОВАНИЯ К ПОДСИСТЕМАМ СЗПДН

СЗПДн Учреждения включает в себя следующие подсистемы:

- а) управления доступом, регистрацией и учетом;
- б) обеспечения целостности и доступности;
- в) антивирусной защиты;
- г) межсетевого экранирования;
- д) анализа защищенности;
- е) обнаружения вторжений;
- ж) отсутствия недеklarированных возможностей;
- з) криптографической защиты.

Подсистемы СЗПДн имеют различный функционал в зависимости от определенных уровней защищенности ИСПДн, определенных в актах определения уровня защищенности персональных данных при их обработке в информационных системах персональных данных Учреждения.

4. ПОЛЬЗОВАТЕЛИ ИСПДН

Пользователи – работники Учреждения, осуществляющие обработку ПДн.

Данные о пользователях, уровне их доступа и информированности отражены в приказе по Учреждению:

- «Об утверждении организационно-технической документации, относящейся к защите персональных данных, списков постоянных пользователей информационных систем персональных данных, об установлении прав доступа к информационным и техническим ресурсам».

Пользователи имеют доступ к обработке ПДн, которая включает в себя: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПДн.

Пользователи не имеют полномочий для управления подсистемами обработки данных и СЗПДн.

Пользователи ИСПДн обладают следующими уровнями доступа и знаний:

- а) обладают всеми необходимыми знаниями для работы с ПДн;
- б) имеют личный идентификатор (имя пользователя) и аутентификатор (пароль).

5. ТРЕБОВАНИЯ К РАБОТНИКАМ УЧРЕЖДЕНИЯ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПДН

Все работники Учреждения, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдать принятый режим безопасности ПДн, а также быть ознакомленными с руководящими документами по информационной безопасности Учреждения.

Организационно-распорядительная и техническая документация, относящаяся к СЗПДн, утверждается в приказах по Учреждению:

- «Об утверждении Положения об обработке и защите персональных данных, организационно-технической, общей документации, относящейся к защите персональных данных»;

- «Об утверждении организационно-технической документации, относящейся к защите персональных данных, списков постоянных пользователей информационных систем персональных данных, об установлении прав доступа к информационным и техническим ресурсам»;

- «Об утверждении комиссий, мест хранения материальных носителей персональных данных, допуске лиц к работе со средствами криптографической защиты информации, общей документации, назначении ответственных».

При вступлении в должность нового работника ответственный за организацию обработки персональных данных и выполнение мероприятий по обеспечению безопасности персональных данных Учреждения (далее – Ответственный) знакомит указанного работника с необходимыми документами, регламентирующими требования по защите ПДн, а также обучает его правилам работы с ПДн в ИСПДн.

Работники Учреждения под роспись знакомятся с должностными инструкциями, организационно-распорядительной документацией, относящейся к системе защиты ПДн Учреждения, настоящей Политикой, принятыми процедурами работы с элементами ИСПДн и СЗПДн, а также с Положением об обработке и защите персональных данных Учреждения.

Работники Учреждения, использующие технические средства аутентификации, в обязательном порядке обеспечивают сохранность идентификаторов (электронных ключей) и не допускают несанкционированного доступа (далее - НСД) к ним, исключают возможность их утери и вероятность использования третьими лицами.

Работники Учреждения проинструктированы о необходимости следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Работники Учреждения ознакомлены с правилами обеспечения надлежащей защиты оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица.

Все работники Учреждения как пользователи ознакомлены с требованиями по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также знают свои обязанности по обеспечению такой защиты.

При работе с ПДн работники Учреждения ознакомлены с требованиями обеспечения отсутствия возможности просмотра ПДн третьими лицами с мониторов автоматизированных рабочих мест (далее – АРМ) или терминалов.

При завершении работы с ПДн все работники Учреждения ознакомлены с правилами защиты АРМ с помощью блокировки (*комбинация Ctrl-Alt-Del, далее Блокировка компьютера; комбинация Клавиша Windows+L*).

Работники Учреждения проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение.

Работники Учреждения ознакомлены с дисциплинарными взысканиями при нарушении требований безопасности работы с ПДн в соответствии с действующим федеральным законодательством Российской Федерации в области защиты информации и персональных данных.

Контроль за соблюдением режима безопасности обработки ПДн возложен на Ответственного в соответствии с приказом по Учреждению:

- «О назначении ответственного за организацию обработки персональных данных, ответственного за эксплуатацию объекта информатизации».

Работники Учреждения, допущенные к работам с техническими и криптографическими средствами защиты, проходят обучение по правилам работы, хранения и учета технических и криптографических средств защиты информации.

Допуск работников Учреждения к работе со средствами криптографической защиты информации утверждается приказом по Учреждению:

- «Об утверждении комиссий, мест хранения материальных носителей персональных данных, допуске лиц к работе со средствами криптографической защиты информации, общей документации, назначении ответственных».

Работники Учреждения под роспись знакомятся с инструкциями, правилами, руководствами, принятыми процедурами работы с установленными средствами криптографической защиты информации.

Работники Учреждения, использующие средства криптографической защиты информации, в обязательном порядке обеспечивают их сохранность и не допускают НСД к ним, исключают возможность их утери и вероятность использования третьими лицами.

