ПРИКАЗ

«27» сентября 2019г. № 100 §1

О защите информации, содержащейся в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город» (Сегмент № 085)

В соответствии со статьями 13 и 14 Федерального закона от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» для обеспечения защиты информации, содержащейся в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город» (далее – пользовательский сегмент ГИС «Сетевой город»),

ПРИКАЗЫВАЮ:

1. Организовать мероприятия по защите информации в пользовательском сегменте ГИС «Сетевой город» в соответствии со следующими нормативными правовыми актами:

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119;

– Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены приказом ФСТЭК России № 21 от 18 февраля 2013 года);

– Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утверждены приказом ФСТЭК России № 17 от 11 февраля 2013 года);

– Меры защиты информации в государственных информационных системах (утверждены ФСТЭК России от 11 февраля 2014 года);

– Состав и содержание 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 защищенности (утв. приказом ФСБ России от 10.07.2014 № 378);

– Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (утв. приказом ФСБ России от 09.02.2005 № 66);

– Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (утв. приказом ФАПСИ от 13.06.2001 № 152).

2. Ответственному за организацию обработки персональных данных и администратору безопасности обеспечить построение пользовательского сегмента ГИС «Сетевой город» и системы защиты информации в ней в соответствии с действующим законодательством по защите конфиденциальной информации и персональных данных.

3. В качестве целей и задач системы защиты информации в пользовательском сегменте ГИС «Сетевой город» определить:

– предотвращение нарушения свойств безопасности информации, таких как целостность, доступность и конфиденциальность;

– нейтрализация угроз, определенных как «актуальные» в модели угроз;

– выполнение требований действующего законодательства в сфере защиты конфиденциальной информации и персональных данных.

В качестве этапов работ по созданию системы защиты информации в пользовательском сегменте ГИС «Сетевой город» определить:

– формирование требований к системе защиты информации (определение актуальных угроз безопасности информации, классификация информационной системы, определение требований к системе защиты информации);

– разработка (проектирование) системы защиты информации в пользовательском сегменте ГИС «Сетевой город»;

– внедрение системы защиты информации в пользовательском сегменте ГИС «Сетевой город»;

– аттестация информационной системы по требованиям к защите информации в пользовательском сегменте ГИС «Сетевой город»;

– ввод в действие аттестованной пользовательского сегмента ГИС «Сетевой город».

4. Ответственным за организацию обработки персональных данных в пользовательском сегменте ГИС «Сетевой город» назначить учителя начальных классов МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» А.С. Спорыхину.

5. Ответственному за организацию обработки персональных данных обеспечить автоматизированную обработку персональных данных на объектах

информатизации, удовлетворяющих нормативно-правовым актам, указанными в пункте 1 настоящего Приказа.

6. Ответственному за организацию обработки персональных данных руководствоваться инструкцией ответственного за организацию обработки персональных данных.

7. Ответственному за организацию обработки персональных данных обеспечить неавтоматизированную обработку персональных данных в соответствии с Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.

8. Ответственному за организацию обработки персональных данных обеспечить неограниченный доступ к документу «Политика МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» в отношении обработки персональных данных обрабатываемых в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город», приложение №22 к настоящему Приказу.

9. Администратором безопасности информации в пользовательском сегменте ГИС «Сетевой город» назначить учителя начальных классов Спорыхину А.С.

10. Администратору безопасности в своей работе руководствоваться инструкцией администратора безопасности пользовательского сегмента ГИС «Сетевой город».

11. Администратору безопасности организовать проведение работ по защите информации в соответствии с нормативно-правовыми актами, указанными в пункте 1 настоящего Приказа.

12. Лицам, допущенным к обработке персональных данных при неавтоматизированной их обработке и хранении, руководствоваться документом «Правила обработки персональных данных обрабатываемых в пользовательском сегменте ГИС «Сетевой город» без использования средств автоматизации».

13. Лицам, допущенным к обработке персональных данных при автоматизированной их обработке, руководствоваться следующими документами:

– политика информационной безопасности в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» пользовательского сегмента государственной информационной системы Камчатского края «Сетевой город»;

– инструкция пользователя государственной информационной системы Камчатского края «Сетевой город»;

14. Назначить комиссию по защите информации обрабатываемой в пользовательском сегменте ГИС «Сетевой город» (далее – Комиссия по защите информации) в составе:

– Спорыхина А.С. учитель начальных классов;
– Мирошниченко О.С. учитель информатики;
– Усачев А.А. учитель физкультуры.

15. Комиссии по защите информации в своей работе руководствоваться инструкцией по реагированию на инциденты информационной безопасности, нормативно-правовым актам, указанными в пункте 1 Настоящего приказа и общедоступными источниками об угрозах и уязвимостях информационных систем.

16. Определить контролируемую зону по периметрам помещений (кабинетов), в которых производится обработка защищаемой информации.

17. Схемы помещений и расположение основных технических средств и систем относительно их границ зафиксировать в технических паспортах на информационную систему.

18. Ответственным за хранение и эксплуатацию средств криптографической защиты информации (далее - СКЗИ) в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город» (далее - органом криптографической защиты – ОКЗ) назначить учителя начальных классов Спорыхину А.С.

19. К работе с СКЗИ допускать только пользователей (далее – Пользователи), прошедших предварительное обучение работе с СКЗИ согласно перечню сотрудников МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева», допущенных к работе с СКЗИ в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город».

20. Определить в качестве мест хранения персональных данных приёмную в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева». Ответственным за соблюдение конфиденциальности персональных данных при их хранении назначить секретаря Бахтину В.В..

21. Утвердить следующий перечень документов:

– Инструкция администратора безопасности в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город», приложение №1;

– Инструкция ответственного за организацию обработки персональных данных в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город», приложение №2;

– Инструкция по реагированию на инциденты информационной безопасности в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город», приложение №3;

– Инструкция по обеспечению безопасности эксплуатации СКЗИ в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город», приложение №4;

– Инструкция пользователя пользовательского сегмента государственной информационной системы Камчатского края «Сетевой город», приложение №5;

– Положение о контролируемой зоне пользовательского сегмента государственной информационной системы Камчатского края «Сетевой город», приложение №6;

– Схема организации криптографической защиты конфиденциальной информации для пользовательского сегмента государственной информационной системы Камчатского края «Сетевой город», приложение №7;

– Политика информационной безопасности пользовательского сегмента государственной информационной системы Камчатского края «Сетевой город», приложение №8;

– План мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город», приложение №9;

– Положение о защите и обработке персональных данных в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город», приложение №10;

– Правила рассмотрения запросов субъектов персональных данных или их представителей, чьи персональные данные обрабатываются в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город», приложение №11;

– Политика МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» в отношении обработки персональных данных обрабатываемых в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город», приложение №12;

– Правила обработки персональных данных обрабатываемых в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город» без использования средств автоматизации, приложение №13;

– Перечень персональных данных обрабатываемых в государственной информационной системе Камчатского края «Сетевой город», приложение №14;

– Перечень сотрудников МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева», допущенных к работе с СКЗИ в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город», приложение №15;

– Перечень лиц, допущенных к обработке персональных данных в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город», приложение №16;

– Перечень лиц, допущенных к обработке персональных данных субъектов персональных данных, чьи персональные данные обрабатываются в

пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город» без использования средств автоматизации», приложение №17;

– Форма журнала поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город», приложение №18;

– Форма журнала учета машинных носителей информации, стационарно устанавливаемых в корпус средств вычислительной техники в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город», приложение №19;

– Форма журнала учета приема/выдачи съемных машинных носителей информации в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город», приложение №20;

– Форма журнала учета средств защиты информации в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город», приложение №21;

– Форма журнала проведения инструктажей по информационной безопасности в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город», приложение №22;

– Форма журнала учета мероприятий по контролю обеспечения защиты информации в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город», приложение №23;

– Форма журнала учета обращений граждан-субъектов персональных данных о выполнении их законных прав, приложение №24;

– Форма акта об уничтожении криптографических ключей и ключевых документов для пользовательского сегмента государственной информационной системы Камчатского края «Сетевой город», приложение №25;

– Форма акта об уничтожении документов, содержащих персональные данные, приложение №26.

22. Контроль за исполнением настоящего приказа оставляю за собой.

Директор Е.Ю. Баневич

Приложение №1 к приказу МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» от 27.09.2019 г. № 100 §1

Инструкция администратора безопасности в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Администратор безопасности в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город» (далее – Администратор) назначается приказом директора МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» и отвечает за обеспечение конфиденциальности, целостности и доступности персональных данных (далее – ПДн) в процессе ее обработки в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город» (далее – ГИС «Сетевой город»).

1.2. Администратор обязан поддерживать в актуальном состоянии свои знания законодательных, нормативно-правовых актов Российской Федерации и методических материалов в сфере обработки и защиты ПДн.

1.3. В своей деятельности Администратор руководствуется настоящей Инструкцией, Политикой информационной безопасности и действующим законодательством в сфере защиты персональных данных и конфиденциальной информации.

1.4. Администратор безопасности подчиняется напрямую директору и имеет право требовать от пользователей ГИС «Сетевой город» выполнения указаний и инструкций, связанных с защитой информации.

1.5. Настоящая инструкция разработана с учетом положений следующих законодательных и нормативно-правовых актов:

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

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

– «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;

– «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 года;

– «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;

– методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;

– «Состав и содержание 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 защищенности», утверждённые приказом ФСБ России № 378 от 10.07.2014;

– «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 №152.

2. ФУНКЦИИ И ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ В ГИС «СЕТЕВОЙ ГОРОД»

2.1. Изучение особенностей технологических процессов обработки информации в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» с целью принятия решения о необходимости защиты информации в ГИС «Сетевой город» и классификации ГИС «Сетевой город», либо поиск специализированных организаций, производящих на договорной основе такой анализ. В случае привлечения сторонних организаций, Администратор обязан контролировать процесс сбора информации о ГИС «Сетевой город» сотрудниками сторонней организации. По окончании аналитических работ Администратор обязан ознакомиться с их результатами и подписать отчетные документы, либо составить мотивированный отказ в подписании таких документов и отправить их на доработку сторонней организации.

2.2. Определение актуальных угроз безопасности информации и разработка документа «Модель угроз безопасности ГИС «Сетевой город»», либо привлечение на договорной основе сторонних организаций для таких работ.

2.3. Периодический пересмотр актуальных угроз безопасности согласно с Банком угроз ФСТЭК в следующих случаях:

– ежегодный плановый пересмотр актуальных угроз безопасности информации;

– появление в общедоступных источниках информации о новых угрозах и уязвимостях, имеющих предпосылки в ГИС «Сетевой город»;

– существенное изменение условий функционирования ГИС «Сетевой город», внедрение новых технологий;

– изменение нормативной документации, касающейся моделирования угроз безопасности информации;

– в результате инцидента безопасности.

2.4. Разработка проектной документации на систему защиты информации в ГИС «Сетевой город» (Техническое задание, Технический проект), либо привлечение на договорной основе сторонних организаций для таких работ.

2.5. Участие в реализации проекта по защите информации в ГИС «Сетевой город» (тестирование системы защиты информации, внедрение системы защиты информации, аттестация ГИС «Сетевой город» по требованиям к защите информации, ввод в действие аттестованной ГИС «Сетевой город»).

2.6. Выработка предложений директору МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» по совершенствованию системы защиты информации в ГИС «Сетевой город».

2.7. Ведение учета применяемых в ГИС «Сетевой город» средств защиты информации (в том числе криптосредств), эксплуатационной и технической документации к ним.

2.8. Знание состава, структуры, назначения и выполняемых задач ГИС «Сетевой город», а также состава информационных технологий и технических средств, позволяющих осуществлять обработку ПДн.

2.9. Обеспечение передачи персональных данных через сети связи общего пользования в зашифрованном виде.

2.10. Разработка плана мероприятий по обеспечению безопасности защищаемой информации в ГИС «Сетевой город» и по защите периметра информационной системы. Принятие мер по выполнению мероприятий по обеспечению безопасности защищаемой информации в ГИС «Сетевой город» и непосредственное участие в проведении таких мероприятий. Актуализация плана мероприятий по мере необходимости.

2.11. Осуществление контроля неизменности состояния аттестованной ГИС «Сетевой город» (расположение и состав технических средств, состав программного обеспечения, физическое и логическое строение сети). В случае планирования изменения условий функционирования ГИС «Сетевой город», Администратор должен связаться с аттестующим органом и получить указания к дальнейшим действиям.

2.12. Осуществление контроля физической сохранности и целостности технических средств ГИС «Сетевой город», а также контроль сохранности и целостности опечатывающих пломб на технических средствах ГИС «Сетевой город» (в том числе и программно-аппаратных средствах защиты информации). Контроль неизменности состава технических средств в ГИС «Сетевой город».

2.13. Организация учета съемных носителей информации. Настройка соответствующих программных механизмов средств защиты информации для запрета неучтенных съемных носителей. Ведение журнала учета съемных носителей.

2.14. Организация учета иных машинных носителей информации.

2.15. Проведение инструктажей сотрудников, работающих с защищаемой информацией в ГИС «Сетевой город» (далее – Пользователи ГИС «Сетевой город»), по темам: правила работы в ГИС «Сетевой город», защита информации в ГИС «Сетевой город», положения законодательства в сфере защиты информации и персональных данных, новые угрозы в сфере защиты информации. Повышение осведомленности всех сотрудников МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» в вопросах информационной безопасности.

2.16. Организация первоначального доступа пользователям ГИС «Сетевой город» к ресурсам информационной системы в соответствии с утвержденным положением о разграничении прав доступа в ГИС «Сетевой город». Блокировка учетных записей, изменение полномочий пользователей и добавление новых пользователей ГИС «Сетевой город» в соответствии с Инструкцией о внесении изменений в списки пользователей и наделению их полномочиями доступа к ресурсам ГИС «Сетевой город».

2.17. Периодическое тестирование функций системы защиты от НСД согласно плану мероприятий по обеспечению безопасности информации, либо при изменении программной среды или полномочий Пользователей ГИС «Сетевой город».

2.18. Участие в составе комиссии по защите информации обрабатываемой в ГИС «Сетевой город» в расследованиях причин инцидентов безопасности, внесение по результатам таких расследований предложений по совершенствованию системы безопасности. По мере возможности, Администратор должен восстанавливать ущерб, нанесенный информационной системе во время инцидента безопасности, а также восстанавливать ПДн и конфиденциальную информацию, модифицированную или уничтоженную в результате такого инцидента.

2.19. Контроль выполнения Пользователями ГИС «Сетевой город» требований Инструкции пользователя ГИС «Сетевой город», а также других установленных требований для обеспечения безопасности ПДн.

2.20. В случае получения от Пользователей ГИС «Сетевой город» информации о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа,

Администратор незамедлительно принимает все необходимые меры для обеспечения безопасности ПДн и иной конфиденциальной информации в пределах своих полномочий.

2.21. Обеспечение отсутствия на АРМ Пользователей ГИС «Сетевой город» средств разработки и отладки программного обеспечения. Контроль за отключением на АРМ Пользователей и невозможностью самостоятельного включения пользователем технологий мобильного кода (JavaScript, Adobe Flash, макросы MS Office и т. д.), кроме случаев, когда использование таких технологий необходимо для выполнения служебных (должностных) обязанностей.

2.22. Контроль обновлений системного, прикладного программного обеспечения и средств защиты информации (в том числе обновлений антивирусных баз, сигнатур сценариев вторжений, информации об уязвимостях).

2.23. Контроль сотрудников сторонних организаций, производящих ремонт/обслуживание технических средств ГИС «Сетевой город» или настройку/установку программного обеспечения ГИС «Сетевой город».

2.24. Обеспечение функционирования и поддержания работоспособности в ГИС «Сетевой город»:

– системы защиты информации от несанкционированного доступа;

– системы межсетевого экранирования;

– системы криптографической защиты информации;

– системы антивирусной защиты.

2.25. Обеспечение непрерывности процессов в ГИС «Сетевой город». В случае нарушения работоспособности технических средств и программного обеспечения ГИС «Сетевой город», в том числе средств защиты ГИС «Сетевой город», Администратор принимает меры по их своевременному восстановлению и выявлению причин, приведших к нарушению работоспособности.

2.26. Своевременное информирование Ответственного за организацию обработки ПДн о выявленных нарушениях требований по обеспечению безопасности ПДн и попытках несанкционированного доступа к ГИС «Сетевой город».

3. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ГИС «СЕТЕВОЙ ГОРОД»

Администратор имеет право:

3.1. Знакомиться с нормативными актами МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева», регламентирующими процессы обработки и защиты ПДн и иной конфиденциальной информации.

3.2. Вносить предложения директору МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» по совершенствованию существующей системы защиты информации.

3.3. Требовать от Пользователей ГИС «Сетевой город» соблюдения требований Инструкции пользователя ГИС «Сетевой город» и иных нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности ПДн и иной конфиденциальной информации.

3.4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности ПДн и иной конфиденциальной информации.

3.5. Требовать прекращения работы в ГИС «Сетевой город», как в целом, так и отдельных Пользователей ГИС «Сетевой город», в случае выявления нарушений требований по обеспечению безопасности ПДн или в связи с нарушением функционирования ГИС «Сетевой город».

3.6. Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности ПДн к Ответственному за организацию обработки ПДн.

4. НАСТРОЙКА И ОБСЛУЖИВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

4.1. Администратору информационной безопасности до идентификации и аутентификации разрешаются следующие действия с целью диагностики проблем на элементах ГИС «Сетевой город» и восстановления работоспособности элементов ГИС «Сетевой город»:

– загрузка операционной системы в безопасном режиме;

– восстановление операционной системы с последней работоспособной конфигурацией;

– изменение параметров BIOS/UEFI;

– загрузка с внешнего носителя с целью восстановления или переустановки операционной системы, восстановления работоспособности средств защиты информации, сканирования жесткого диска на вирусы, сканирования оперативной памяти или жесткого диска с целью выявления проблем и других действий восстановительного или диагностического характера.

4.2. При первичной настройке сетевого оборудования, Администратор изменяет все пароли по умолчанию, установленные производителем сетевого оборудования.

4.3. Общие правила работы с криптосредствами описаны в утвержденной Инструкции по обеспечению безопасности эксплуатации средств криптографической защиты информации (далее - СКЗИ). В данном разделе описана часть, касающаяся функций и обязанностей Администратора.

4.4. Администратор обеспечивает соответствие работы с СКЗИ технической и эксплуатационной документации к ним.

4.5. Администратор в составе комиссии по уничтожению принимает участие в уничтожении ключевой информации и ключевых документов. Уничтожение ключевой информации производится путем физического уничтожения ключевого носителя или путем гарантированного затирания ключевой информации.

