УТВЕРЖДЕНО

Приказом МАОУ

«СОШ №1» г. Светлогорска

от 29.12.2017. № 213 – II

_____ Н.В.Гречкина

Настоящая Политика информационной безопасности (далее – Политика) **муниципального автономного общеобразовательного учреждения «Средняя общеобразовательная школа №1» г. Светлогорска** (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 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Федерального закона Российской Федерации от 3 ноября 2006 года 174-ФЗ «Об автономных учреждениях»,
- Федерального закона Российской Федерации от 29 декабря 2012 года №273-ФЗ «Об образовании в Российской Федерации»;
- постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа ФСТЭК России от 18 февраля 2013 года № 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 года № 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».

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

1. ОБЩИЕ ПОЛОЖЕНИЯ

Целью настоящей Политики является:

❖ обеспечение безопасности объектов защиты Учреждения от всех видов угроз (внешних, внутренних, умышленных, непреднамеренных);

❖ 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, допущенным для выполнения своих должностных обязанностей в информационных системах 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 в Учреждения утвержден приказами по Учреждению:

- **«Об утверждении перечня информационных систем персональных данных, перечня персональных данных, обрабатываемых в информационных системах персональных данных, списков постоянных пользователей и установление прав доступа пользователям к информационным и техническим ресурсам»;**
- **«Об утверждении комиссий, организационно-распорядительной документации, мест хранения материальных носителей персональных данных, ответственных за помещения».**

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

- **«Об утверждении перечня информационных систем персональных данных, перечня персональных данных, обрабатываемых в информационных системах персональных данных, списков постоянных пользователей и установление прав доступа пользователям к информационным и техническим ресурсам».**

Настоящая Политика утверждена директором Учреждения.

Требования настоящей Политики распространяются на всех работников Учреждения, а также всех 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 информационной системе персональных данных;
- ❖ Перечня персональных данных, подлежащих защите;
- ❖ Актов определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных;
- ❖ Приказов 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.

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

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

В Учреждении ИСПДн, относящиеся 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:

- Перечень основных технических средств и систем (далее – ОТСС);
- Перечень вспомогательных технических средств, располагаемых совместно с ОТСС;
- Перечень программного обеспечения, используемого в ИСПДн;
- 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):

- антивирусные средства для рабочих мест пользователей и серверов;
- средства защиты информации от несанкционированного доступа;
- средства межсетевого экранирования;
- 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 Администрации включает в себя следующие подсистемы:

- управления доступом, регистрацией и учетом;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- отсутствие недекларированных возможностей;
- криптографической защиты.

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

4. ПОЛЬЗОВАТЕЛИ ИСПДН

В ИСПДн Учреждения выделены следующие группы пользователей, участвующих в обработке и хранении ПДн:

- администратор информационной безопасности;
- пользователь.

Администратор ИБ назначается приказом по Учреждению:

- **«О назначении администратора информационной безопасности, утверждении инструкций и журналов».**

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

- **«Об утверждении перечня информационных систем персональных данных, перечня персональных данных, обрабатываемых в информационных системах персональных данных, списков постоянных пользователей и установление прав доступа пользователям к информационным и техническим ресурсам».**

4.1. Администратор информационной безопасности

Администратор информационной безопасности (далее – администратор ИБ) это работник Учреждения, ответственный за функционирование СЗПДн, включая обслуживание и настройку клиентской и серверной составляющих.

Администратор ИБ обладает следующим уровнем доступа и знаний:

- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.

Администратор ИБ уполномочен:

- реализовывать политику безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователи получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других организаций и учреждений;
- осуществлять внутренние проверки режима защиты персональных данных в информационных системах персональных данных Учреждения и фиксировать их в «Журнале внутренних проверок режима защиты персональных данных в информационных системах персональных данных».

4.2. Пользователи

Пользователи – работники Учреждения, осуществляющие обработку ПДн.

Пользователи назначаются приказом по Учреждению:

- **«Об утверждении перечня информационных систем персональных данных, перечня персональных данных,**

обрабатываемых в информационных системах персональных данных, списков постоянных пользователей и установление прав доступа пользователям 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 ИСПД.

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

Пользователи ИСПДн обладают следующими уровнями доступа и знаний:

- ❖ обладают всеми необходимыми знаниями для работы с ПДн;
- ❖ 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 с СЗПДн утверждается в приказах по Учреждению:

- ❄ **«Об утверждении Положения, инструкций и форм журналов по информационной безопасности»**;
- ❄ **«Об утверждении комиссий, организационно-распорядительной документации, мест хранения материальных носителей персональных данных, ответственных за помещения».**

При вступлении в должность нового работника ответственный за организацию обработки персональных данных и выполнение мероприятий по обеспечению безопасности персональных данных в Учреждении (далее – Ответственный) знакомит данного 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 НСД к ним, возможности их утери, 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 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 обработку персональных данных, проведении обследования информационных систем персональных данных, актуализации технической документации, относящейся к системе защиты персональных данных**».

