УТВЕРЖДАЮ
Директор

_____ **Ж.В. Кравцова**
м.п. «17» сентября 2018 г.

Политика информационной безопасности

Настоящая Политика информационной безопасности (далее – Политика) ***муниципального бюджетного учреждения социального обслуживания «Комплексный центр социального обслуживания населения в Светловском городском округе»*** (далее – Бюджетное 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 1 ноября 2012 г. № 1119 «Требования 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 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, допущенным для работы в информационных системах персональных данных (далее – ИСПДн), степень ответственности данных работников, структура и необходимый уровень защищенности ИСПДн Бюджетного учреждения, статус и обязанности работников, ответственных за обеспечение безопасности персональных данных (далее – ПДн) в ИСПДн Бюджетного учреждения.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Целью настоящей Политики является: обеспечение безопасности объектов защиты Бюджетного учреждения от всех видов угроз (внешних, внутренних, умышленных, непреднамеренных), минимизация ущерба от возможной реализации угроз безопасности персональных данных (далее - УБПДн).

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.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей.

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

Состав объектов защиты утвержден приказами директора Бюджетного учреждения:

- «Об утверждении перечня информационных систем, персональных данных, перечня персональных данных, подлежащих защите, определении контролируемой зоны помещений, назначении ответственных»;
- «Об утверждении комиссий, организационно-распорядительной документации, определении мест хранения материальных носителей персональных данных».

Состав ПДн, подлежащих защите, утвержден приказом директора Бюджетного учреждения:

- «Об утверждении перечня информационных систем, персональных данных, перечня персональных данных, подлежащих защите, определении контролируемой зоны помещений, назначении ответственных».

Настоящая Политика утверждена приказом директора Бюджетного учреждения:

- «Об утверждении комиссий, организационно-распорядительной документации, определении мест хранения материальных носителей персональных данных».

Требования настоящей Политики распространяются на всех работников Бюджетного учреждения, а также всех иных лиц, взаимодействующих с Бюджетным учреждением.

2. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Система защиты персональных данных (далее - СЗПДн) 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;
- Локальных актов (приказов, распоряжений) по Бюджетному учреждению;
- Организационно-распорядительной документации, относящейся к системе защиты информации и персональных данных Бюджетного 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 Бюджетного учреждения.

На основании анализа актуальных угроз безопасности ПДн, описанных в частных моделях угроз безопасности персональных данных, технических заданиях, на разработку системы защиты информационной системы персональных данных, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн Бюджетного учреждения.

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

План мероприятий по обеспечению безопасности персональных данных утверждается приказом директора Бюджетного учреждения:

- «О проведении работ по обеспечению безопасности персональных данных, разработке технической и общей документации, относящейся к системе защиты персональных данных».

Для каждой ИСПДн Бюджетного учреждения 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 Бюджетного 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 КСЗИ соответствующие изменения должны быть внесены в «Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов».

3. ТРЕБОВАНИЯ К ПОДСИСТЕМАМ СЗПДН

СЗПДн включает в себя следующие подсистемы:

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

Подсистемы СЗПДн имеют различный функционал в зависимости от определенных уровней защищенности ИСПДн, определенных в акте определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных Бюджетного учреждения.

4. ПОЛЬЗОВАТЕЛИ ИСПДН

Пользователи – работники Бюджетного учреждения, осуществляющие обработку ПДн.

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

- «Об утверждении списка лиц, имеющих доступ к персональным данным, установление 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 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 ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПДН

Все работники Бюджетного 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 со сборником руководящих инструкций по информационной безопасности Бюджетного учреждения.

Организационно-распорядительная и техническая документация, относящаяся с СЗПДн, утверждается в приказах по Бюджетному учреждению:

- «О проведении работ по обеспечению безопасности персональных данных, разработке технической и общей документации, относящейся к системе защиты персональных данных»;
- «Об утверждении комиссий, организационно-распорядительной документации, определении мест хранения материальных носителей персональных данных».

При вступлении в должность нового работника ответственный за организацию обработки персональных данных и выполнение мероприятий по обеспечению безопасности персональных данных в Бюджетном 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 Бюджетного учреждения под роспись знакомятся с должностными инструкциями, организационно-распорядительной документацией, относящейся к системе защиты ПДн Бюджетного учреждения, настоящей Политикой, принятыми процедурами работы с элементами ИСПДн и СЗПДн, а также с Положением об обработке и защите персональных данных Бюджетного учреждения.

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

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

Все работники Бюджетного 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 Бюджетного 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 работники ознакомлены с правилами защиты АРМ с помощью блокировки *(комбинация Ctrl-Alt-Del, далее Блокировка компьютера; комбинация Клавиша Windows+L).*

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

Работники Бюджетного 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 директора Бюджетного учреждения:

- «О назначении ответственного за организацию обработки персональных данных».

Работники Бюджетного учреждения, допущенные к работам с техническими и криптографическими средствами защиты, обязаны пройти обучение по правилам работы, хранения и учета технических и криптографических средств защиты информации.

Допуск работников со средствами криптографической защиты информации утверждается приказом директора Бюджетного учреждения:

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

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

Работники Бюджетного учреждения, использующие средства криптографической защиты информации, в обязательном порядке обеспечивают их сохранность и не допускают НСД к ним, возможности их утери, использования третьими лицами.

Работники Бюджетного учреждения обязаны без промедления сообщать директору, Ответственному обо всех случаях работы ИСПДн, которые могут повлечь за собой угрозу безопасности ПДн.

Работникам Бюджетного 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 с информационными системами Бюджетного учреждения третьим лицам.

6. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ РАБОТНИКОВ (ПОЛЬЗОВАТЕЛЕЙ) ИСПДН

Должностные обязанности пользователей ИСПДн Бюджетного 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;

- Должностных инструкциях работников Бюджетного учреждения.

7. ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ БЮДЖЕТНОГО УЧРЕЖДЕНИЯ, ОБРАБАТЫВАЮЩИХ ПДН В ИСПДН

Бюджетное учреждение, как Оператор, **ОБЯЗАНО** назначить лицо, ответственное за организацию обработки персональных данных, в соответствии с приказом директора:

- «О назначении ответственного за организацию обработки персональных данных».

Лицо, ответственное за организацию обработки персональных данных в Бюджетном учреждении получает указания непосредственно от директора Бюджетного учреждения и подотчетно ему.

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

- осуществлять внутренний контроль за соблюдением работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников Бюджетного учреждения положения: законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных (приказы, 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 персональных данных и другой конфиденциальной информации, в Бюджетного учреждения созданы комиссии, утвержденные приказом директора:

- «Об утверждении комиссий, организационно-распорядительной документации, определении мест хранения материальных носителей персональных данных».

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.**