4.6. Администратор осуществляет проверку функционирования средства антивирусной защиты (обновление антивирусных баз, наличие периодического сканирования). Обновление антивирусных баз и сигнатур проводится ежедневно, в случае несоответствия Администратор обращаться в краевое государственное автономное учреждение «Камчатский центр информатизации и оценки качества образования».

4.7. Администратор самостоятельно или в составе комиссии по защите информации обрабатываемой в ГИС «Сетевой город» (в случае значительного инцидента безопасности) реагирует на сообщения системы антивирусной защиты или пользователей об обнаружении вредоносных компьютерных программ (вирусов), или на подозрение наличия таковых, и принимает меры по нейтрализации обнаруженных угроз, связываясь с краевым государственным автономным учреждением «Камчатский центр информатизации и оценки качества образования».

4.8. Сканирование ГИС «Сетевой город» на наличие уязвимостей проводится краевым государственным автономным учреждением «Камчатский центр информатизации и оценки качества образования».

4.9. Администратор принимает меры по устранению или нейтрализации выявленных уязвимостей, если краевое государственное автономное учреждение «Камчатский центр информатизации и оценки качества образования», оповестила МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» о имеющихся уязвимостях в ГИС «Сетевой город». В первую очередь обрабатываются уязвимости с наивысшим баллом по шкале CVSS. В случае необходимости, до устранения уязвимости могут быть локализованы (отключены от общей сети) сегменты или отдельные автоматизированные рабочие места информационной системы.

4.10. С целью оперативного устранения известных уязвимостей информационной системы настраивается обновление в автоматическом режиме компонентов операционных систем, прикладного программного обеспечения и средств защиты информации.

4.11. Администратор не реже чем один раз в месяц осуществляет контроль состава технических средств, программного обеспечения и средств защиты информации, а также корректности функционирования и настроек программного обеспечения и средств защиты информации.

4.12. Программное обеспечение и средства защиты информации в случае нарушения целостности или работоспособности восстанавливаются с эталонных дистрибутивов, поставляемых в комплекте с документацией. Эталонные

дистрибутивы хранятся в сейфе у Администратора или в краевом государственном автономном учреждении «Камчатский центр информатизации и оценки качества образования».

4.1. Резервирование основных технических средств и систем (далее – ОТСС) обеспечивается подключения к этим средствам источников бесперебойного питания и путем замещения, вышедшего из строя ОТСС на резервное устройство Администратором вручную.

4.2. Администратор присутствует в процессе установки, обновления, настройки программного обеспечения в ГИС «Сетевой город» (в том числе и средств защиты информации) сотрудниками сторонних организаций.

4.3. Администратор присутствует в процессе ремонта технических средств ГИС «Сетевой город» сотрудниками сторонних организаций на территории МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева». Администратор обеспечивает гарантированное затирание данных с носителей информации, либо демонтаж носителей информации (в том числе и оперативной памяти) с технических средств в случае необходимости отправки технических средств для ремонта на территорию сторонних организаций.

4.4. Администратор обеспечивает гарантированное затирание данных на машинных носителях информации при утилизации технических средств, либо принимает участие в физическом уничтожении машинных носителей информации в составе комиссии по уничтожению.

4.5. По результатам уничтожения составляется Акт уничтожения информации с машинных носителей информации. Копия акта направляется в КГАУ «Камчатский центр информатизации и оценки качества образования».

Приложение №2 к приказу МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» от 27.09.2019 г. № 100 §1

Инструкция ответственного за организацию обработки персональных данных в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Ответственный за организацию обработки персональных данных в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» (далее – Ответственный) назначается приказом директора МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» (далее – Учреждение) и отвечает за организацию, обеспечение своевременного и квалифицированного выполнения сотрудниками Учреждения законодательства Российской Федерации о персональных данных (далее – ПДн), в том числе требований к обработке и защите ПДн в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город» (далее – ГИС «Сетевой город»).

1.2. Ответственный должен знать законодательные и иные нормативные правовые акты Российской Федерации, методические материалы в сфере обработки и защиты ПДн обрабатываемых в ГИС «Сетевой город». Ответственный поддерживает в актуальном состоянии свои знания в сфере действующего законодательства и законодательных инициатив, связанных с защитой персональных данных.

1.3. В своей деятельности Ответственный руководствуется Положением об обработке и защите персональных данных, настоящей Инструкцией и действующим законодательством в сфере защиты персональных данных и конфиденциальной информации.

2. ОСНОВНЫЕ ФУНКЦИИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Ответственный изучает все стороны деятельности Учреждения и вырабатывает рекомендации по организации обработки ПДн в ГИС «Сетевой город» при решении следующих основных вопросов:

– организация доступа к ПДн и учет сотрудников Учреждения, допущенных к обработке ПДн в ГИС «Сетевой город», как хранимых на бумажных носителях, так и в программных комплексах, входящих в состав ГИС «Сетевой город»;

– контроль за поддержанием в актуальном состоянии действующих локальных нормативных актов, журналов и форм учета по работе с ПДн;

– контроль за обеспечением соответствия проводимых работ в части обработки ПДн в ГИС «Сетевой город» технике безопасности, правилам и нормам охраны труда;

– организация работы совместно Администратором по заключению договоров на работы по защите ПДн;

– контроль изменений в процессах обработки ПДн в ГИС «Сетевой город» и, в случае необходимости, отправка информации об этих изменениях в уполномоченный территориальный орган по защите прав субъектов персональных данных (Роскомнадзор) с целью актуализации уведомления МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» в реестре операторов ПДн;

– рассмотрение предложений по совершенствованию действующей системы защиты ПДн обрабатываемых в ГИС «Сетевой город», предоставленных Администратором, назначаемым приказом руководителя МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»;

– осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами Учреждения.

3. ОСНОВНЫЕ ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Знать цели обработки ПДн в ГИС «Сетевой город» и перечень обрабатываемых ПДн.

3.2. Соблюдать требования нормативных актов Учреждения, устанавливающих порядок работы с ПДн обрабатываемых в ГИС «Сетевой город».

3.3. Обеспечивать доведение до сведения сотрудников Учреждения законодательства Российской Федерации о ПДн, нормативных актов по вопросам обработки ПДн, требований к защите ПДн.

3.4. Осуществлять внутренний контроль за соблюдением сотрудниками Учреждения законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн.

3.5. Обеспечивать доработку локальных нормативных документов по защите ПДн обрабатываемых в ГИС «Сетевой город» в случае такой необходимости или при поступлении такого требования от регулирующего органа.

3.6. Участвовать в расследовании нарушений по вопросам защиты ПДн обрабатываемых в ГИС «Сетевой город», имевших место, разрабатывать

предложения по устранению недостатков и предупреждению подобного рода нарушений.

3.7. Обеспечивать организацию проведения занятий со специалистами Учреждения по организационным вопросам обработки ПДн в ГИС «Сетевой город» (проводить инструктаж сотрудников, осуществляющих обработку ПДн в ГИС «Сетевой город» и имеющих доступ к ПДн обрабатываемых в ГИС «Сетевой город»).

3.8. Обеспечивать организацию приема и обработки обращений и запросов субъектов ПДн или их представителей по вопросам обработки ПДн в ГИС «Сетевой город» и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов согласно п.3 ч.4 ст.22.1 Федерального закона от 27.07.06 № 152-ФЗ «О персональных данных».

4. ПРАВА ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Знакомиться с документами и материалами, необходимыми для выполнения возложенных на него задач.

4.2. Проводить проверки соблюдения режима обеспечения безопасности ПДн в структурных и (или) территориальных подразделениях Учреждения (при их наличии) в соответствии с утвержденным приказом руководителя Учреждения планом мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации в пользовательском сегменте ГИС «Сетевой город».

4.3. Требовать от сотрудников Учреждения соблюдения требований нормативно-правовых и организационно-распорядительных документов по вопросам обработки ПДн в ГИС «Сетевой город».

4.4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обработки ПДн в ГИС «Сетевой город».

4.5. Требовать от сотрудников Учреждения письменных объяснений при проведении служебных расследований по вопросам нарушений требований по обработке и защите ПДн обрабатываемых в ГИС «Сетевой город».

4.6. Вносить предложения руководителю Учреждения об отстранении от выполнения служебных обязанностей сотрудников, систематически нарушающих требования по обработке и защите ПДн обрабатываемых в ГИС «Сетевой город».

4.7. Давать сотрудникам Учреждения обязательные для выполнения указания по обработке и защите ПДн, определяемые законодательством Российской Федерации и локальными нормативными актами Учреждения.

4.8. Привлекать в установленном порядке специалистов Учреждения, имеющих непосредственное отношение к рассматриваемым проблемам, для более детального изучения отдельных вопросов, возникающих в процессе работы.

Приложение №3 к приказу МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» от 27.09.2019 г. № 100 §1

Инструкция по реагированию на инциденты информационной безопасности в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политики информационной безопасности и меры по защите информации в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город» (далее – ГИС «Сетевой город») не могут полностью гарантировать защиту информации, информационных систем, сервисов или сетей. Всегда существует вероятность, что после внедрения системы защиты информации останутся слабые места, которые могут сделать обеспечение информационной безопасности неэффективным, и, следовательно, инциденты информационной безопасности – возможными. Инциденты информационной безопасности могут оказывать прямое или косвенное негативное воздействие на деятельность МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева». Также неизбежно выявление новых, ранее не идентифицированных угроз безопасности информации. Исходя из вышесказанного, важно применять структурный подход к:

– обнаружению, оповещению об инцидентах безопасности и их оценке;

– реагированию на инциденты информационной безопасности, включая активизацию соответствующих защитных мер для предотвращения, уменьшения последствий и (или) восстановления после наступления негативных последствий вследствие инцидента безопасности информации;

– извлечению уроков из инцидентов информационной безопасности, совершенствованию системы защиты информации, введению превентивных защитных мер и улучшению общего подхода к менеджменту инцидентов информационной безопасности.

1.2. Регистрация событий безопасности, выявление инцидентов безопасности информации и реагирование на них производится, в том числе, с целью выполнения требований Приказа ФСТЭК № 17 от 11.02.2013 с индексами: РСБ.1, РСБ.2, РСБ.3, РСБ.4, РСБ.5, РСБ.6, РСБ.7.

1.3. Для реагирования на инциденты информационной безопасности создается комиссия по защите информации обрабатываемой в ГИС «Сетевой город» (далее – Комиссия).

1.4. Важным членом Комиссии является Администратор безопасности информации (далее – Администратор), назначаемый приказом директора МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева». Он осуществляет мониторинг событий безопасности в соответствии с Инструкцией администратора безопасности.

1.5. Инцидентом информационной безопасности (далее – инцидент ИБ) является событие, нарушающее одно из свойств защищаемой информации (целостность, доступность или конфиденциальность) или несколько таких свойств одновременно.

2. РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ В ГИС «СЕТЕВОЙ ГОРОД»

2.1. Событиями безопасности, подлежащими регистрации, являются записи в журналах операционных систем, прикладного программного обеспечения и средств защиты информации (электронные журналы сообщений). К событиям безопасности относятся следующие виды записей в таких системных журналах:

– записи о входе пользователя в операционную систему или прикладное программное обеспечение;

– записи о неудачных попытках аутентификации пользователя в системе (время, количество попыток, время блокировки учетной записи);

– записи о времени окончания сеанса работы пользователя в операционной системе или в прикладном программном обеспечении;

– записи о доступе к легальной для данного пользователя защищаемой информации;

– записи о попытках доступа к запрещенной для данного пользователя защищаемой информации;

– записи об использовании разрешенных съемных носителей информации и мобильных устройств (время включения, копируемая информация, время отключения и т. д.);

– записи о попытках использования запрещенных в системе съемных носителей информации и мобильных устройств;

– записи о попытках повышения собственных полномочий в системе;

– записи об аномальной сетевой активности;

– записи о попытках доступа к управлению разграничением доступа к информации и к управлению средствами защиты информации;

– записи об обнаружениях вирусов, червей, троянов антивирусными средствами;

– записи о попытках установки запрещенного прикладного программного обеспечения;

– записи о запуске подозрительных файлов, полученных по электронной почте или по другим каналам;

– записи о нарушении правил и политик информационной безопасности;

– записи о передаче защищаемой информации по каналам связи.

2.2. Информация о событиях безопасности информации является защищаемой информацией и к ней применяются те же, утвержденные правила и политики по защите информации, что и к другой защищаемой конфиденциальной информации в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева».

2.3. Далеко не все события безопасности информации являются инцидентами безопасности информации. Инцидентами безопасности являются только запрещенные в ГИС «Сетевой город» действия, с которыми может быть связано создание угрозы информационной безопасности.

2.4. Информация о событиях безопасности также может поступать Администратору безопасности от сотрудников МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева», заметивших аномальную активность в информационной системе. Информацией о событиях безопасности также являются сведения о потере, краже или компрометации машинных и других носителей информации.

2.5. Администратор анализирует электронные журналы сообщений и принимает решение, является ли событие безопасности инцидентом информационной безопасности.

2.6. По степени возможного ущерба информационной системы инциденты информационной безопасности можно условно разделить на незначительные и значительные.

2.7. Незначительными признаются инциденты информационной безопасности, соответствующие одному или нескольким критериям:

– инцидент был быстро обнаружен и локализован, значительных последствий в результате инцидента не произошло;

– инцидент затронул небольшое количество сотрудников МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»;

– инцидент не требует существенных усилий и затрат на восстановление работоспособности информационной системы или ее частей;

– в результате инцидента не была нарушена конфиденциальность, целостность и доступность больших массивов защищаемой информации (например, всей базы

данных), нарушена безопасность только небольшого фрагмента информации (одной или нескольких записей базы данных);

– инцидент не требует концептуального пересмотра политик информационной безопасности в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»;

– в результате инцидента организации нанесен минимальный ущерб или не нанесено никакого ущерба;

– инцидент не вызвал долгосрочного простоя информационной системы и не нарушил бизнес-процессы и технологические процессы обработки информации.

2.8. Значительными признаются все инциденты информационной безопасности, которые не могут быть признаны незначительным в соответствии с пунктом 2.7 данной Инструкции.

3. РЕАГИРОВАНИЕ НА ИНЦИДЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УСТРАНЕНИЕ ПОСЛЕДСТВИЙ И ПРИЧИН ИНЦИДЕНТА

3.1. В случае обнаружения незначительных инцидентов, Администратор самостоятельно принимает меры по устранению последствий инцидента информационной безопасности.

3.2. В случае обнаружения значительных инцидентов, Администратор созывает Комиссию, которая оценивает инцидент и реагирует на него наиболее целесообразным и результативным способом.

3.3. После устранения последствий инцидента, Комиссией делаются соответствующие выводы (оформляемые в виде акта) и вносятся предложения по совершенствованию технических и организационных аспектов защиты информации в ГИС «Сетевой город» с целью предотвращения подобных инцидентов в будущем.

3.4. Процесс реагирования на инцидент информационной безопасности и восстановление ущерба, нанесенного ГИС «Сетевой город», может состоять из следующих этапов:

– обнаружение и оповещение о возникновении событий ИБ (человеком или автоматическими средствами);

– сбор информации, связанной с событиями информационной безопасности и оценка этой информации с целью определения, какие события можно отнести к категории инцидентов ИБ;

– незамедлительное реагирование на инцидент ИБ;

– локализация АРМ или сегмента сети, на который распространились негативные последствия инцидента;

– при необходимости - привлечение специалистов сторонних организаций для получения качественных консультаций;

– выполнение мер по нейтрализации факторов, вызвавших инцидент ИБ;

– восстановление ущерба, вызванного инцидентом ИБ;

– регистрация всех действий и решений для последующего анализа;

– правовая оценка инцидента ИБ;

– при необходимости и при наличии правовых оснований, обращение в правоохранительные органы;

– принятия мер для предотвращения подобных инцидентов в будущем.

4. РАССЛЕДОВАНИЕ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Расследование инцидента информационной безопасности проводится с целью выявления и наказания лиц, виновных в инциденте, а также с целью выявления недоработок в политиках информационной безопасности и их оперативного устранения.

4.2. Расследование инцидента проводится Администратором безопасности самостоятельно (в случае незначительного инцидента) либо Комиссия (в случае значительного инцидента). В случаях, когда виновником инцидента является внешний нарушитель, к расследованию инцидента могут привлекаться сотрудники правоохранительных органов в установленном порядке.

4.3. Расследование инцидента проводится в следующем порядке:

– проводится сбор информации об инциденте из всех возможных источников, проводится анализ собранной информации, формируется доказательная база;

– анализируются каналы атаки, уязвимости и другие факторы, которые сделали возможным появление инцидента информационной безопасности;

– анализируются сценарии действий нарушителя, в случае антропогенной природы инцидента;

– составляется список подозреваемых в инциденте лиц, в случае антропогенной природы инцидента;

– выявляются лица, виновные в инциденте информационной безопасности, в случае антропогенной природы инцидента;

– определяется степень ущерба, нанесенная информационной системе, организации, субъектам персональных данных в результате инцидента информационной безопасности;

– составляется отчет о расследовании.

4.4. В случаях, если инцидент произошел по вине сотрудников МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева», руководство принимает решение о мерах, которые будут применены к виновному лицу.

4.5. В случаях, если инцидент произошел по вине контрагента или сотрудника сторонней организации, осуществляющей какие-либо работы в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева», виновный в инциденте несет ответственность в соответствии с положениями договора между МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» и контрагентом/сторонней организацией.

4.6. В случаях, если инцидент произошел по вине внешнего нарушителя, виновный несет ответственность в соответствии с уголовным и административным кодексами Российской Федерации.

4.7. После выявления и наказания виновных в инциденте, Администратором безопасности, после согласования с руководством МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева», могут быть проведены занятия с сотрудниками МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» по разбору произошедшего инцидента с целью предотвращения повторения инцидента в будущем.

4.8. Из каждого инцидента информационной безопасности извлекаются уроки, делаются выводы о необходимости изменения и улучшения организационных и технических частей системы защиты информации в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева». Изменения в системе защиты информации, призванные предотвратить появление выявленного и расследованного инцидента информационной безопасности, должны быть осуществлены в кратчайшие сроки.

5. КЛАССИФИКАЦИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Инциденты ИБ по происхождению делятся на преднамеренные и случайные. Случайные инциденты могут быть вызваны антропогенными факторами (ошибка сотрудника, техническая неграмотность), социальными явлениями, природными явлениями, техногенными факторами (аварии, катастрофы).

5.2. Инциденты ИБ также можно разделить на инциденты, вызванные техническими средствами, и инциденты, вызванные нетехническими средствами.