Контроль за выполнением технических мероприятий по обеспечению безопасности ПДн возложен на работника Учреждения в соответствии с приказом по Учреждению:

- **«О защите персональных данных, обрабатываемых в информационных системах персональных данных».**

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:

- **«О допуске лиц к работе со средствами криптографической защиты информации».**

Работники Учреждения обязаны без промедления сообщать директору Учреждения, Ответственному, ответственному за технические мероприятия в Учреждении обо всех случаях работы ИСПДн, которые могут повлечь за собой угрозу безопасности ПДн.

Работникам Учреждения **ЗАПРЕЩАЕТСЯ**

- устанавливать постороннее программное обеспечение,
- подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.
- 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;
- Инструкции о порядке планирования и проведения проверок информационной безопасности в информационных системах персональных данных;
- Положении по использованию средств криптографической защиты информации;
- Руководстве ответственного пользователя средств криптографической защиты информации;
- Руководстве пользователя средств криптографической защиты информации;

- ❖ Инструкции по организации защиты средств криптографической защиты информации;
- ❖ Инструкции о порядке учёта, хранения, выдачи и уничтожения средств криптографической защиты информации;
- ❖ Положении об обработке и защите персональных данных;
- ❖ Должностных инструкциях работников 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 обработку персональных данных, проведении обследования информационной системе персональных данных, актуализации технической документации, относящейся к системе защиты персональных данных».**

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

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

- ❖ осуществлять внутренний контроль за соблюдением работниками Учреждения законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- ❖ доводить до сведения работников Учреждения положения: законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных (распоряжения, инструкции), требования к защите персональных данных;

❖ 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 Учреждения созданы комиссии.

Состав комиссий утверждается приказом по Учреждению:

❋ **«Об утверждении комиссий, организационно-распорядительной документации, мест хранения материальных носителей персональных данных, ответственных за помещения».**

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

❖ 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;**

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

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

Администратор ИБ Учреждения несет ответственность за все действия, совершенные от имени учетных записей или системных учетных записей пользователей, если не доказан факт несанкционированного использования учетных записей.

ОПРЕДЕЛЕНИЯ

При обработке персональных данных используются следующие определения:

АВТОМАТИЗИРОВАННАЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ - обработка персональных данных с помощью средств вычислительной техники.

БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

ДОСТУП К ИНФОРМАЦИИ – получение возможности ознакомления с информацией, в том числе при помощи технических средств.

ЗАЩИЩАЕМАЯ ИНФОРМАЦИЯ – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

ИДЕНТИФИКАЦИЯ – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

ИНФОРМАЦИОННАЯ СИСТЕМА ПЕРСОНАЛЬНЫХ ДАННЫХ (ИСПДН) – информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

ИСПОЛЬЗОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

ИСТОЧНИК УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

КОНТРОЛИРУЕМАЯ ЗОНА – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

МЕЖСЕТЕВОЙ ЭКРАН – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

НАРУШИТЕЛЬ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

НЕАВТОМАТИЗИРОВАННАЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

НЕДЕКЛАРИРОВАННЫЕ ВОЗМОЖНОСТИ – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП (НЕСАНКЦИОНИРОВАННЫЕ ДЕЙСТВИЯ) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

НОСИТЕЛЬ ИНФОРМАЦИИ – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

ОБЩЕДОСТУПНЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

ОПЕРАТОР (ПЕРСОНАЛЬНЫХ ДАННЫХ) – оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели

обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

ТЕХНИЧЕСКИЕ СРЕДСТВА ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

ПЕРЕХВАТ (ИНФОРМАЦИИ) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

ПОБОЧНЫЕ ЭЛЕКТРОМАГНИТНЫЕ ИЗЛУЧЕНИЯ И НАВОДКИ – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

ПОЛИТИКА «ЧИСТОГО СТОЛА» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

ПОЛЬЗОВАТЕЛЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ – лицо, участвующее в функционировании

информационной системы персональных данных или использующее результаты ее функционирования.

ПРАВИЛА РАЗГРАНИЧЕНИЯ ДОСТУПА – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

ПРОГРАММНАЯ ЗАКЛАДКА – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

ПРЕДОСТАВЛЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

РАСКРЫТИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ – умышленное или случайное нарушение конфиденциальности персональных данных.

РАСПРОСТРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

СПЕЦИАЛЬНЫЕ КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

СУБЪЕКТ ДОСТУПА (СУБЪЕКТ) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

ТЕХНИЧЕСКИЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

УГРОЗЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ – совокупность условий и факторов, создающих опасность 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 при их обработке в информационной системе персональных данных.

УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

УТЕЧКА (ЗАЩИЩАЕМОЙ) ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

УЯЗВИМОСТЬ – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).