Работники Учреждения обязаны без промедления сообщать руководителю Учреждения, Ответственному Учреждения обо всех случаях работы в ИСПДн, которые могут повлечь за собой угрозу безопасности ПДн.

Работникам Учреждения **ЗАПРЕЩАЕТСЯ**

- а) устанавливать постороннее программное обеспечение,
- б) подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.
- в) разглашать защищаемую информацию, которая стала им известна при работе в информационных системах Учреждения, третьим лицам.

6. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ РАБОТНИКОВ (ПОЛЬЗОВАТЕЛЕЙ) ИСПДН

Должностные обязанности пользователей ИСПДн Учреждения описаны в следующих организационно-распорядительных документах:

- инструкции ответственного за организацию обработки персональных данных;
- инструкции пользователя информационных систем персональных данных;
- инструкции по организации режима доступа в помещения, о порядке действий при несанкционированном проникновении в помещения и других нештатных ситуациях;
- инструкции о порядке планирования и проведения проверок информационной безопасности в информационных системах персональных данных;
- положении об обработке и защите персональных данных Учреждения;

- должностных инструкциях Учреждения.

7. ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ УЧРЕЖДЕНИЯ, ОБРАБАТЫВАЮЩИХ ПДН В ИСПДН

Учреждение как Оператор **ОБЯЗАНО** назначить лицо, ответственное за организацию обработки персональных данных в соответствии с приказом по Учреждению:

- «О назначении ответственного за организацию обработки персональных данных, ответственного за эксплуатацию объекта информатизации».

Лицо, ответственное за организацию обработки персональных данных в Учреждении, получает указания непосредственно от руководителя Учреждения и подотчетно ему.

Должностное лицо, ответственное за организацию обработки персональных данных в Учреждении, **ОБЯЗАНО**:

а) осуществлять внутренний контроль за соблюдением работниками Учреждения законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

б) доводить до сведения работников Учреждения положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных (распоряжений, инструкций); требования к защите персональных данных;

в) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных, подлежит возмещению в соответствии с законодательством Российской Федерации.

Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Для решения вопросов по расследованию инцидентов информационной безопасности, возникших при обработке ПДн и другой конфиденциальной информации, уничтожения документов, содержащих персональные данные, в Учреждении создаются комиссии.

Состав комиссий утверждается приказом по Учреждению:

- «Об утверждении комиссий, мест хранения материальных носителей персональных данных, допуске лиц к работе со средствами криптографической защиты информации, общей документации, назначении ответственных».

Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных, изложена в:

а) Кодексе об административных правонарушениях Российской Федерации (КоАП РФ) – статьи 5.27, 5.39, 13.11-13.14, 19.4-19.7, 19.20, 20.25, 32.2;

б) Уголовном кодексе Российской Федерации (УК РФ) – статьи 137, 140, 155, 183, 272, 273, 274, 292, 293;

в) Трудовом кодексе Российской Федерации (ТК РФ) – статьи 81, 90, 195, 237, 391.

8. РАЗМЕЩЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОФИЦИАЛЬНОМ САЙТЕ УЧРЕЖДЕНИЯ

Учреждение, в соответствии с законодательством Российской Федерации, имеет право размещать следующие персональные данные без письменного согласия субъекта персональных данных:

- фамилию, имя, отчество и должность руководителей структурных подразделений;

- сведения о руководителе Учреждения, заместителях руководителя Учреждения, руководителях филиалов Учреждения (при их наличии), а именно:
 - фамилию, имя, отчество (при наличии) руководителя, заместителей руководителя;
 - должность руководителя, заместителей руководителя;
 - адрес электронной почты;
 - контактные телефоны;
- сведения о персональном составе педагогических работников с указанием уровня образования, квалификации и опыта работы, а именно:
 - фамилия, имя, отчество (при наличии) работника;
 - сведения о занимаемой должности (должностях);
 - сведения о преподаваемых дисциплинах;
 - сведения об ученой степени (при наличии);
 - сведения об ученом звании (при наличии);
 - наименование направления подготовки и (или) специальности;
 - данные о повышении квалификации и (или) профессиональной переподготовке (при наличии);
 - сведения об общем стаже работы;
 - сведения о стаже работы по специальности;
- иную информацию, которая размещается, публикуется по решению Учреждения и (или) размещение, опубликование которой являются обязательными в соответствии с законодательством Российской Федерации.

Учреждение обновляет вышеуказанные сведения не позднее 10 (десяти) рабочих дней после их изменений.

Учреждение производит размещение изображения субъекта персональных данных на официальном сайте (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) только с согласия субъекта.

Учреждение имеет право на размещение изображения субъекта персональных данных на официальном сайте (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) без согласия субъекта в случаях, когда:

- использование изображения осуществляется в государственных, общественных или иных публичных интересах;
- изображение субъекта персональных данных получено при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях (собраниях, съездах, конференциях, концертах, представлениях, спортивных соревнованиях и подобных мероприятиях), за исключением случаев, когда такое изображение является основным объектом использования;
- субъект персональных данных позировал за плату.

Опубликование иных сведений субъектов персональных данных, не указанных в данном разделе, производится только после получения письменного согласия от субъекта персональных данных или его законного представителя, с указанием в согласии перечня персональных данных, которые будут опубликованы на официальном сайте Учреждения.