5.3. В целом все инциденты безопасности можно разделить на следующие категории:

– вирусная атака (заражение элементов информационной системы вирусами, троянами, бэкдорами и прочим вредоносным программным обеспечением);

– попытки несанкционированного доступа к защищаемой информации;

– отказ в обслуживании (в результате программного или аппаратного сбоя, либо в результате целенаправленной или веерной атаки);

– нарушение сотрудниками МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» предписаний внутренних руководящих документов по защите информации (политик, инструкций, регламентов);

– нарушение технологического процесса обработки и защиты информации в информационной системе;

– потеря, утрата, компрометация машинных и иных носителей информации;

– нарушение конфиденциальности защищаемой информации;

– нарушение целостности защищаемой информации;

– сетевые атаки на информационную систему (как из-за пределов защищаемого периметра, так и внутри него);

– техногенная авария;

– нештатная ситуация.

5.4. Более подробное описание угроз безопасности ГИС «Сетевой город», а, следовательно, и возможности для возникновения инцидентов ИБ приведено в документе «Модель угроз безопасности информации в ГИС «Сетевой город».

Приложение №4 к приказу МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» от 27.09.2019 г. № 100 §1

Инструкция по обеспечению безопасности эксплуатации СКЗИ в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет порядок учета, хранения и использования СКЗИ, криптографических ключей и ключевых документов, а также порядок изготовления, смены, уничтожения и компрометации криптографических ключей в целях обеспечения безопасности эксплуатации СКЗИ в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город» (далее – ГИС «Сетевой город»).

1.2. Настоящая Инструкция разработана в соответствии со следующими нормативными правовыми актами Российской Федерации:

– Состав и содержание 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 защищенности (утв. приказом ФСБ России от 10.07.2014 № 378);

– Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (утв. приказом ФСБ России от 09.02.2005 № 66);

– Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (утв. приказом ФАПСИ от 13.06.2001 № 152).

1.3. В МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» используются только сертифицированные ФСБ России СКЗИ, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну.

1.4. В МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» приказом директора МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» назначается ответственный за

хранение и эксплуатацию СКЗИ, именуемый также органом криптографической защиты информации (далее – ОКЗ).

1.5. Подписывая лист ознакомления с настоящей Инструкцией, ОКЗ подтверждает, что также ознакомлен с Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (утв. приказом ФАПСИ от 13.06.2001 № 152).

1.6. ОКЗ осуществляет:

– учет пользователей СКЗИ (далее – Пользователи) и представление на утверждение директору МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» списка пользователей СКЗИ;

– контроль за соблюдением условий использования СКЗИ;

– расследования и составление заключений по фактам нарушений условий использования СКЗИ;

– разработку и обеспечение мер по предотвращению возможных нежелательных последствий таких нарушений;

– инструктаж Пользователей правилам работы с СКЗИ и правилам хранения СКЗИ, ключевых носителей и ключевых документов. Отметка о проведении инструктажа проставляется в Журнале учета инструктажей по информационной безопасности в ГИС «Сетевой город»;

– расследование случаев попыток посторонних лиц получить сведения об используемых СКЗИ, случаев компрометации или при подозрении на компрометацию ключевой информации, случаев утраты дистрибутивов СКЗИ (при их наличии), ключевой информации, ключевых носителей, технической и эксплуатационной документации к СКЗИ (при ее наличии), ключей от помещений и хранилищ СКЗИ. В случае компрометации ключевой информации, Администратор инициирует вывод из эксплуатации ключевой информации, связываясь с краевом государственным автономным учреждением «Камчатский центр информатизации и оценки качества образования».

1.7. Список Пользователей утверждается приказом директора МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева».

1.8. Пользователь обязан:

– не разглашать конфиденциальную информацию, к которой он допущен, в том числе: сведения об СКЗИ, ключевых документах к ним и других мерах защиты;

– соблюдать требования по обеспечению безопасности конфиденциальной информации при использовании СКЗИ;

– хранить ключевую информацию в сейфах и помещениях, гарантирующую ее сохранность и конфиденциальность;

– сообщать ОКЗ о попытках посторонних лиц получить сведения об СКЗИ или ключевых документах к ним;

– незамедлительно уведомлять ОКЗ о фактах утраты или недостачи СКЗИ, криптографических ключей, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений;

– сдать СКЗИ, эксплуатационную и техническую документацию к ним, криптографические ключи ОКЗ, в соответствии с порядком, установленным настоящей Инструкцией, при прекращении использования СКЗИ (увольнении, перевода на другую должность и в иных подобных случаях).

1.9. К работе с СКЗИ Пользователи допускаются только после соответствующего инструктажа.

2. УЧЕТ СКЗИ, ХРАНЕНИЕ И ПЕРЕДАЧА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

2.1. СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы и ключевые носители подлежат поэкземплярному учету. Программные СКЗИ учитываются совместно с аппаратными средствами, на которых осуществляется их штатная эксплуатация. Учет осуществляется ОКЗ в Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал).

2.2. Единицей поэкземплярного учета ключевых документов считается отчуждаемый носитель с записанными криптографическими ключами. Если один и тот же носитель используется для записи другого криптографического ключа, его необходимо зарегистрировать снова.

2.3. Все полученные экземпляры СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы выдаются Пользователям под роспись в Журнале. Пользователи несут персональную ответственность за сохранность СКЗИ и ключевых документов.

2.4. Ключевые носители с криптографическими ключами хранятся у ОКЗ.

2.5. Хранение осуществляется в ящиках, шкафах, сейфах (хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

2.6. Ключевые носители с неработоспособными криптографическими ключами ОКЗ принимает от Пользователя и делает соответствующую запись в Журнале. Неработоспособные ключевые носители подлежат уничтожению.

2.7. Аппаратные средства, с которыми осуществляется штатное использование СКЗИ, а также аппаратные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ и аппаратных средств должно быть визуально контролируемым.

3. ИСПОЛЬЗОВАНИЕ СКЗИ

3.1. В МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» СКЗИ используется с целью обеспечения конфиденциальности и целостности электронных документов и сетевого трафика.

3.2. Для шифрования электронного документа и/или сетевого трафика Пользователь использует свой собственный закрытый криптографический ключ и открытый криптографический ключ.

3.3. В МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» используются только те СКЗИ, которые реализуют стойкие криптографические алгоритмы, не позволяющие в разумные сроки вычислить закрытый ключ по открытому ключу.

3.4. Пользователь ежедневно проверяет сохранность технических средств и целостность печатей и пломб на них.

3.5. В случае обнаружения неразрешенного программного обеспечения или факта повреждения целостности печати (пломбы) на техническом средстве с СКЗИ, работа с СКЗИ на таком техническом средстве должна быть прекращена. По данному факту созывается комиссия по защите информации обрабатываемой в ГИС «Сетевой город» (далее – Комиссия), которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

3.6. Вскрытие технического средства с СКЗИ для проведения ремонта или технического обслуживания осуществляется только в присутствии ОКЗ.

3.7. При работе с СКЗИ запрещается:

– оставлять без присмотра (контроля) технические средства, на которых эксплуатируется СКЗИ;

– самостоятельно вносить изменения в программную часть СКЗИ;

– разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и другие средства вывода информации;

– использовать ключевые носители в режимах, не предусмотренных штатными функциями СКЗИ;

– осуществлять несанкционированное копирование криптографических ключей;

– изменять настройки или пытаться изменить настройки СКЗИ или операционной системы, сделанные ОКЗ;

– использовать бывшие в работе ключевые носители для записи новой информации без предварительного гарантированного уничтожения на них ключевой информации;

– осуществлять самостоятельное несанкционированное вскрытие технических средств с СКЗИ.

3.8. С целью обеспечения непрерывности работы МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» плановая замена ключевой информации должна производиться заблаговременно.

4. ДЕЙСТВИЯ ПРИ КОМПРОМЕТАЦИИ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

4.1. Криптографические ключи считаются скомпрометированными в следующих случаях:

– потеря ключевых носителей (в том числе с последующим обнаружением);

– увольнение сотрудников, имевших доступ к ключевым носителям;

– возникновение подозрений на утечку информации или ее искажение в информационной системе;

– нарушение печати на хранилище с ключевыми носителями ли на техническом средстве с СКЗИ;

– временный бесконтрольный доступ посторонних лиц к ключевым носителям или техническим средствам с СКЗИ;

– иные случаи подозрения компрометации криптографических ключей.

4.2. В случае подозрения в компрометации криптографических ключей, Пользователь должен немедленно прекратить эксплуатацию СКЗИ и продолжить ее только после замены криптографических ключей.

4.3. Скомпрометированные криптографические ключи подлежат уничтожению.

5. УНИЧТОЖЕНИЕ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

5.1. Неиспользованные или выведенные из действия криптографические ключи подлежат уничтожению.

5.2. Уничтожение криптографических ключей на ключевых носителях производятся комиссией в составе председателя и членов комиссии, назначенной директором МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева».

5.3. Криптографические ключи, записанные на машинные ключевые носители, уничтожаются методом гарантированного стирания информации на машинном носителе в соответствии с требованиями эксплуатационной и технической документации на СКЗИ.

5.4. Криптографические ключи, записанные на бумажных носителях, уничтожаются физически (сжигание, измельчение и т. д.).

5.5. Перед уничтожением криптографических ключей и/или ключевых носителей, комиссия обязана:

– установить наличие оригинала и количество копий криптографических ключей;

– проверить внешнюю целостность каждого ключевого носителя;

– идентифицировать каждый ключевой носитель в соответствии с Журналом поэкземплярного учета средств криптографической защиты информации;

– убедиться, что криптографические ключи, находящиеся на ключевых носителях, действительно подлежат уничтожению;

– произвести уничтожение криптографических ключей на оригинале и всех копиях ключевого носителя.

5.6. По факту уничтожения криптографических ключей составляется Акт уничтожения .

5.7. Акт подписывается председателем и членами комиссии по уничтожению.

5.8. В Журнале поэкземплярного учета средств криптографической защиты информации делается отметка об уничтожении криптографических ключей.

5.9. Акты уничтожения криптографических ключей хранятся у ОКЗ.

6. ТРЕБОВАНИЯ К ПОМЕЩЕНИЯМ, В КОТОРЫХ ВЕДЕТСЯ РАБОТА С СКЗИ И/ИЛИ ХРАНЯТСЯ КРИПТОГРАФИЧЕСКИЕ КЛЮЧИ

6.1. Размещение, специально оборудование, охрана и организация режима в помещениях, где установлены СКЗИ и/или хранятся криптографические ключи (далее – спецпомещения), должны обеспечивать сохранность СКЗИ и криптографических ключей.

6.2. При оборудовании спецпомещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

6.3. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежную защиту от проникновения посторонних лиц в нерабочее

время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение посторонних лиц, необходимо оборудовать средствами, препятствующими неконтролируемому проникновению в спецпомещения. При этом, применение нераспахиваемых железных решеток на окнах запрещено, поскольку это противоречит правилам пожарной безопасности.

6.4. Мониторы рабочих станций с СКЗИ должны быть повернуты задней стороной к дверям и окнам, либо должны применяться шторы, рольставни, жалюзи или другие средства для пресечения несанкционированного просмотра содержимого, отображаемого на мониторах.

6.5. Для хранения криптографических ключей, эксплуатационной и технической документации, дистрибутивов СКЗИ выделяется необходимое число надежных металлических хранилищ. Ключи от хранилищ хранятся у ОКЗ и у Пользователей.

6.6. По окончании рабочего дня спецпомещения и установленные в них хранилища должны быть закрыты на замок.

6.7. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в спецпомещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ОКЗ. ОКЗ должен оценить вероятность компрометации хранящихся криптографических ключей, составить акт и принять, при необходимости, меры к локализации последствия компрометации криптографических ключей и к их замене.

Приложение №5 к приказу МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» от 27.09.2019 г. № 100 §1

Инструкция пользователя пользовательского сегмента государственной информационной системы Камчатского края «Сетевой город»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. С целью автоматизации процессов, в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» введен в действие пользовательский сегмент государственной информационной системы Камчатского края ГИС «Сетевой город» (далее – ГИС «Сетевой город»).

1.2. К работе с компонентами ГИС «Сетевой город» допущены: администратор информационной безопасности (далее – Администратор), пользователи информационной системы (далее – Пользователи) и ответственный за хранение и эксплуатацию средств криптографической защиты информации. В МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» назначен ответственный за организацию обработки персональных данных (далее – Ответственный).

1.3. С целью защиты информации от несанкционированного нарушения ее конфиденциальности, целостности и доступности в ГИС «Сетевой город» организационными и техническими средствами реализована система защиты информации.

1.4. Несмотря на то, что многие действия по защите информации производятся прозрачно для Пользователя, он остается активным участником процесса по защите конфиденциальной информации и является вовлеченным в процессы обеспечения информационной безопасности в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева».

1.5. Пользователи ГИС «Сетевой город» не являются привилегированными пользователями информационной системы и получают доступ к ресурсам информационной системы в соответствии с Положением о разграничении доступа в пользовательском сегменте ГИС «Сетевой город». Каждому Пользователю предоставляется минимально необходимый для выполнения своих служебных обязанностей доступ к ресурсам ГИС «Сетевой город».

1.6. Пользователи ГИС «Сетевой город» при работе с техническими средствами и информационными технологиями, являющимися частью ГИС «Сетевой город», должны соблюдать положения настоящей Инструкции.

1.7. Настоящая инструкция разработана с учетом положений следующих законодательных и нормативно-правовых актов:

– Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информатизации и защите информации»;

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

– «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;

– «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 года;

– «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;

– Методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;

– «Состав и содержание 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 защищенности», утверждённые приказом ФСБ России № 378 от 10.07.2014;

– «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом ФСБ от 9 февраля 2005 №66;

– «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 №152.

2. ОБЩИЕ ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ГИС «СЕТЕВОЙ ГОРОД»

2.1. Пользователь в ГИС «Сетевой город» выполняет только те действия, которые необходимы для выполнения его служебных обязанностей. Любые посторонние действия в ГИС «Сетевой город» запрещены.

2.2. Пользователь подписывает соглашение о неразглашении конфиденциальной информации перед началом выполнения служебных обязанностей, связанных с доступом к такой информации.

2.3. Пользователь незамедлительно оповещает Администратора о любой подозрительной активности в ГИС «Сетевой город».

2.4. Пользователю запрещено использовать личные технические средства (ноутбуки, смартфоны, планшеты, фотокамеры, флеш-носители, съемные жесткие диски и пр.) для несанкционированного копирования, фотографирования, распространения и передачи защищаемой информации.

2.5. Пользователь принимает участие в инструктажах по информационной безопасности, проводимым Администратором и Ответственным. При получении дополнительных материалов от Администратора и Ответственного во время инструктажей, Пользователь самостоятельно изучает их с целью повышения своей осведомленности в вопросах информационной безопасности и защиты персональных данных.

2.6. Пользователь визуально контролирует целостность технических средств на своем рабочем месте (отсутствие попыток физического вскрытия системного блока и пр.). При подозрении на нарушение целостности технических средств ГИС «Сетевой город», Пользователь сообщает об этом Администратору. Пользователю запрещен самостоятельный ремонт технических средств ГИС «Сетевой город», а также привлечение посторонних лиц для такого ремонта.

2.7. В случае объективной необходимости, Пользователь участвует в составе комиссии по защите информации обрабатываемой в ГИС «Сетевой город» в расследованиях причин инцидентов безопасности.

2.8. В целях блокирования возможности несанкционированного ознакомления с защищаемой информацией на экране монитора, Пользователь должен блокировать сеанс работы в ГИС «Сетевой город» при покидании рабочего места более чем на 2 минуты. Блокировка сеанса работы в ГИС «Сетевой город» производится нажатием клавиш Win+L.

2.9. Пользователю запрещены любые действия в ГИС «Сетевой город» до прохождения процедуры идентификации и аутентификации в системе (до ввода логина и пароля).

2.10. Антивирусная защита в ГИС «Сетевой город» реализована прозрачно для пользователя, установка антивирусных программ, обновление антивирусных баз, запуск антивирусных проверок, сбор информации о найденных вирусах производится краевым государственным автономным учреждением «Камчатский центр информатизации и оценки качества образования» централизованно. Пользователю запрещено изменять настройки антивирусного программного обеспечения или отключать его (даже на короткое время). Пользователь должен оповещать

Администратора о локальных сообщениях антивирусного программного обеспечения на его автоматизированного рабочего места (далее – АРМ). Пользователь должен оповещать Администратора о любых аномалиях в работе АРМ. К таким аномалиям могут относиться:

– загрузка другой операционной системы, сбой в загрузке операционной системы или аномально долгая загрузка операционной системы;

– медленная работа локальной сети;

– медленная работа глобальной сети;

– отказ операционной системы Пользователю во входе в систему при условии правильно введенных учетных данных;

– появление сообщений о шифровании данных на жестком диске и о требовании выкупа за расшифровку этих данных;

– появление посторонних окон консоли cmd.exe, открытие незапрашиваемых вкладок в браузере, самопроизвольное открытие других окон и программ в операционной системе;

– медленная работа АРМ, быстрое исчерпание ресурсов АРМ при отсутствии ресурсоемких задач, запущенных на АРМ;

– самопроизвольная работа мыши и клавиатуры;

– быстрое исчерпание свободного места на жестком диске;

– отказ в доступе к файловой системе в целом или некоторым логическим томам в частности;

– мерцание монитора;

– несанкционированное появление баннеров и посторонних звуков на АРМ;

– замена рисунка рабочего стола;

– несанкционированное открытие/закрытие CD/DVD-привода;

– исчезновение файлов и каталогов, а также несанкционированное изменение их содержимого;

– частое обращение к жесткому диску АРМ;

– другие аномалии.

2.11. Пользователю запрещается самостоятельная установка любого программного обеспечения, даже необходимого для выполнения своих служебных обязанностей. Установка разрешенного в ГИС «Сетевой город» программного обеспечения осуществляется Администратором. Также к установке и настройке программного обеспечения в ГИС «Сетевой город», при условии соблюдения мер по защите информации, допускаются сотрудники сторонних организаций.

2.12. Пользователь должен пресекать попытки посторонних лиц (или лиц, не имеющих соответствующих полномочий) тем или иным образом получить доступ к его учетным данным, конфиденциальной информации в ГИС «Сетевой город»,

ключевой информации криптосредства и к любой другой защищаемой информации. Пользователь незамедлительно сообщает Администратору о подобных попытках (как удачных, так и неудачных).

2.13. Администратор отключает возможность использования на АРМ технологий мобильного кода (JavaScript, Adobe Flash, макросы в Microsoft Office и др.). Пользователю запрещено использовать технологии мобильного кода в обход принятых в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» политик информационной безопасности.

2.14. Пользователь в меру своих сил и возможностей содействует проведению служебных расследований, инициированных в связи с инцидентами информационной безопасности.

2.15. В МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» действует политика управления информационными потоками и фильтрации сетевого трафика. Пользователь работает только с теми сетевыми ресурсами (сетевые папки, веб сайты и пр.), которые разрешены и, работа с которыми необходима Пользователю для выполнения своих служебных обязанностей. Пользователю запрещено получать доступ к запрещенным внешним ресурсам в обход политик безопасности.

2.16. Пользователь осуществляет обработку защищаемой информации в ГИС «Сетевой город» в соответствии с технологическими процессами обработки информации, описанными в Политике информационной безопасности.

2.17. Пользователь принимает меры по противодействию несанкционированному просмотру защищаемой информации с экрана монитора посторонними лицами. К таким мерам относятся:

– сворачивание окна, в котором отображена защищаемая информация или блокирование сеанса Пользователя при нахождении посторонних лиц вблизи рабочего места Пользователя с фронтальной стороны монитора;

– ориентация монитора задней частью к дверным проемам и окнам;

– в случае вынужденной ориентации монитора фронтальной частью к окну, Пользователь во время работы с защищаемой информацией закрывает шторы, жалюзи или рольставни.

2.18. Пользователь должен знать и соблюдать положения настоящей Инструкции, а также других внутренних нормативных документов МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева». При возникновении у Пользователя вопросов по защите информации и защите персональных данных в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева», он обращается к Администратору и Ответственному. Новые Пользователи ГИС «Сетевой город» перед началом выполнения своих служебных обязанностей изучают положения настоящей Инструкции.

2.19. При работе с криптографическими средствами защиты информации (далее - СКЗИ) Пользователь выполняет предписание Инструкции по обеспечению безопасности эксплуатации СКЗИ.

3. ПРАВИЛА УПРАВЛЕНИЯ ИДЕНТИФИКАТОРАМИ, УЧЕТНЫМИ ЗАПИСЯМИ И ПАРОЛЯМИ

3.1. В МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» с целью обеспечения информационной безопасности внедрены политики управления идентификаторами, учетными записями и паролями.

3.2. Внутренними руководящими документами, определяющими политики управления идентификаторами, учетными записями и паролями, являются:

– политика информационной безопасности;

– порядок разграничения доступа к ресурсам ГИС «Сетевой город»;

– инструкция администратора информационной безопасности;

– инструкция пользователя ГИС «Сетевой город».

3.3. Пользователь перед началом работы в ГИС «Сетевой город» получает учетные данные (логин, временный пароль) у краевого государственного автономного учреждения «Камчатский центр информатизации и оценки качества образования», либо у Администратора безопасности.

3.4. При первом входе в систему Пользователь изменяет первичный временный пароль. Временной промежуток между выдачей временного пароля и первым входом Пользователя в информационную систему не должен составлять более одного часа. Пароли должны соответствовать следующим требованиям:

– минимальная длина пароля составляет 8 символов, пароль должен содержать буквы английского алфавита верхнего и нижнего регистров, как минимум одну цифру и один спецсимвол;

– новый пароль должен отличаться минимум на два символа от предыдущего;

– запрещается использование пользователями пяти последних использованных паролей при создании новых паролей.

3.5. Максимальное время действия пароля - 90 дней. По истечении срока действия пароля, Пользователь должен придумать новый пароль, удовлетворяющий требованиям к паролям (п. 3.4 настоящей инструкции).

3.6. При восьми неудачных попытках входа, учетная запись Пользователя блокируется. Для разблокировки учетной записи Пользователю необходимо обратиться к Администратору.

3.7. Пользователю запрещено записывать и хранить пароли в местах, доступных для просмотра посторонним лицам (на отдельных листах бумаги, в не запираемой тумбе, под клавиатурой, на мониторе и т. п.).

3.8. Пользователь должен удостовериться, что при вводе пароля никто не наблюдает за процессом ввода пароля.

3.9. Пользователю запрещено разглашать другим пользователям свой пароль, в том числе Администратору.

3.10. Пользователю запрещено вводить свои учетные данные для предоставления возможности временной работы в ГИС «Сетевой город» другим Пользователями или посторонним лицам, поскольку все выполненные этими лицами действия в ГИС «Сетевой город» будут считаться действиями, выполненными Пользователем. Ответственность за неправомерные действия таких посторонних лиц несет Пользователь.

3.11. При подозрении на компрометацию пароля или иной идентификационной информации, Пользователь должен незамедлительно сообщить об этом Администратору.

4. ПРОТИВОДЕЙСТВИЕ МЕТОДАМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ И ПРАВИЛА РАБОТЫ С ЭЛЕКТРОННОЙ ПОЧТОЙ

4.1. Применение злоумышленником методов социальной инженерии является самым эффективным и разрушительным способом нарушения информационной безопасности на любом предприятии в обход всех технических мер по защите информации. Методы социальной инженерии направлены на использование человеческого фактора (человеческих слабостей и недостатков) с целью получения от Пользователя защищаемой информации или его учетных данных в ГИС «Сетевой город» (логин и пароль). Злоумышленники - социальные инженеры для достижения своих целей могут эксплуатировать следующие особенности того или иного Пользователя:

– лень;
– спешка (паника);
– безразличие;
– профессиональный интерес;
– желание;
– жадность;
– сострадание;
– доверчивость;
– страх.

4.2. Основным способом реализации методов социальной инженерии является обман Пользователя. Поскольку социальная инженерия нацелена на слабости человека, а не на технические недоработки или уязвимости информационной

системы, наиболее эффективным методом противодействия социальной инженерии является повышение осведомленности Пользователей о методах социальной инженерии.

4.3. Взаимодействие социального инженера с Пользователем бывает трех типов: контактное (личное), телефонное и взаимодействие через электронные каналы связи. Наиболее распространено взаимодействие через электронные каналы связи, в особенности по электронной почте.

4.4. При личном и телефонном общении Пользователь должен убедиться, что разговаривает именно с тем человеком, за которого себя выдает собеседник. При личном или телефонном взаимодействии социальный инженер обычно использует следующие тактики:

– представившись сотрудником технической поддержки какого-либо сервиса или службы, социальный инженер сообщает Пользователю о какой-либо поломке или нарушении в функционировании того или иного необходимого в работе сервиса, вызывая тем самым панику и заставляя Пользователя сообщить свои учетные данные;

– представившись руководителем высокого ранга, социальный инженер изображает гнев и недовольство действием или бездействием Пользователя, вынуждая сообщить учетные данные или иную конфиденциальную информацию;

– представившись сотрудником организации, деятельность которой, так или иначе, может быть интересна Пользователю, вынуждает сообщить учетную или иную конфиденциальную информацию;

– иные подобные тактики.

4.5. При взаимодействии через электронную почту, социальный инженер преследует одну из двух основных целей:

– заражение АРМ Пользователя вредоносным программным обеспечением через запуск приложенного к письму файла или переходом по вредоносной ссылке;

– переход Пользователя по поддельной ссылке, по которой находится точная копия формы авторизации легального сервиса, и ввод в эту форму идентификационной информации (как правило, при первом вводе логина и пароля поддельная форма сообщает о неправильном вводе пароля и перенаправляет на настоящую форму авторизации сервиса).

4.6. Наиболее распространенные примеры применения методов социальной инженерии с использованием каналов электронной почты:

– письмо от налоговой инспекции с предложением установить из вложенного файла новые формы для сдачи налоговых деклараций;

– письмо из банка о просроченном платеже по кредиту, подробности во вложенном файле;

– письмо из суда о возбуждении административного/уголовного дела, подробности во вложении;

– письмо от провайдера об одностороннем изменении тарифного плана, подробности во вложении;

– письмо от банка (или любого другого учреждения) о блокировке учетной записи на сайте или личного кабинета, необходимо пройти по ссылке, ввести учетные данные и вручную разблокировать личный кабинет или учетную запись;

– письмо от сервиса электронной почты (gmail.com, mail.ru, yandex.ru и т. п.) о грядущей блокировке почтового ящика, об исчерпании свободного места и т. д., необходимо пройти по ссылке, ввести учетные данные и выполнить некоторые действия.

4.7. При работе с электронной почтой в контексте противодействия методам социальной инженерии Пользователь руководствуется следующей информацией:

– совпадение адреса отправителя электронного письма с доверенным адресом не является гарантией подлинности самого письма, поскольку поле «от кого» может быть подделано злоумышленником;

– любые письма с вложениями являются подозрительными;

– любые письма, в которых отсутствует альтернативная контактная информация отправителя (ФИО, должность, мобильный, рабочий телефон, почтовый адрес), являются подозрительными;

– при получении неожидаемого электронного письма с вложением или ссылкой от якобы доверенного отправителя, необходимо по альтернативным каналам связи (лично, по телефону, через мессенджер) уточнить факт отправки такого письма;

– государственные и иные организации (банки, операторы связи и т. д.) не уведомляют своих клиентов о каких-либо проблемах, исках, блокировках по электронной почте, это делается официальным письмом на бумажном носителе, через СМС (например, в случае подключенного он-лайн банкинга) или по телефону;

– необходимо тщательно проверять корректность ссылок, по которым просят пройти в письме, чаще всего злоумышленники используют похожие, но другие доменные имена, чтобы ввести Пользователя в заблуждение, например, заменяя букву “b” на букву “d” или цифру “1” на букву “l” и наоборот.

4.8. Атаки социальных инженеров могут быть веерными (нацеленными на как можно большее число жертв), так и целенаправленными (нацеленными на конкретную организацию или на конкретного человека). В случае целенаправленных атак, социальный инженер изучает информацию о потенциальной жертве и об организации из открытых источников (сайт компании, сайты партнеров и контрагентов, электронные биржи труда, социальные сети, новостные ленты и прочие ресурсы). В случае, если о Пользователе публикуется информация в открытых

источниках или он сам публикует информацию о своем месте работы, роде деятельности, должностных обязанностях, Пользователь должен быть готов к применению этой информации социальным инженером против него.

4.9. В случае подозрения Пользователя на применение против него методов социальной инженерии, Пользователь незамедлительно сообщает о данном факте Администратору.

5. РАБОТА СО СЪЕМНЫМИ НОСИТЕЛЯМИ ИНФОРМАЦИИ

5.1. Пользователю разрешается использовать только учтенные съемные носители информации в ГИС «Сетевой город» (флешки, съемные жесткие диски, карты памяти и пр.).

5.2. При необходимости использования для исполнения служебных обязанностей съемных носителей информации, Пользователь в письменной форме делает запрос Администратору на выдачу учтенного съемного носителя информации. Пользователь расписывается за получение и сдачу учтенного съемного носителя информации в Журнале учета носителей информации.

5.3. При необходимости выноса съемного носителя из помещения, Пользователь обеспечивает защиту съемного носителя от утери, кражи или компрометации защищаемой информации на этом носителе.

5.4. В случае утери, кражи или компрометации учтенного носителя, Пользователь оперативно сообщает об этом Администратору.

5.5. Пользователь несет ответственность за сохранность выданных ему съемных носителей информации и за конфиденциальность защищаемой информации, записанной на него.

Приложение №6 к приказу
МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»
от 27.09.2019 г. № 100 §1

Положение о контролируемой зоне пользовательского сегмента государственной информационной системы Камчатского края «Сетевой город»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Под контролируемой зоной (далее – КЗ) понимается территория, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.

1.2. Схемы контролируемой зоны фиксируются в техническом паспорте на пользовательский сегмент государственной информационной системы Камчатского края «Сетевой город» (далее – ГИС «Сетевой город»). Администратор информационной безопасности (далее – Администратор) обеспечивает актуальность приведенной в техническом паспорте.

1.3. Охраной помещений во внерабочее время занимается штатный сторож.

2. ПОРЯДОК ДОСТУПА В ОХРАНЯЕМЫЕ ПОМЕЩЕНИЯ

2.1. Допуск в охраняемые помещения осуществляется в соответствии с утвержденным в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» документом «Перечень помещений, в которых разрешена работа с ресурсами пользовательского сегмента ГИС «Сетевой город», в которых размещены технические средства ГИС «Сетевой город», а также перечень лиц, допущенных в эти помещения».

2.2. Помещения, в которых осуществляется обработка защищаемой информации, оборудовано пожарной сигнализацией, а также прочными дверьми с механическими замками.

2.3. Ключи от помещений выдаются и находятся на хранении у сотрудников, которым необходим доступ в эти помещения для выполнения своих служебных (должностных) обязанностей.

2.4. Сотрудникам, которым необходим временный доступ в помещения, к которым у них нет допуска, может быть предоставлен такой доступ, но только в присутствии сотрудников, работающих в этом помещении (имеющих доступ в это помещение) и при условии соблюдения правил ограничения доступа к обрабатываемой информации.

2.5. При покидании помещения и при отсутствии в нем других лиц, допущенных в это помещение, сотрудник обязан проследить, чтобы в помещении не было посторонних лиц, и закрыть помещение на ключ.

2.6. Перед началом рабочего дня помещения снимаются с охраны. После окончания рабочего дня, помещения устанавливаются под охрану в соответствии с установленным в разделе 3 настоящего положения порядком.

3. ПОРЯДОК ПЕРЕДАЧИ ПОМЕЩЕНИЙ ПОД ОХРАНУ

3.1. Закрытие помещений, в которых обрабатывается защищаемая информация, осуществляется по окончании рабочего дня последним сотрудником, покидающим помещение. Закрытие помещения осуществляется после проведения в нем уборки, обесточивания оборудования, закрытия окон.

3.2. После запирания помещения на ключ, сдачи ключа от помещения под роспись вахтеру, помещение считается принятым под охрану.

3.3. При вскрытии помещения, допущенные в него сотрудники осуществляют осмотр на предмет выявления признаков несанкционированных действий в помещении в их отсутствие (повреждения дверей, повреждения пломб, изменение местоположения мебели, включенная техника и т. п.). При отсутствии нарушений, помещение считается снятым с охраны.

3.4. В случае обнаружения нарушений, сотрудник сообщает об этом Администратору, который, в свою очередь, созывает комиссию по защите информации обрабатываемой в ГИС «Сетевой город» (далее – Комиссия). Далее Комиссия действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

4. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

4.1. Настоящее положение может быть изменено и дополнено по следующим причинам:

– появление информации о новых угрозах безопасности информации, связанных с физическим доступом к техническим средствам информационных систем;

– при возникновении инцидентов информационной безопасности, связанных с физическим доступом, извлечения из них уроков и понимания необходимости пересмотра настоящего положения;

– при изменении законодательства в сфере защиты информации.

4.2. За нарушение настоящего положения, сотрудники могут нести дисциплинарную ответственность или иную ответственность (уголовную, административную) в соответствии с законодательством Российской Федерации.

Приложение №8 к приказу МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» от 27.09.2019 г. № 100 §1

Политика информационной безопасности пользовательского сегмента государственной информационной системы Камчатского края «Сетевой город»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая политика информационной безопасности (далее – Политика) утверждается приказом МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» и определяет мероприятия, процедуры и правила по защите информации в информационных системах МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева».

1.2. Положения настоящей Политики распространяются на пользовательский сегмент государственной информационной системы Камчатского края «Сетевой город» (далее – ГИС «Сетевой город») принадлежащий МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева».

1.3. Положения настоящей Политики обязательны к исполнению для всех пользователей ГИС «Сетевой город» (далее - Пользователи), а также для администратора безопасности (далее - Администратор).

1.4. В соответствии с указом Президента Российской Федерации № 188 от 6 марта 1997 года к сведениям конфиденциального характера (защищаемой информации) в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» относятся:

– сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

1.5. Целями настоящей Политики являются:

– обеспечение конфиденциальности, целостности, доступности защищаемой информации;

– предотвращение утечек защищаемой информации;

– мониторинг событий безопасности и реагирование на инциденты безопасности;

– нейтрализация актуальных угроз безопасности информации;

– выполнение требований действующего законодательства по защите информации.

1.6. В настоящей Политике используются термины и определения, установленные законодательством Российской Федерации об информации, информационных технологиях и о защите информации, а также термины и определения, установленные национальными стандартами в области защиты информации.

1.7. Настоящая Политика разработана с учетом положений следующих законодательных и нормативно-правовых актов:

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

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

– «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;

– «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 года;

– «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;

– методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;

– «Состав и содержание 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 защищенности», утверждённые приказом ФСБ России № 378 от 10.07.2014;

– «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом ФСБ от 9 февраля 2005 №66;

– «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 №152.

2. ТЕХНОЛОГИЧЕСКИЕ ПРОЦЕССЫ ОБРАБОТКИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

2.1. В данном разделе настоящей Политики описаны технологические процессы обработки различных видов защищаемой информации в информационных системах МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева». Администратор и Пользователи, допущенные к обработке той или иной защищаемой информации, обязаны производить обработку этой информации в соответствии с описаниями технологических процессов обработки информации, приведенных в данном разделе.

2.2. Технологический процесс обработки защищаемой информации МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»:

– пользовательский сегмент ГИС «Сетевой город» состоит из 3 автоматизированных рабочих мест. ГИС «Сетевой город» имеет одноточечный выход в сети общего пользования и международного телекоммуникационного обмена. Задачей информационной системы является отправка данных на веб портал серверного сегмента ГИС «Сетевой город». Основным программным обеспечением, которое используется в работе для обработки данных является Microsoft Office (либо иной текстовый редактор) и браузер. Персональные данные вносятся путем ручного ввода оператором с бумажного носителя в электронную форму. Файлы с данными формируются при помощи прикладного программного обеспечения Microsoft Office (либо с помощью иного текстового редактора). Отправка данных организована в виде веб-формы, просматриваемой в браузере. Для передачи защищаемой информации на веб-портал серверного сегмента ГИС «Сетевой город» используется СКЗИ ViPNet Client. Физически все введённые данные хранятся в серверном сегменте ГИС «Сетевой город».

3. ПРАВИЛА И ПРОЦЕДУРЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ГИС «СЕТЕВОЙ ГОРОД», ПОЛИТИКА РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ ГИС «СЕТЕВОЙ ГОРОД»

3.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева», допущенному к работе с ресурсами ГИС «Сетевой город», присваивается уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ГИС «Сетевой город».

3.2. Под учетной записью Пользователя понимается учетная запись для доступа к информационной системе в домене Active Directory.

3.3. Использование одного и того же имени пользователя несколькими пользователями (или группового имени для нескольких пользователей) в ГИС «Сетевой город» запрещено.

3.4. Процедура регистрации (создания учетной записи и выдачи, при необходимости, электронного ключа) пользователя ГИС «Сетевой город» для сотрудника МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» и предоставления ему (или изменения его) прав доступа к ресурсам ГИС «Сетевой город» инициируется заявкой Администратора в Краевое государственное автономное учреждение «Камчатский центр информатизации и оценки качества образования».

3.5. Администратор дает ознакомиться с инструкцией Пользователя ГИС «Сетевой город» под роспись, сообщает пользователю идентификационные данные и допускает к работе в ГИС «Сетевой город». После допуска к работе в ГИС «Сетевой город», Пользователь самостоятельно формирует пароль доступа к своей учетной записи в соответствии с требованиями раздела 3 Инструкции Пользователя ГИС «Сетевой город».

3.6. В качестве модели разграничения доступа к ресурсам ГИС «Сетевой город» выбрана ролевая модель. Пользователям назначается роль в разграничительной системе ГИС «Сетевой город» в зависимости от выполняемых должностных обязанностей и задач и, соответственно, в зависимости от необходимости по доступу к тем или иным ресурсам ГИС «Сетевой город». Обязанности и задачи пользователей определяются исходя из технологических процессов обработки информации, описанных в разделе 2 настоящей Политики. Описание всех возможных ролей в ГИС «Сетевой город» приведено в Приложении № 1 к настоящей Политике. Помимо учетных записей Пользователей, доступ к системе получают различные системные службы и процессы.

3.7. Перечень лиц, их должностей, а также служб и процессов, допущенных к работе с ресурсами ГИС «Сетевой город», и сопоставляемые им роли приведены в Приложении № 2 к настоящей Политике. Администратор обеспечивает оперативное обновление и актуальность данного перечня.

3.8. Перечень помещений, в которых разрешена работа с ресурсами ГИС «Сетевой город», расположены технические средства ГИС «Сетевой город», а также перечень лиц, допущенных в эти помещения, приведен в Приложении № 3 к настоящей Политике. Администратор обеспечивает оперативное обновление и актуальность данного перечня.

3.9. Идентификация и аутентификация на сетевом оборудовании (коммутаторы, маршрутизаторы, точки доступа и т. д.) разрешена только Администратору и сотрудникам сторонней организации, производящим работы в сети МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» на договорной основе под контролем Администратора. При вводе в эксплуатацию сетевого оборудования на

нем обязательно меняются идентификационные и аутентификационные данные, установленные производителем устройства по умолчанию. Новые идентификационные данные на сетевых устройствах должны соответствовать установленной парольной политике.

3.10. Пользователям запрещены любые действия в ГИС «Сетевой город» до прохождения процедуры идентификации и аутентификации в системе. Администратору разрешается ряд действий до прохождения идентификации и аутентификации в ГИС «Сетевой город» в ряде случаев. Условия, при которых разрешаются такие действия, и перечень разрешенных действий для Администратора, до прохождения процедуры идентификации и аутентификации в ГИС «Сетевой город», перечислены в пункте 4.1 инструкции Администратора.

4. ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ПОТОКАМИ

4.1. Контроль и фильтрация информационных потоков между ГИС «Сетевой город» и внешними телекоммуникационными сетями осуществляется с помощью межсетевого экрана «ViPNet Client».

4.2. Для контроля и фильтрации информационных потоков между ГИС «Сетевой город» и внешними телекоммуникационными сетями выбирается политика «Блокировать все, кроме явно разрешенного». Такая политика выбрана с целью исключения возможности доступа Пользователей к сайтам с вредоносным содержимым, а также к фишинговым сайтам (сайты, имитирующие другие легальные сайты с целью кражи аутентификационной и/или личной информации Пользователей). Также такая политика выбрана исходя из практической невозможности блокировки всех фишинговых сайтов и ресурсов с вредоносным содержимым при выборе политики «Разрешено все, кроме явно запрещенного».

4.3. С целью реализации политики контроля и фильтрации информационных потоков между ГИС «Сетевой город» и внешними телекоммуникационными сетями «Блокировать все, кроме явно разрешенного» утверждается список разрешающих правил взаимодействия с внешними телекоммуникационными сетями, приведенный в Приложении № 4 к настоящей Политике. Данный список может быть дополнен на основании заявки Администратора Краевому государственному автономному учреждению «Камчатский центр информатизации и оценки качества образования» с указанием обоснования добавления того или иного ресурса/сайта/протокола/порта в список разрешенных.

4.4. Администратор контролирует соответствие настроек межсетевого экрана «ViPNet Client», приведенному в Приложении № 4 к настоящей Политике, списку разрешительных правил.

5. ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ УСТАНОВКОЙ (ИНСТАЛЛЯЦИЕЙ) КОМПОНЕНТОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

5.1. В ГИС «Сетевой город» разрешено использование только того программного обеспечения, его компонентов, утилит и драйверов, которые необходимы для обеспечения функционирования информационной системы, а также необходимы для выполнения служебных (должностных) обязанностей пользователями.

5.2. Перечень разрешенного программного обеспечения в ГИС «Сетевой город» определен в Приложении № 5 к настоящей Политике.

5.3. Установка программного обеспечения, его компонент, утилит и драйверов осуществляется только Администратором безопасности в соответствии с Приложением № 5. Пользователям запрещена установка любого ПО в ГИС «Сетевой город».

5.4. Пользователь имеет право подать заявку в виде служебной записки на включение в список разрешенного в ГИС «Сетевой город» программного обеспечения, необходимых ему для выполнения служебных (должностных) обязанностей, программ, утилит, драйверов. В такой служебной записке обязательно указывается обоснование необходимости включения в этот список нового программного обеспечения. Срок рассмотрения заявки должен составлять не более 3 рабочих дней.

5.5. Администратор ежемесячно проводит проверку соответствия состава программного обеспечения в ГИС «Сетевой город» списку разрешенного ПО. В случае выявления постороннего программного обеспечения, созывается комиссия по защите информации обрабатываемой в ГИС «Сетевой город», которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

6. ЗАЩИТА МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ, КОНТРОЛЬ ИНТЕРФЕЙСОВ ВВОДА-ВЫВОДА, ГАРАНТИРОВАННОЕ УНИЧТОЖЕНИЕ ИНФОРМАЦИИ

6.1. Одной из основных целей злоумышленников являются машинные носители информации, используемые в ГИС «Сетевой город» для хранения и обработки защищаемой информации. Исходя из этого, защита машинных носителей информации (как в стационарных АРМ и серверах) является ключевым звеном политики информационной безопасности МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева».

6.2. Учет машинных носителей осуществляется Администратором в соответствующих журналах. Администратор несет ответственность, за достоверность и своевременность сведений, отраженных в журнале учета машинных носителей информации.

6.3. В МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» учету подлежат:

– съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные подобные устройства);

– машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

6.4. Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

6.5. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

6.6. Администратор маркирует съемные машинные носители и портативные вычислительные устройства и делает соответствующую отметку в журнале. Использование маркированного соответствующим образом носителя информации за пределами контролируемой зоны и/или информационной системы является инцидентом информационной безопасности и расследуется в установленном порядке, кроме использование в установленном порядке флэш-носителя.

6.7. Использование неучтенных съемных носителей и/или портативных устройств (в том числе личных) в ГИС «Сетевой город» запрещено.

6.8. Невозможность использования неучтенных съемных носителей информации обеспечивается путем программных настроек СЗИ от НСД «Secret Net Studio». Настройками «Secret Net Studio» неучтенные носители информации блокируются на всех стационарных устройствах ГИС «Сетевой город». Попытки использования неучтенных съемных носителей информации фиксируются средствами «Secret Net Studio». Такие попытки являются инцидентами безопасности и расследуются в установленном порядке.

6.9. Невозможность использования неучтенных портативных вычислительных устройств обеспечивается путем организации аутентификации в системе не только пользователя ГИС «Сетевой город», но и самого устройства по нескольким параметрам (имя устройства, IP-адрес, MAC-адрес и другие).

6.10. Невозможность использования неучтенных машинных носителей в стационарных устройствах обеспечивается путем физического контроля доступа в соответствии с инструкциями Пользователя и Администратора, а также путем проведения периодических мероприятий по инвентаризации ресурсов ГИС «Сетевой город» и комплектности технических средств.

6.11. Гарантированное уничтожение (стирание) информации на машинных носителях организовывается Администратором в случаях:

– возвращения учтенного съемного носителя информации Администратору;

– при вводе в эксплуатацию нового машинного носителя или технического средства со встроенными носителями информации;

– при передаче носителя информации в сторонние организации (в том числе и для проведения ремонта технического средства);

– при утилизации технических средств.

6.12. Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации. Контроль невозможности восстановления уничтоженной информации производится Администратором с помощью специализированных утилит по восстановлению информации.

6.13. При возвращении учтенного съемного носителя информации Пользователем, а также при вводе в эксплуатацию нового машинного носителя, информация уничтожается путем использования механизма СЗИ от НСД «Secret Net Studio» затирания файлов случайной битовой последовательностью.

6.14. При передаче носителя информации в сторонние организации (не с целью передачи на нем информации), в том числе и для ремонта носителя или технического средства, информация уничтожается путем полной многократной перезаписи машинного носителя информации специальными битовыми последовательностями, зависящими от типа накопителя и используемого метода кодирования информации. Затем производится очистка всего физического пространства накопителя, включая сбойные и резервные элементы памяти, специализированными программами или утилитами производителя.

6.15. В случаях уничтожения информации способами, описанными в пунктах 6.13 и 6.14 настоящей Политики, Администратор фиксирует факт уничтожения информации, а также факт контроля уничтожения информации в Журнале учета мероприятий по защите информации в ГИС «Сетевой город».

6.16. При утилизации технических средств, а также при возникновении необходимости уничтожения информации на неперезаписываемых машинных носителях (например, CD-R), физически уничтожается сам машинный носитель.

6.17. В случае физического уничтожения машинного носителя информации, составляется акт уничтожения. Акт уничтожения машинных носителей

подписывается назначенной приказом руководителя комиссией по защите информации обрабатываемой в пользовательском сегменте ГИС «Сетевой город» по форме утвержденного акта уничтожения персональных данных.

7. УПРАВЛЕНИЕ ВЗАИМОДЕЙСТВИЕМ С ИНФОРМАЦИОННЫМИ СИСТЕМАМИ СТОРОННИХ ОРГАНИЗАЦИЙ (ВНЕШНИМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ)

7.1. В МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» осуществляется взаимодействие со следующими внешними информационными системами:

– Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационнотехнологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» обеспечивает идентификацию и аутентификацию пользователей ГИС «Сетевой город»;

– Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг (функций)»;

– Федеральная государственная информационная система «Единая система межведомственного электронного взаимодействия»;

– Государственная информационная система Камчатского края «Региональная система межведомственного электронного взаимодействия Камчатского края»;

– Портал государственных и муниципальных услуг Камчатского края;

– Государственная информационная система Камчатского края «Многофункциональный центр»;

– Федеральная государственная информационная система, обеспечивающая ведение электронной очереди приема детей в дошкольные образовательные организации;

– Федеральный реестр сведений о документах об образовании и (или) квалификации, документах об обучении.

7.2. Администратор совместно с краевым государственным автономным учреждением «Камчатский центр информатизации и оценки качества образования» обеспечивает управление информационными потоками при взаимодействии с внешними информационными системами в соответствии с правилами и процедурами, описанными в разделе 4 настоящей инструкции.

7.3. Порядок обработки, хранения и передачи информации с использованием внешних информационных систем определяются технологическими процессами обработки информации, описанными в разделе 2 настоящей Политики.

7.4. Разрешение обработки, хранения и передачи защищаемой информации с использованием внешних информационных систем в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» возможно только при выполнении следующих условий:

– при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы;

– при наличии подтверждения выполнения во внешней информационной системе предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

8. ПРАВИЛА И ПРОЦЕДУРЫ ВЫЯВЛЕНИЯ, АНАЛИЗА И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

8.1. В МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» в качестве средства выявления уязвимостей используется сертифицированный сканер уязвимостей Сканер-ВС.

8.2. Сканирование ГИС «Сетевой город» на наличие уязвимостей проводится краевым государственным автономным учреждением «Камчатский центр информатизации и оценки качества образования».

8.3. Администратор изучает отчеты по результатам сканирования полученные от краевого государственного автономного учреждения «Камчатский центр информатизации и оценки качества образования» и принимает решение о немедленном устранении выявленных уязвимостей, либо о включении мероприятий по устранению выявленных уязвимостей в план мероприятий по защите информации, в случае, если выявленные уязвимости не являются критичными, или если есть возможность сделать невозможным их эксплуатацию потенциальным злоумышленником (например, путем отключения отдельных АРМ и/или сегментов сети от Интернет). При необходимости, для адекватного реагирования на вновь выявленные угрозы может созываться Комиссия.

8.4. Критичность уязвимостей может быть установлена как на основании рейтинга уязвимости по шкале CVSS, так и на основании оценки рисков информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

8.5. В случае невозможности оперативного устранения критичной уязвимости, Администратор уведомляет об этом руководителя МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» и краевое государственное автономное учреждение «Камчатский центр информатизации и оценки качества образования».

9. ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ УСТАНОВКИ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

9.1. С целью противодействия эксплуатации известных уязвимостей, в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» устанавливаются правила и процедуры контроля установки обновлений системного и прикладного программного обеспечения.

9.2. В программном обеспечении, поддерживающем автоматические обновления, таких как Java, Acrobat Reader и т. д. автоматические обновления не отключаются.

9.3. Общесистемное программное обеспечение и основное прикладное программное обеспечение обновляется во внерабочее время. Администратор перед обновлениями создает образы системы, точки восстановления и резервные копии.

9.4. Администратор контролирует источники обновлений программного обеспечения. Обновления должны осуществляться из доверенных источников, в соответствии с документацией на программное обеспечение.

9.5. Обновления общесистемного и основного прикладного программного обеспечения осуществляются не реже одного раза в неделю. Экстренные обновления осуществляются в случае поступления информации о критичных уязвимостях, для которых существует обновление безопасности.

9.6. Администратор в соответствии с эксплуатационной документацией на программное обеспечение осуществляет проверку установки обновлений, а также корректность установки обновлений. В МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» должно применяться только такое программное обеспечение, которое поддерживает проверку целостности файлов обновлений.

9.7. Обновление антивирусных баз, сигнатур уязвимостей, баз решающих правил средств защиты информации осуществляется в соответствии с эксплуатационной документацией на СЗИ и разделами настоящей Политики.

9.8. Обновление микропрошивок и программного обеспечения BIOS/UEFI производится только при поступлении информации о критичных уязвимостях в таком программном обеспечении, применяемом в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева».

10. ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ СОСТАВА ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

10.1. Состав технических средств (далее – ТС), программного обеспечения (далее – ПО) и средств защиты информации (далее – СрЗИ) ГИС «Сетевой город»

фиксируется в техническом паспорте на информационную систему. Технический паспорт является эталоном состава ТС, ПО и СрЗИ, по которому осуществляется периодический контроль.

10.2. В случае добавления новых ТС, ПО и СрЗИ в состав ГИС «Сетевой город» или удаления существующих компонентов, на основании акта ввода в эксплуатацию (или акта вывода из эксплуатации) максимально оперативно вносятся изменения в Технический паспорт.

10.3. Администратор осуществляет контроль состава ТС, ПО и СрЗИ не реже одного раза в месяц.

10.4. Выявление несоответствия состава ТС, ПО и СрЗИ техническому паспорту ГИС «Сетевой город» является инцидентом безопасности. В случае выявления фактов несоответствия Администратор устанавливает причины самостоятельно или созывает Комиссию.

10.5. В случае выявления несоответствия состава ТС, ПО и СрЗИ, Администратор принимает меры по оперативному исключению (восстановлению) из состава (в составе) информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

10.6. Администратор осуществляет контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принимает меры, направленные на устранение выявленных недостатков. В случае, если сертификат соответствия истек, но был продлен производителем СрЗИ, Администратор запрашивает актуальную заверенную копию сертификата. В случае, если сертификат соответствия истек, но не был продлен производителем СрЗИ, то Администратор сообщает об этом директора МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева», который принимает решение об организации самостоятельной сертификации использующегося СрЗИ, либо об обновлении использующегося СрЗИ до актуальной версии, либо о замене использующегося СрЗИ на другое аналогичное сертифицированное СрЗИ.

11. ПРАВИЛА И ПРОЦЕДУРЫ РЕЗЕРВИРОВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ИХ ВОССТАНОВЛЕНИЯ ПРИ ВОЗНИКНОВЕНИИ НЕШТАТНЫХ СИТУАЦИЙ

11.1. Резервирование информационных ресурсов (программного обеспечения, средств защиты информации) ГИС «Сетевой город» осуществляется в соответствии с инструкцией администратора безопасности информации и в соответствии с Приложением № 6 к настоящей Политике.

11.2. Резервирование технических средств осуществляется в соответствии с проектной документацией (эскизным проектом) на систему защиты информации ГИС «Сетевой город».

11.3. Восстановление из резервных копий является основным методом восстановления работоспособности информационной системы после ликвидации нештатных ситуаций.

11.4. Нештатными ситуациями являются:

– разглашение информации ограниченного доступа сотрудниками МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева», имеющими к ней право доступа, в том числе:

– разглашение информации лицам, не имеющим права доступа к защищаемой информации;

– передача информации по незащищенным каналам связи;

– обработка информации на незащищенных технических средствах обработки информации;

– опубликование информации в открытой печати и других средствах массовой информации;

– передача носителя информации лицу, не имеющему права доступа к ней;

– утрата носителя с информацией.

– неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:

– несанкционированное изменение информации;

– несанкционированное копирование информации;

– несанкционированный доступ к защищаемой информации:

– несанкционированное подключение технических средств к средствам и системам ГИС «Сетевой город»;

– использование закладочных устройств;

– использование злоумышленником легальных учетных записей пользователей для доступа к информационным ресурсам ГИС «Сетевой город»;

– использование злоумышленником уязвимостей программного обеспечения ГИС «Сетевой город»;

– использование злоумышленником программных закладок;

– заражение ГИС «Сетевой город» злоумышленником программными вирусами;

– хищение носителей информации;

– нарушение функционирования технических средств обработки информации;

– блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;

– дефекты, сбои, отказы, аварии технических средств и систем ГИС «Сетевой город»;

– дефекты, сбои, отказы программного обеспечения ГИС «Сетевой город»;

– сбои, отказы и аварии систем обеспечения ГИС «Сетевой город»;

– природные явления, стихийные бедствия:

– термические, климатические факторы (аномально низкие или аномально высокие температуры воздуха, пожары, наводнения, снегопады и т. д.);

– механические факторы (повреждения зданий, землетрясения и т. д.);

– электромагнитные факторы (отключение электропитания, скачки напряжения, удары молний и т. д.).

11.5. В случае возникновения нештатной ситуации, порядок действий при которой не регламентирован настоящей Политикой, Администратором, Ответственным и Комиссией вырабатывается конкретный план действий с учетом текущей ситуации.

11.6. Порядок оповещения должностных лиц и сроки выполнения мероприятий при нештатных ситуациях определены в Приложении № 7 настоящей Политики.

11.7. С целью усовершенствования координации действий должностных лиц по реагированию на нештатные ситуации должны проводиться регулярные тренировки по различным видам нештатных ситуаций. В случае выявления, по результатам тренировок, изъянов в положениях настоящей Политики, касающихся реагирования на нештатные ситуации, в нее могут вноситься изменения.

11.8. Инциденты безопасности информации также являются нештатной ситуацией. При выявлении нештатных ситуаций, повлекших нарушение целостности, доступности или конфиденциальности защищаемой информации по вине внутреннего или внешнего нарушителя, созывается Комиссия, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

11.9. В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем предпринимаются следующие действия:

– корректное отключение технических средств ГИС «Сетевой город» до истощения ресурса источников бесперебойного питания, перегрева технических средств и до наступления других негативных последствий;

– предпринимаются меры по устранению причин, вызвавших сбои, отказы и аварии средств и систем ГИС «Сетевой город», а также меры по замене/ремонту вышедших из строя средств и систем;

– в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, средств защиты информации, Администратор восстанавливает их из резервных копий.

11.10. В случае нештатных ситуаций, связанных со стихийными бедствиями и деструктивными природными явлениями, выполняются следующие действия:

– Пользователи корректно отключают и обесточивают свои рабочие места;

– системные администраторы корректно отключают и обесточивают серверы и сетевое оборудование;

– Администратор предпринимает меры к эвакуации носителей информации и носителей резервных копий;

– в случае нарушения корректной работы технических средств в ГИС «Сетевой город» в результате стихийных бедствий или природных явлений принимаются меры по ремонту/замене вышедшего из строя оборудования;

– в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, средств защиты информации, в результате стихийных бедствий или природных явлений, Администратор восстанавливает их из резервных копий;

– в случае стихийных бедствий/природных явлений, опасных для жизни человека, в первую очередь организуется эвакуация сотрудников и только по возможности организуется эвакуация технических средств, носителей информации и носителей с резервными копиями.

Приложение № 1 к Политике информационной безопасности пользовательского сегмента государственной информационной системы Камчатского края «Сетевой город», утвержденной приказом от 27.09.2019 г. № 100 §1

Положение о разграничении прав доступа в пользовательском сегменте ГИС «Сетевой город»

Исходя из характера и режима обработки защищаемой информации в ГИС «Сетевой город» определяется следующий перечень групп Пользователей, служб и процессов, участвующих в обработке защищаемой информации. Перечень ролей и описание параметров доступа к ресурсам ГИС «Сетевой город» приведен в таблице.

Роль	**Описание параметров доступа к ресурсам ГИС «Сетевой город» для данной роли**
Администратор безопасности	Доступ на запись и чтение защищаемой информации при работе с прикладным программным обеспечением. Из под учетных записей с этой ролью разрешен запуск системных процессов. Доступ к просмотру настроек СЗИ и полный доступ к настройкам операционной системы.
Пользователь	Доступ на запись и чтение защищаемой информации при работе с прикладным программным обеспечением. Из под учетных записей с этой ролью разрешен запуск всех не системных процессов, необходимых для выполнения служебных обязанностей.

Приложение № 7 к Политике информационной безопасности пользовательского сегмента государственной информационной системы Камчатского края «Сетевой город», утвержденной приказом от 27.09.2019 г. № 100 §1

План обеспечения непрерывности функционирования пользовательского сегмента ГИС «Сетевой город»

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
1.	Разглашение защищаемой информации сотрудниками, имеющими легальные права доступа к ней	-	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	1 день
2.	Обнаружение несанкционированно скопированной или измененной конфиденциальной информации	-	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	1 день
3.	Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц имеющих право доступа к ней	-	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	Сразу после получения информации об инциденте	1 день

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
4.	Обнаружение подключения технических средств к средствам и системам объекта информатизации	-	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	3 часа
5.	Подключение технических средств к средствам и системам ГИС «Сетевой город» в текущий момент времени	-	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	Сразу после получения информации об инциденте	3 часа
6.	Обнаружение закладочных устройств	-	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	Сразу после получения информации об инциденте	1 день
7.	Установка закладочных устройств злоумышленником в текущий момент времени	-	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
8.	Маскировка под зарегистрированного пользователя внешним злоумышленником в текущий момент времени	-	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
9.	Маскировка под зарегистрированного пользователя внутренним	-	Администратору сразу после	Администратору не позднее 8	10 минут в рабочее время	12 часов

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
	злоумышленником или обнаружением факта маскировки		обнаружения инцидента	часов после инцидента	(1 час в нерабочее)	
10.	Использование дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени	-	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
11.	Использование программных закладок внешним нарушителем в текущий момент времени	-	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
12.	Использование программных закладок внутренним злоумышленником или обнаружение факта использования	-	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
13.	Обнаружение программных вирусов	-	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
14.	Хищение носителя защищаемой информации	-	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 сутки	3 дня

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
15.	Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником	Нарушена работа одного пользователя	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	2 дня
		Нарушена работа группы пользователей	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	1 день
16.	Обнаружение нарушения функционирования ТС обработки информации произведенного злоумышленником	Нарушена работа одного пользователя	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	2 дня
		Нарушена работа группы пользователей	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	1 день
17.	Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внешним злоумышленником в текущий момент времени	-	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	7 дней

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
18.	Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внутренним злоумышленником в текущий момент времени	-	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	1 день
19.	Обнаружение произошедшего факта блокировки доступа к защищаемой информации	-	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	1 день
20.	Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации	-	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	2 часа в рабочее время (12 часов в нерабочее)	1 день
21.	Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО	Нарушена работа одного пользователя	Администратору сразу после обнаружения инцидента	Администратору в первый рабочий день после инцидента	20 минут	2 дня
		Нарушена работа группы пользователей	Администратору сразу после	Администратору сразу после	20 минут	1 день

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
			обнаружения инцидента	обнаружения инцидента		
22.	Дефекты, сбои, отказы, аварии ТС, программных средств и систем ГИС «Сетевой город»	Сбой ТС и систем ГИС «Сетевой город»	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	1 час	2 дня
		Отказ ТС и систем ГИС «Сетевой город», затронувший работу группы пользователей	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час в рабочее время (8 часов в нерабочее)	1 день
		Отказ ТС и систем ГИС «Сетевой город», затронувший работу одного пользователя	Администратору сразу после обнаружения инцидента	Администратору в первый рабочий день после инцидента	1 час	2 дня
		Авария ТС и систем ГИС «Сетевой город»	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	1 день

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
23.	Сбои, отказы и аварии систем обеспечения ГИС «Сетевой город»	Сбой систем обеспечения ГИС «Сетевой город»	Ответственному за материально-техническое обеспечение сразу после инцидента	Ответственному за материально-техническое обеспечение в первый рабочий день после инцидента	1 час	1 день
		Отказ систем обеспечения ГИС «Сетевой город», затронувший работу группы пользователей	Ответственному за материально-техническое обеспечение и Администратору сразу после обнаружения инцидента	Ответственному за материально-техническое обеспечение и Администратору сразу после обнаружения инцидента	1 час	1 день
		Отказ систем обеспечения ГИС «Сетевой город», затронувший работу одного пользователя	Ответственному за материально-техническое обеспечение сразу после инцидента	Ответственному за материально-техническое обеспечение в первый рабочий день после инцидента	1 час	2 дня
		Авария систем обеспечения	Ответственному за материально-	Ответственному за материально-	1 час	1 день

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
		ГИС «Сетевой город»	техническое обеспечение, Администратору сразу после обнаружения инцидента	техническое обеспечение, Администратору не позднее 8 часов после инцидента		
24.	Природные явления, стихийные бедствия, несущие угрозу жизни человека	-	Руководителю, заместителям руководителя, которые оповещают всех своих сотрудников сразу после получения информации	Руководителю, заместителям руководителя, которые оповещают всех своих сотрудников сразу после получения информации	10 минут	30 минут
25.	Природные явления, стихийные бедствия, не несущие угрозу жизни человека	-	Руководителю, заместителям Руководителя, Администратору	Руководителю, заместителям Руководителя, Администратору	10 минут	1 час

Приложение №9 к приказу
МАОУ «Средняя школа № 28
им. Г.Ф. Кирдищева»
от 27.09.2019 г. № 100 §1

ПЛАН МЕРОПРИЯТИЙ

по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город»

Контролирующие и периодические мероприятия

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
Документирование					
1.	Контроль наличия согласий на обработку персональных данных субъектов персональных данных, чьи ПДн обрабатываются в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»	Ответственный за организацию обработки ПДн	Вручную	Ежеквартально	
2.	Контроль наличия соглашений о неразглашении конфиденциальной информации, подписанных сотрудниками, допущенными к обработке такой информации	Ответственный за организацию обработки ПДн	Вручную	Ежеквартально	
3.	Контроль актуальности внутренней документации по защите информации, в том числе списков лиц, допущенных к обработке конфиденциальной информации	Ответственный за организацию обработки ПДн, Администратор безопасности	Вручную	Ежеквартально либо при существенном изменении законодательства в сфере защиты информации	
4.	Контроль наличия актуальных договоров с организациями, которым передаются персональные данные, а также наличия в этих договорах пунктов, регламентирующих	Ответственный за организацию обработки ПДн	Вручную	Каждые полгода	

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
	обязанность этих организаций обеспечивать конфиденциальность персональных данных				
5.	Пересмотр актуальных угроз безопасности и актуализация документа «Модель угроз безопасности информации»	Администратор безопасности	Вручную	Ежегодно, либо при изменении нормативной документации в сфере моделирования угроз безопасности информации, либо при поступлении информации о новых угрозах, актуальных для информационных систем МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»	
6.	Повторная аттестация пользовательского сегмента ГИС «Сетевой город»	Организация-лицензиат ФСТЭК России, привлекаемая для проведения аттестационных испытаний	Согласовываются в документе «Программа и методики аттестационных испытаний»	1 раз в 5 лет, либо при существенном изменении структурно-функциональных характеристик пользовательского сегмента ГИС «Сетевой город»	
Информирование и обучение персонала					
7.	Доведение до персонала информации о новых угрозах информационной безопасности	Администратор безопасности	Устные лекции, информирование по каналам электронной почты	Не реже 1 раза в месяц	

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
8.	Доведение до персонала положений законодательства в сфере защиты персональных данных	Ответственный за организацию обработки ПДн	Устные лекции, информирование по каналам электронной почты	Не реже 1 раза в квартал	
9.	Доведение до персонала положений внутренних нормативных документов по защите информации	Администратор безопасности, Ответственный за организацию обработки ПДн	Устно	По мере появления новых внутренних документов или по мере существенного изменения старых	
10.	Повышение квалификации и переподготовка лиц, ответственных за защиту информации в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» на курсах по направлению «Информационная безопасность» (не менее 72 часов)	Отдел кадров	Планирование учебных курсов	Не реже 1 раза в 5 лет	Учебные курсы должны быть согласованы со ФСТЭК России
11.	Проверка осведомленности персонала в сфере защиты информации	Администратор безопасности, Ответственный за организацию обработки ПДн	Устный опрос, письменное тестирование, имитация действий злоумышленника	Ежеквартально	
Физический контроль					
12.	Осмотр помещений на предмет несанкционированного доступа, нарушения пломб, физического	Администратор безопасности	Визуальный осмотр	Ежедневно	

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
	воздействия и внедрения неучтенных технических средств				
13.	Выборочный осмотр рабочих мест пользователей на предмет несанкционированного доступа, нарушения пломб, физического воздействия и внедрения неучтенных технических средств	Администратор безопасности	Визуальный осмотр	Ежедневно	
Тестирование работоспособности средств защиты информации					
14.	Контроль актуальности антивирусных баз	Администратор безопасности	Kaspersky Security Center	Ежедневно	
15.	Контроль корректной работы запрещающих правил межсетевого экрана	Администратор безопасности	Браузер, командная строка	Еженедельно	
16.	Контроль корректности разграничения прав доступа к ресурсам пользовательского сегмента ГИС «Сетевой город»	Администратор безопасности	ОС Windows, Secret Net Studio	Ежемесячно	
17.	Контроль корректной работы подсистемы гарантированного уничтожения информации	Администратор безопасности	Утилиты восстановления удаленной информации (R.Saver и аналоги)	Ежеквартально, либо при передаче учтенных съемных носителей между пользователями, либо при утилизации/передаче на ремонт технических средств с	

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
				машинными носителями информации	
Контроль программного обеспечения и технических средств ИС					
18.	Контроль отсутствия у пользователей на рабочих местах средств разработки и технологий интерпретации мобильного кода (кроме пользователей, которым это необходимо для выполнения своих должностных обязанностей)	Администратор безопасности	Ручной выборочный контроль	Ежемесячно	
19.	Контроль наличия необходимых обновлений безопасности общесистемного и прикладного программного обеспечения	Администратор безопасности	Ручной выборочный контроль	Еженедельно	
20.	Контроль отсутствия в пользовательском сегменте ГИС «Сетевой город» посторонних технических средств	Администратор безопасности, пользователи ГИС «Сетевой город»	Визуальный осмотр	Еженедельно	
21.	Контроль отсутствия в пользовательском сегменте ГИС «Сетевой город» неразрешенного программного обеспечения	Администратор безопасности	Вручную	Еженедельно	
Пользователи, учетные записи, парольная политика					
22.	Смена паролей доступа к интерфейсам управления сетевыми	Администратор безопасности	Вручную	Каждые 90 суток	

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
	устройствами (коммутаторами, маршрутизаторами)				

Приложение №10 к приказу
МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»
от 27.09.2019 г. № 100 §1

ПОЛОЖЕНИЕ
О ЗАЩИТЕ И ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ПОЛЬЗОВАТЕЛЬСКОМ СЕГМЕНТЕ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ КАМЧАТСКОГО КРАЯ «СЕТЕВОЙ ГОРОД»

СОДЕРЖАНИЕ

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Назначение и область действия документа

Настоящее Положение об обработке персональных данных в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город» (далее — Положение) определяет порядок сбора, хранения, передачи, использования, уничтожения и любых других видов обработки персональных данных субъектов персональных данных обрабатываемых в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город» (далее - ГИС «Сетевой город»).

Настоящее Положение разработано в соответствии с федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — Закон), постановлением Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Трудовым кодексом РФ.

Цель данного Положения – определение порядка обработки персональных данных субъектов персональных данных обрабатываемых в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город» в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» (далее — Организация).

Юридические и физические лица, в соответствии со своими полномочиями владеющие, получающие и использующие информацию о субъектах персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную, предусмотренную законодательством Российской Федерации, ответственность за нарушение правил обработки и защиты этой информации.

Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно до замены его новым Положением.

Все изменения в Положение вносятся приказом директора Организации.

Все сотрудники Организации, имеющие доступ к персональным данным субъектов персональных данных, в обязательном порядке должны быть ознакомлены с настоящим Положением под роспись для последующего его исполнения.

2 ОСНОВНЫЕ ПОНЯТИЯ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Термины и определения

Автоматизированная обработка персональных данных - обработка персональных данных с использованием средств вычислительной техники.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Атака – целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой криптосредством информации или с целью создания условий для этого.

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Безопасность объекта – состояние защищенности объекта от внешних и внутренних угроз.

Безопасность информации – состояние защищённости информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации.

Блокирование информации – временное прекращение сбора, систематизации, накопления, использования, распространения, информации, в том числе её передачи.

Доступ к информации – возможность получения информации и ее использования.

Жизненно важные интересы – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

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 – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информация – сведения (сообщения, данные) независимо от формы их представления.

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.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

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.

Контролируемая зона - это пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

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.

Модель угроз – перечень возможных угроз информации.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

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.

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

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.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому лицу (субъекту персональных данных).

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.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Уничтожение информации – действия, в результате которого невозможно восстановить содержание информации в информационной системе или в результате которых уничтожаются материальные носители информации.

Уполномоченное оператором лицо – лицо, которому на основании договора оператор поручает обработку персональных данных.

Целостность информации - способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2.2 Определение перечня персональных данных, обрабатываемых в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город»

Категории и перечень персональных данных обрабатываемых в Организации как с помощью средств автоматизации, так и без использования таких средств представлен в Перечне персональных данных обрабатываемых в государственной информационной системе Камчатского «Сетевой город».

Цели обработки персональных данных в Организации:

– формирования единого информационного пространства в сфере образования в Камчатском крае;

– повышения эффективности государственного и муниципального управления в сфере образования в Камчатском крае за счет использования современных информационных технологий;

– повышения качества оказания государственных и муниципальных услуг в сфере образования.

3 ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Общие принципы обработки

Обработка персональных данных должна осуществляться на основе принципа соответствия объема и характера обрабатываемых персональных данных, а также способов обработки персональных данных заявленным целям обработки персональных данных.

Сбор, накопление, хранение, изменение, использование и распространение, а также другие действия, понимаемые под обработкой персональных данных, могут осуществляться только при условии письменного согласия физического лица, за исключением случаев, предусмотренных Законом.

Обработка персональных данных осуществляется как с помощью средств автоматизации, так и без использования таких средств.

Правила обработки и защиты персональных данных без использования средств автоматизации установлены в соответствующем внутреннем документе МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева».

Правила обработки персональных данных в информационной системе персональных данных установлены в Инструкции администратора информационной безопасности и в Инструкции пользователя информационной системы персональных данных.

3.2 Порядок сбора, получения и хранения персональных данных

При сборе персональных данных Организация обязана предоставить физическому лицу (субъекту персональных данных) по его запросу информацию о целях, способах обработки персональных данных, сведения о лицах, имеющих доступ к персональным данным, перечень обрабатываемых персональных данных и источник их получения, сведения о сроках обработки и хранения персональных данных.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

Персональные данные субъектов персональных данных поступают в Организацию при заключении договора, подтверждаются оригиналами документов и хранятся в течение исполнения договорных обязательств.

Все персональные данные субъектов персональных данных следует получать непосредственно от него самого.

Если персональные данные субъектов персональных данных возможно получить только у третьей стороны, то субъект персональных данных должен быть

уведомлен об этом заранее и от него должно быть получено письменное согласие на получение его персональных данных у третьей стороны. Организация должна сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъектов персональных данных дать письменное согласие на их получение.

3.3 Передача персональных данных третьим лицам

Передача персональных данных третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных федеральным законом, не допускается. Данное ограничение не распространяется на обмен персональными данными субъектов персональных данных в порядке, установленном федеральными законами.

Передача персональных данных субъекта персональных данных в коммерческих целях без его письменного согласия исключается. Обработка персональных данных субъекта в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

Лица, получившие доступ к персональным данным субъекта, должны быть предупреждены о том, что эти данные могут быть использованы лишь в целях, для которых они переданы, и обязаны соблюдать это правило. Лица, получившие персональные данные, обязаны соблюдать режим конфиденциальности.

Передача или получение персональных данных осуществляются в соответствии с утвержденными Правилами рассмотрения запросов субъектов персональных данных или их представителей.

Персональные данные субъектов персональных данных передаются во внешние информационные системы:

– Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационнотехнологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» обеспечивает идентификацию и аутентификацию пользователей ГИС «Сетевой город»;

– Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг (функций)»;

– Федеральная государственная информационная система «Единая система межведомственного электронного взаимодействия»;

– Государственная информационная система Камчатского края «Региональная система межведомственного электронного взаимодействия Камчатского края»;

– Портал государственных и муниципальных услуг Камчатского края;

– Государственная информационная система Камчатского края «Многофункциональный центр»;

– Федеральная государственная информационная система, обеспечивающая ведение электронной очереди приема детей в дошкольные образовательные организации;

– Федеральный реестр сведений о документах об образовании и (или) квалификации, документах об обучении.

3.4 Трансграничная передача персональных данных

Трансграничная передача персональных данных Организацией не осуществляется.

Все технические средства обработки персональных данных (рабочие станции и сервера) находятся в пределах Российской Федерации.

3.5 Порядок уничтожения и блокирования персональных данных

Организация обязана прекратить обработку персональных данных и уничтожить их после достижения цели обработки или в случае отзыва субъектом персональных данных согласия на обработку, за исключением случаев, когда уничтожение противоречит федеральному законодательству, а также уведомить о своих действиях субъекта персональных данных и (или) уполномоченный орган. Во всех случаях предусмотрен срок уничтожения персональных данных – три рабочих дня.

В целях оперативной организации уничтожения персональных данных на бумажных носителях приказом Организации назначена комиссия по защите информации обрабатываемой в ГИС «Сетевой город», а также утверждена форма акта уничтожения персональных данных.

Персональные данные, обрабатываемые в ГИС «Сетевой город», удаляются путем стирания записи в базах данных администратором информационной безопасности Организации по запросу субъекта или при достижении целей обработки персональных данных.

Временное прекращение операций по обработке персональных данных (блокирование) должно возникать по требованию субъекта персональных данных при выявлении им недостоверности обрабатываемых сведений или неправомерных действий в отношении его данных.

3.6 Защита персональных данных

При обработке персональных данных Организация принимает организационные и технические меры для защиты персональных данных от неправомерных действий в соответствии с требованиями, устанавливаемыми Правительством РФ.

Защита персональных данных при неавтоматизированной их обработке регламентируется внутренним документом «Правила обработки персональных данных без использования средств автоматизации».

Защита персональных данных при их обработке в ГИС «Сетевой город» регламентирована Инструкцией администратора безопасности ГИС «Сетевой город», Инструкцией пользователя ГИС «Сетевой город» и другими внутренними документами Организации по защите информации.

Приказом Организации назначена комиссия по защите информации обрабатываемой в ГИС «Сетевой город».

В Организации разработана Модель угроз ГИС «Сетевой город» и Модель нарушителя. Проведена классификация ГИС «Сетевой город». Для ГИС «Сетевой город» сформировано Техническое задание на систему защиты информации, в котором описаны все организационные и технические меры, которые необходимо осуществить для нейтрализации актуальных угроз и выполнения требований действующего законодательства по защите персональных данных установленного уровня защищенности.

В Организации проведена аттестация ГИС «Сетевой город», подтвердившая в целом удовлетворительное состояние системы защиты персональных данных.

3.7 Согласие на обработку персональных данных

Со всех субъектов персональных данных Организации собирается согласие на обработку их персональных данных.

4 ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

4.1 Организация доступа работников к персональным данным субъектов

Должностные лица Организации должны иметь доступ только к тем персональным данным, которые необходимы им для выполнения своих функциональных обязанностей.

В Организации разработана и утверждена разрешительная система допуска к персональным данным (Положение о разграничении прав доступа к персональным данным). Круг лиц, допущенных к обработке персональных данных, определяет руководство Организации на основании данных, представленных руководителями подразделений, в которых ведется обработка персональных данных. Данный Перечень утверждается директором Организации.

Должностные лица Организации допускаются к обработке персональных данных после ознакомления с настоящим Положением, инструкцией пользователя ГИС «Сетевой город», а также с иной организационно-распорядительной документацией Организации по защите персональных данных.

Должностные лица Организации перед началом обработки персональных данных подписывают соглашение о неразглашении персональных данных.

Доступ должностных лиц к обработке персональных данных осуществляется в соответствии с Перечнем лиц, должностей, служб и процессов, допущенных к работе с персональными данными.

В случае обнаружения нарушений правил обработки персональных данных в Организации директор Организации и/или администратор безопасности информации и/или ответственный за организацию обработки персональных данных обязаны приостановить предоставление персональных данных пользователям до выявления и устранения причин нарушений.

Субъекты персональных данных имеют право на свободный бесплатный доступ к своим персональным данным, а также на получение копий любой записи о своих персональных данных, обрабатываемых в Организации.

Лица, не имеющие доступа к персональным данным в соответствии с Перечнем подразделений и сотрудников, допущенных к работе с персональными данными, могут быть допущены к ним на основании приказа, подписанного директором Организации либо руководителем подразделения данного лица.

4.2 Организация доступа субъекту персональных данных к его персональным данным

Организация, обрабатывающая персональные данные, должна обеспечивать бесплатный доступ субъекта к персональным данным, ему соответствующим, за

исключением случаев получения персональных данных в результате оперативно-розыскной деятельности, а также других случаев, предусмотренных федеральным законодательством.

Для получения доступа к своим персональным данным субъекту необходимо направить в Организацию запрос, содержащий паспортные данные субъекта персональных данных, в бумажной или электронной форме, подписанные собственноручно или квалифицированной электронной подписью.

Работники Организации должны предоставить персональные данные субъекту в доступной форме, в них не должны содержаться персональные данные, относящиеся к другим субъектам.

В случае если персональные данные субъекта являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, Организация обязана удовлетворить требование субъекта по устранению нарушений обработки персональных данных.

С целью организации своевременной обработки запросов и обращений субъектов персональных данных в Организации разработан и утвержден документ «Правила рассмотрения запросов субъектов персональных данных или их представителей».

5 ПРАВА И ОБЯЗАННОСТИ МАОУ «СРЕДНЯЯ ШКОЛА № 28 ИМ. Г.Ф. КИРДИЩЕВА»

5.1 Права и обязанности Организации

Организация имеет право осуществлять обработку персональных данных в законных и обоснованных целях, в том числе предоставлять персональные данные третьим лицам, если на это дано информированное согласие субъекта персональных данных или если это предусмотрено действующим законодательством.

В случае выявления недостоверных персональных данных или неправомерных действий с ними Организации при обращении или по запросу субъекта персональных данных или его законного представителя, либо уполномоченного органа по защите прав субъектов персональных данных, Организация обязана устранить допущенные нарушения или, в случае невозможности устранения, уничтожить персональные данные, а также уведомить о своих действиях субъекта персональных данных или уполномоченный орган.

Должностные лица Организации, в обязанность которых входит обработка запросов и обращений субъектов персональных данных, обязаны обеспечить каждому субъекту возможность ознакомления с документами и материалами, содержащими их персональные данные, если иное не предусмотрено законом, в соответствии с Правилами рассмотрения запросов субъектов персональных данных.

В случае предоставления субъектом неполных, устаревших, недостоверных или незаконно полученных персональных данных Организация обязана внести необходимые изменения, уничтожить или блокировать их, а также уведомить о своих действиях субъекта персональных данных.

Организация обязуется не принимать на основании исключительно автоматизированной обработки решения, порождающие юридические последствия в отношении субъектов персональных данных или иным образом затрагивающие их права и законные интересы.

По запросу уполномоченного органа по защите прав субъектов персональных данных Организация обязана предоставить ему необходимую информацию.

6 ПРАВА И ОБЯЗАННОСТИ РАБОТНИКОВ МАОУ «СРЕДНЯЯ ШКОЛА № 28 ИМ. Г.Ф. КИРДИЩЕВА»

6.1 Общие положения

Работники, допущенные к обработке персональных данных, обязаны ознакомиться с документами Организации, которые устанавливают порядок обработки персональных данных в Организации, и подписать лист ознакомления с ними, а также подписать соглашение о неразглашении персональных данных, полученных в ходе исполнения своих должностных обязанностей.

6.2 Права работника

В целях защиты персональных данных, хранящихся в Организации, работник, осуществляющий обработку персональных данных, имеет право:

– получать и вводить информацию в соответствии с его полномочиями;

– требовать оповещения Организацией субъекта персональных данных обо всех произведенных в них исключениях, исправлениях или дополнениях.

6.3 Обязанности работника

В части обработки персональных данных субъекта:

– соблюдать режим конфиденциальности;

– не сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия;

– не сообщать персональные данные субъекта третьей стороне без письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных федеральным законом;

– разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;

– не запрашивать дополнительную информацию, содержащую персональные данные, за исключением тех сведений, которые необходимы для достижения целей обработки персональных данных.

7 ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1 Получение сведений об Организации

Субъект персональных данных имеет право на получение сведений об Организации, о месте ее нахождения, о наличии у Организации персональных данных, относящихся к нему, а также на ознакомление с такими персональными данными. Субъект персональных данных вправе требовать от Организации уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

7.2 Доступ к своим персональным данным

Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю Организацией при обращении либо при получении запроса субъекта персональных данных или его законного представителя.

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

– подтверждение факта обработки персональных данных Организацией, а также цель такой обработки;

– способы обработки персональных данных, применяемые Организацией;

– сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

– перечень обрабатываемых персональных данных и источник их получения;

– сроки обработки персональных данных, в том числе сроки их хранения;

– сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

Если субъект персональных данных считает, что Организация осуществляет обработку его персональных данных с нарушением требований федерального законодательства или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Организации в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

7.3 Ограничение прав субъектов персональных данных

Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если:

1) обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) предоставление персональных данных нарушает конституционные права и свободы других лиц.

8 ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1 Общие положения

Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность за нарушение режима защиты, обработки и порядка использования этой информации.

Неправомерность деятельности органов государственной власти и организаций по сбору персональных данных может быть установлена в судебном порядке по требованию субъекта персональных данных, действующего на основании законодательства о персональных данных.

8.2 Персональная ответственность должностных лиц МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»

Должностные лица Организации, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность, предусмотренную федеральным законодательством.

Руководитель подразделения, разрешивший доступ должностному лицу к персональным данным несет персональную ответственность за данное решение.

Должностные лица Организации, получающие доступ к персональным данным несут персональную ответственность за обеспечение конфиденциальности предоставленной им информации. Кроме того, должностные лица Организации, получающие для работы документы, содержащие персональные данные, несут персональную ответственность за их сохранность.

В случае, когда нарушение конфиденциальности, целостности или доступности персональных данных повлекло за собой какие-либо финансовые потери для Организации, виновные должностные лица обязаны возместить причиненный ущерб.

Приложение №11 к приказу
МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»
от 27.09.2019 г. № 100 §1

Правила рассмотрения запросов субъектов персональных данных или их представителей, чьи персональные данные обрабатываются в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город»

1. Настоящими Правилами рассмотрения запросов субъектов персональных данных или их представителей, чьи персональные данные обрабатываются в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город» (далее – ГИС «Сетевой город») определяются порядок учета (регистрации), рассмотрения запросов субъектов персональных данных или их представителей (далее – запросы).

2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27 июля 2006 г. № 152 ФЗ «О персональных данных» (далее – Федеральный закон), Трудовым кодексом Российской Федерации, Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации» и другими нормативными правовыми актами.

3. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных (часть 7 статьи 14 Федерального закона), в том числе содержащей:

− подтверждение факта обработки персональных данных в ГИС «Сетевой город»;

− правовые основания и цели обработки персональных данных;

− цели и применяемые в ГИС «Сетевой город» способы обработки персональных данных;

8.3 наименование и место нахождения МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»

− (далее - Организация), сведения о лицах (за исключением работников Организации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании федерального закона;

− обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

− сроки обработки персональных данных, в том числе сроки их хранения;

− порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

− информацию об осуществленной или о предполагаемой трансграничной передаче данных;

− наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению руководителя, если обработка поручена или будет поручена такому лицу;

− иные сведения, предусмотренные Федеральным законом или другими федеральными законами.

4. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона, в том числе если:

− обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

− обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

− обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

− доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

− обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

5. Субъект персональных данных вправе требовать от Организации уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6. Сведения, указанные в части 7 статьи 14 Федерального закона, должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

7. Сведения, указанные в части 7 статьи 14 Федерального закона, предоставляются субъекту персональных данных или его представителю Организации при обращении либо при получении запроса субъекта персональных данных или его представителя.

8. Запрос должен содержать: номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя; сведения о дате выдачи указанного документа и выдавшем его органе; сведения, подтверждающие участие субъекта персональных данных в отношениях с Организацией (номер заявки на возврат, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Организацией; подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

9. Рассмотрение запросов является служебной обязанностью уполномоченных должностных лиц, в чьи обязанности входит обработка персональных данных.

10. Должностные лица Организации обеспечивают:

− объективное, всестороннее и своевременное рассмотрения запроса;

− принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;

− направление письменных ответов по существу запроса.

Ведение делопроизводства по запросам осуществляется назначенным сотрудником Организации.

Все поступившие запросы регистрируются в день их поступления. На запросе проставляется штамп, в котором указывается входящий номер и дата регистрации.

11. Запрос прочитывается, проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской. В случае если сведения, указанные в части 7 статьи 14 Федерального закона № 152-ФЗ, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Организацию или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Субъект персональных данных вправе обратиться повторно в Организацию или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона № 152-ФЗ, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в настоящем пункте, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения

первоначального обращения. Повторный запрос наряду с необходимыми сведениями должен содержать обоснование направления повторного запроса.

12. Организация вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона № 152-ФЗ. Такой отказ должен быть мотивированным.

13. Прошедшие регистрацию запросы в тот же день докладываются директору Организации либо лицу, его заменяющему, который определяет порядок и сроки их рассмотрения, дает по каждому из них письменное указание исполнителям.

14. Директор Организации, и другие должностные лица при рассмотрении и разрешении запроса обязаны:

− внимательно разобраться в их существе, в случае необходимости истребовать дополнительные материалы или направить сотрудников на места для проверки фактов, изложенных в запросах, принять другие меры для объективного разрешения поставленных заявителями вопросов, выявления и устранения причин и условий, порождающих факты нарушения законодательства о персональных данных;

− принимать по ним законные, обоснованные и мотивированные решения и обеспечивать своевременное и качественное их исполнение;

− сообщать в письменной форме заявителям о решениях, принятых по их запросам, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса - разъяснять также порядок обжалования принятого решения.

15. Организация обязана сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

16. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя уполномоченные должностные лица Организации обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона № 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

17. Организация обязана предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

18. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, уполномоченные должностные лица Организации обязаны внести в них необходимые изменения.

19. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уполномоченные должностные лица Организации обязаны уничтожить такие персональные данные.

20. Организации обязана уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

21. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных уполномоченные должностные лица Организации обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения или получения указанного запроса на период проверки.

22. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных уполномоченные должностные лица Организации обязаны осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

23. В случае подтверждения факта неточности персональных данных уполномоченные должностные лица Организации на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязаны уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

24. В случае выявления неправомерной обработки персональных данных уполномоченные должностные лица Организации в срок, не превышающий трех рабочих дней с даты этого выявления, обязаны прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, уполномоченные должностные лица Организации в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязаны уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Организация обязана уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

25. Для проверки фактов, изложенных в запросах при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации.

26. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения сотрудниками Организации действия (бездействия), содержащего признаки административного правонарушения или состава преступления информация передается незамедлительно в правоохранительные органы. Результаты служебной проверки докладываются директору Организации.

27. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

28. Ответы на запросы печатаются на бланке установленной формы и регистрируются за теми же номерами, что и запросы.

29. Директор Организации осуществляет непосредственный контроль за соблюдением установленного законодательством и настоящими Правилами порядка рассмотрения запросов.

30. Директор Организации осуществляет контроль за работой с запросами и организацией их приема как лично, так и через своих заместителей. На контроль берутся все запросы.

31. При осуществлении контроля обращается внимание на сроки исполнения поручений по запросам и полноту рассмотрения поставленных вопросов, объективность проверки фактов, изложенных в запросах, законность и обоснованность принятых по ним решений, своевременность их исполнения и направления ответов заявителям.

32. Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

Приложение №1 К Правилам рассмотрения запросов субъектов персональных данных или их представителей

Сводная таблица действий в ответ запросы по персональным данным

№	Запрос	Действия	Срок	Ответ
I. Запрос Субъекта ПДн или его Представителя				
1.1.	Наличие ПДн	Подтверждение обработки ПДн	30 дней (согласно пункту 1 статьи 20 152-ФЗ)	Подтверждение обработки ПДн
		Отказ подтверждения обработки ПДн	30 дней (согласно пункту 2 статьи 20 152-ФЗ)	Уведомление об отказе подтверждения обработки ПДн
1.2.	Ознакомление с ПДн	Предоставление информации по ПДн	30 дней (согласно пункту 1 статьи 20 152-ФЗ)	1. Подтверждение обработки ПДн, а также правовые основания и цели такой обработки. 2. Способы обработки ПДн. 3. Сведения о лицах, которые имеют доступ к ПДн. 4. Перечень обрабатываемых ПДн и источник их получения. 5. Сроки обработки ПДн, в том числе сроки их хранения. 6. Информация об осуществленных или о предполагаемой трансграничной передаче. 7. Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу.

№	Запрос	Действия	Срок	Ответ
		Отказ предоставления информации по ПДн	30 дней (согласно пункту 2 статьи 20 152-ФЗ)	Уведомление об отказе предоставления информации
1.3.	Уточнение ПДн	Изменение ПДн	7 рабочих дней со дня предоставления уточняющих сведений (согласно пункту 3 статьи 20 152-ФЗ)	Уведомление о внесенных изменениях
		Отказ изменения ПДн		Уведомление об отказе изменения ПДн
1.4.	Уничтожение ПДн	Уничтожение ПДн	7 рабочих дней со дня предоставления сведений о незаконном получении ПДн или отсутствии необходимости ПДн для заявленной цели обработки (согласно пункту 3 статьи 20 152-ФЗ)	Уведомление об уничтожении
		Отказ уничтожения ПДн		Уведомление об отказе уничтожения ПДн
1.5.	Отзыв согласия на обработку ПДн	Прекращение обработки и уничтожение ПДн	30 дней (согласно пункту 5 статьи 21 152-ФЗ)	Уведомление о прекращении обработки и уничтожении ПДн
		Отказ прекращения обработки и уничтожения ПДн		Уведомление об отказе прекращения обработки и уничтожения ПДн
1.6.	Недостоверность ПДн Субъекта	Блокировка ПДн	С момента обращения Субъекта ПДН о недостоверности или с момента получения запроса на период проверки (согласно пункту 1 статьи 21 152-ФЗ)	Уведомление о внесенных изменениях
		Изменение ПДн	7 рабочих дней со дня предоставления уточненных сведений (согласно пункту 2 статьи 21 152-ФЗ)	
		Снятие блокировки ПДн		
		Отказ изменения ПДн		Уведомление об отказе изменения ПДн

№	Запрос	Действия	Срок	Ответ
1.7.	Неправомерность действий с ПДн Субъекта	Прекращение неправомерной обработки ПДн	3 рабочих дня (согласно пункту 3 статьи 21 152-ФЗ)	Уведомление об устранении нарушений
		Уничтожение ПДн в случае невозможности обеспечения правомерности обработки	10 рабочих дней (согласно пункту 3 статьи 21 152-ФЗ)	Уведомление об уничтожении ПДн
1.8.	Достижение целей обработки ПДн Субъекта	Прекращение обработки ПДн	30 дней (согласно пункту 4 статьи 21 152-ФЗ), если иное не предусмотрено договором с субъектом ПДн	Уведомление об уничтожении ПДн
		Уничтожение ПДн		
II. Запрос Уполномоченного органа по защите прав Субъекта ПДн				
2.1.	Информация для осуществления деятельности уполномоченного органа	Предоставление затребованной информации по ПДн	30 дней (согласно пункту 4 статьи 20 152-ФЗ)	Предоставление затребованной информации по ПДн
2.2.	Недостоверность ПДн Субъекта	Блокировка ПДн	С момента обращения Уполномоченного органа о недостоверности или с момента получения запроса на период проверки (согласно пункту 1 статьи 21 152-ФЗ)	Уведомление о внесенных изменениях
		Изменение ПДн	7 рабочих дней со дня предоставления уточненных сведений (согласно пункту 2 статьи 21 152-ФЗ)	
		Снятие блокировки ПДн		
		Отказ изменения ПДн		Уведомление об отказе изменения ПДн

№	Запрос	Действия	Срок	Ответ
2.3.	Неправомерность действий с ПДн Субъекта	Прекращение неправомерной обработки ПДн	3 рабочих дня (согласно пункту 3 статьи 21 152-ФЗ)	Уведомление об устранении нарушений
		Уничтожение ПДн в случае невозможности обеспечения правомерности обработки	10 рабочих дней (согласно пункту 3 статьи 21 152-ФЗ)	Уведомление об уничтожении ПДн
2.4.	Достижение целей обработки ПДн Субъекта	Блокировка ПДн	30 дней (согласно пункту 4 статьи 21 152-ФЗ), если иное не предусмотрено договором с субъектом ПДн	Уведомление об уничтожении ПДн
		Уничтожение ПДн		

Приложение № 2 К Правилам рассмотрения запросов субъектов персональных данных или их представителей

ФОРМЫ ОТВЕТА
на запрос субъекта персональных данных
о наличии и на ознакомление с ПД

Г-ну/Г-же _____
На Ваш запрос от «___» _____ 20___ г. относительно обработки Ваших персональных данных могу сообщить следующее.
МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» в период с «__» _____ 20__ г. по настоящее время обрабатывает следующие полученные от Вас персональные данные:
_____
_____
_____
с целью
_____
Эта информация обрабатывается в соответствии с законодательством РФ о персональных данных, в Ваших интересах и с Вашего согласия. Обработка данных включает хранение, использование и, в случае необходимости, передачу третьим сторонам. Обработкой Ваших персональных данных занимаются сотрудники МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева», ознакомленные с обязанностями, возложенными на них в связи с обработкой Ваших персональных данных, и давшие подписку об их неразглашении. Никто другой к обработке Ваших персональных данных не допускается. Ваши персональные данные будут обрабатываться вплоть до достижения указанных целей.
Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением,
_____ (должность)
_____ (ФИО)
тел. _____

(дата, подпись, печать МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»*)*

Г-ну/Г-же _____

На Ваш запрос от «____» _____ 20___ г. относительно обработки Ваших персональных данных могу сообщить следующее.
МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» не осуществляет обработки Ваших персональных данных.

С уважением,
_____ (должность)
_____ (ФИО)
тел. _____

(дата, подпись, печать МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»

Приложение № 3 К Правилам рассмотрения запросов субъектов персональных данных или их представителей

ФОРМЫ ОТВЕТА
на запрос субъекта персональных данных
на уточнение ПД

Г-ну/Г-же _____
На Ваш запрос от «____» _____ 20___ г. относительно уточнения Ваших персональных данных могу сообщить следующее.
МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» были внесены изменения в Ваши персональные данные:
_____
_____
_____
Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением,
_____ (должность)
_____ (ФИО)
тел. _____

(дата, подпись, печать МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»*)*

Г-ну/Г-же _____

На Ваш запрос от «____» _____ 20___ г. относительно уточнения Ваших персональных данных могу сообщить следующее.
МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» не может внести изменения в Ваши персональные данные, так как Вами не было предоставлено необходимые документы, подтверждающие запрашиваемые Вами изменения.

С уважением,
_____ (должность)
_____ (ФИО)
тел. _____

(дата, подпись, печать МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» *)*

Приложение № 4 К Правилам рассмотрения запросов субъектов персональных данных или их представителей

ФОРМЫ ОТВЕТА
на запрос субъекта персональных данных
на уничтожение ПД

Г-ну/Г-же _____
На Ваш запрос от «____» _____ 20___ г. относительно уничтожения Ваших персональных данных могу сообщить следующее.
МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» были уничтожены Ваши персональные данные:
_____
_____
_____

С уважением,
_____ (должность)
_____ (ФИО)
тел. _____

(дата, подпись, печать МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» *)*

Г-ну/Г-же _____

На Ваш запрос от «____» _____ 20___ г. относительно уничтожения Ваших персональных данных могу сообщить следующее.
МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» не может уничтожить Ваши персональные данные, так их обработка осуществляется согласно требованиям следующих законодательных актов:
_____
_____
_____
Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением,
_____ (должность)
_____ (ФИО)
тел. _____

(дата, подпись, печать МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»

Приложение № 5 К Правилам рассмотрения запросов субъектов персональных данных или их представителей

ФОРМЫ ОТВЕТА
на запрос субъекта персональных данных
с отзывом согласия на обработку ПД

Г-ну/Г-же _____

На Ваш запрос от «___» _____ 20___ г. относительно отзыва согласия на обработку Ваших персональных данных могу сообщить следующее.
МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» были прекращена обработка и уничтожены Ваши персональные данные:
_____
_____
_____

С уважением,
____ _____ (должность)
_____ (ФИО)
тел. _____

(дата, подпись, печать МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» *)*

Г-ну/Г-же _____

На Ваш запрос от «___» _____ 20___ г. относительно отзыва согласия на обработку Ваших персональных данных могу сообщить следующее.

МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» не может прекратить обработку и уничтожить Ваши персональные данные, так их обработка осуществляется согласно требованиям следующих законодательных актов:

_____

_____

_____

Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением,

_____ (должность)

_____ (ФИО)

тел. _____

(дата, подпись, печать МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» *)*

Приложение № 6 К Правилам рассмотрения запросов субъектов персональных данных или их представителей

ФОРМЫ УВЕДОМЛЕНИЯ
субъекта персональных данных,
его законного представителя или
уполномоченного органа
по защите прав субъектов персональных данных
при выявлении недостоверности ПДн

Г-ну/Г-же _____

В связи с выявлением недостоверности Ваших персональных данных (персональных данных г-на/г-жи _____) могу сообщить следующее.
МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» были внесены изменения в Ваши персональные данные (персональные данные г-на/г-жи _____):
_____
_____
_____
Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных (персональных данных г-на/г-жи _____), пожалуйста, обращайтесь.

С уважением,
_____ (должность)
_____ (ФИО)
тел. _____

(дата, подпись, печать МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» *)*

Г-ну/Г-же _____

На Ваш запрос от «___» _____ 20___ г. относительно недостоверности Ваших персональных данных (персональных данных г-на/г-жи _____) могу сообщить следующее.
МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» не может внести изменения в Ваши персональные данные (персональные данные г-на/г-жи _____), так как факт недостоверности не подтвержден и не было предоставлено необходимых документов, подтверждающих недостоверность персональных данных.
Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных (персональных данных г-на/г-жи _____), пожалуйста, обращайтесь.

С уважением,
_____ (должность)
_____ (ФИО)
тел. _____

(дата, подпись, печать МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»

Приложение № 7 К Правилам рассмотрения запросов субъектов персональных данных или их представителей

ФОРМЫ УВЕДОМЛЕНИЯ
субъекта персональных данных,
его законного представителя или
уполномоченного органа
по защите прав субъектов персональных данных
при выявлении неправомерности действий с ПДн

Г-ну/Г-же _____

В связи с выявлением неправомерности действий с Вашими персональными данными (персональными данными г-на/г-жи _____) могу сообщить следующее.
МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» были уничтожены Ваши персональные данные (персональные данные г-на/г-жи _____):
_____
_____
_____
Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных (персональных данных г-на/г-жи _____), пожалуйста, обращайтесь.

С уважением,
_____ (должность)
_____ (ФИО)
тел. _____

(дата, подпись, печать МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» *)*

Г-ну/Г-же _____

На Ваш запрос от «___» _____ 20___ г. относительно неправомерности действий с Вашими персональными данными (персональными данными г-на/г-жи _____) могу сообщить следующее.

МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» не может уничтожить Ваши персональные данные (персональные данные г-на/г-жи _____), так как факт неправомерности действий с Вашими персональными данными (персональными данными г-на/г-жи _____) не подтвержден и Вами не было предоставлено необходимых документов, подтверждающих неправомерность действий с Вашими персональными данными (персональными данными г-на/г-жи _____).

МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» осуществляет обработку Ваших персональных данных (персональных данных г-на/г-жи _____) согласно требованиям следующих законодательных актов:

_____

_____

_____

Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных (персональных данных г-на/г-жи _____), пожалуйста, обращайтесь.

С уважением,

_____ (должность)

_____ (ФИО)

тел. _____

(дата, подпись, печать МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» *)*

Приложение № 9 К Правилам рассмотрения запросов субъектов персональных данных или их представителей

ФОРМЫ УВЕДОМЛЕНИЯ
субъекта персональных данных,
его законного представителя или
уполномоченного органа
по защите прав субъектов персональных данных
при достижении целей обработки ПДн

Г-ну/Г-же _____

В связи с достижением целей обработки Ваших персональных данных (персональных данных г-на/г-жи _____) могу сообщить следующее.
МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» были прекращена обработка и уничтожены Ваши персональные данные (персональных данных г-на/г-жи _____):
_____
_____
_____
Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных (персональных данных г-на/г-жи _____), пожалуйста, обращайтесь.

С уважением,
_____ (должность)
_____ (ФИО)
тел. _____

(дата, подпись, печать МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» *)*

Г-ну/Г-же _____

На Ваш запрос от «____» _____ 20___ г. относительно достижения целей обработки Ваших персональных данных (персональных данных г-на/г-жи _____) могу сообщить следующее.

МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» не может прекратить обработку и уничтожить Ваши персональные данные (персональные данные г-на/г-жи _____), так как их обработка осуществляется согласно требованиям следующих законодательных актов:

_____

_____

_____

Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных (персональных данных г-на/г-жи _____), пожалуйста, обращайтесь.

С уважением,

_____ (должность)

_____ (ФИО)

тел. _____

(дата, подпись, печать МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» *)*

Приложение №12 к приказу
МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»
от 27.09.2019 г. № 100 §1

ПОЛИТИКА
МАОУ «СРЕДНЯЯ ШКОЛА № 28 им. Г.Ф. КИРДИЩЕВА» В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБРАБАТЫВАЕМЫХ В ПОЛЬЗОВАТЕЛЬСКОМ СЕГМЕНТЕ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ КАМЧАТСКОГО КРАЯ «СЕТЕВОЙ ГОРОД»

1. Общие положения

Обеспечение конфиденциальности и безопасности обработки персональных данных в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город» (далее – ГИС «Сетевой город») является одной из приоритетных задач организации.

В МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» для этих целей введен в действие комплект организационно-распорядительной документации, обязательный к исполнению всеми сотрудниками МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» , допущенными к обработке персональных данных.

Обработка, хранение и обеспечение конфиденциальности и безопасности персональных данных осуществляется в соответствии с действующим законодательством РФ в сфере защиты персональных данных, и в соответствии с локальными актами МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» .

Настоящая Политика определяет принципы, порядок и условия обработки субъектов персональных данных, чьи персональные данные обрабатываются в ГИС «Сетевой город», с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также устанавливает ответственность должностных лиц МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» , имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

Поскольку к настоящей Политике в соответствии с ч. 2 ст. 18.1 Федерального закона № 152-ФЗ «О персональных данных» необходимо обеспечить неограниченный доступ, в ней не публикуется детальная информация о принятых мерах по защите персональных данных в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева», а также иная информация, использование которой неограниченным кругом лиц может нанести ущерб МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» или субъектам персональных данных.

Основные понятия, используемые в политике:

– персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

– 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;

– обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя, в том числе:

– сбор;

– запись;

– систематизацию;

– накопление;

– хранение;

– уточнение (обновление, изменение);

– извлечение;

– использование;

– передачу (распространение, предоставление, доступ);

– обезличивание;

– блокирование;

– удаление;

– уничтожение.

– автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

– распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

– предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

– блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения 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;

– обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

– информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

– трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2. Понятие и состав персональных данных

Сведениями, составляющими персональные данные обрабатываемых в ГИС «Сетевой город», в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Перечень персональных данных обрабатываемых в ГИС «Сетевой город», подлежащих защите в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» определятся целями их обработки, Федеральным законом № 152-ФЗ «О защите персональных данных» и другими нормативно-правовыми актами.

В МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» утвержден перечень персональных данных подлежащих защите.

Категории и перечень персональных данных обрабатываемых в Организации как с помощью средств автоматизации, так и без использования таких средств представлен в Перечне персональных данных обрабатываемых в государственной информационной системе Камчатского «Сетевой город».

3. Цели сбора персональных данных

МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» осуществляет обработку персональных данных в следующих целях:

– формирования единого информационного пространства в сфере образования в Камчатском крае;

– повышения эффективности государственного и муниципального управления в сфере образования в Камчатском крае за счет использования современных информационных технологий;

– повышения качества оказания государственных и муниципальных услуг в сфере образования.

4. Правовые основания обработки персональных данных

Персональные данные МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» обрабатываются на основании:

– согласия на обработку персональных данных.

5. Сроки обработки персональных данных

Сроки обработки персональных данных определяются в соответствии со сроком действия договора (соглашением) с субъектом персональных данных, Приказом Минкультуры РФ от 25.08.2010 № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», сроком исковой давности, а также иными требованиями законодательства РФ.

В МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» создаются и хранятся документы, содержащие сведения о субъектах персональных данных. Требования к использованию в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» данных типовых форм документов установлены Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

6. Права и обязанности

МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» как оператор персональных данных в праве:

– отстаивать свои интересы в суде;

– предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);

– отказывать в предоставлении персональных данных в случаях предусмотренных законодательством;

– использовать персональные данные субъекта без его согласия, в случаях предусмотренных законодательством.

МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» как оператор персональных данных обязан:

– обеспечить каждому субъекту персональных данных возможность ознакомления с документами и материалами, содержащими их персональные данные, если иное не предусмотрено законом;

– внести необходимые изменения, уничтожить или блокировать персональные данные в случае предоставления субъектом неполных, устаревших, недостоверных или незаконно полученных персональных данных, а также уведомить о своих действиях субъекта персональных данных;

– выполнять требования законодательства Российской Федерации.

Субъект персональных данных имеет право:

– требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

– требовать перечень своих персональных данных, обрабатываемых МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» и источник их получения;

– получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;

– требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

– обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных.

Субъект персональных данных обязан:

– передавать достоверные, необходимые для достижения целей обработки, персональные данные, а также подтверждать достоверность персональных данных предъявлением оригиналов документов;

– в случае изменения персональных данных, необходимых для достижения целей обработки, сообщить МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» уточненные персональные данные и подтвердить изменения оригиналами документов;

– выполнять требования законодательства Российской Федерации.

7. Порядок и условия обработки персональных данных

МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» осуществляет как автоматизированную, так и неавтоматизированную обработку персональных данных.

Под обработкой персональных данных в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» понимается сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Персональные данные субъектов персональных данных передаются во внешние информационные системы:

– Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационнотехнологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» обеспечивает идентификацию и аутентификацию пользователей ГИС «Сетевой город»;

– Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг (функций)»;

– Федеральная государственная информационная система «Единая система межведомственного электронного взаимодействия»;

– Государственная информационная система Камчатского края «Региональная система межведомственного электронного взаимодействия Камчатского края»;

– Портал государственных и муниципальных услуг Камчатского края;

– Государственная информационная система Камчатского края «Многофункциональный центр»;

– Федеральная государственная информационная система, обеспечивающая ведение электронной очереди приема детей в дошкольные образовательные организации;

– Федеральный реестр сведений о документах об образовании и (или) квалификации, документах об обучении.

– Оператор вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

Обработка персональных данных в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» производится на основе соблюдения принципов:

– законности целей и способов обработки персональных данных;

– соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;

– соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

– достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

– недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;

– хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки;

– уничтожения по достижении целей обработки персональных данных или в случае утраты необходимости в их достижении.

Отказ субъекта персональных данных МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» от предоставления согласия на обработку его персональных данных влечет за собой невозможность достижения целей обработки.

8. Обеспечение безопасности персональных данных

МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» предпринимает необходимые организационные и технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.

В МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» для обеспечения безопасности персональных данных приняты следующие меры:

– назначено лицо, ответственное за организацию обработки персональных данных;

– назначен администратор безопасности информационной системы персональных данных;

– утверждены документы, определяющие политику МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» в отношении обработки персональных данных и устанавливающие процедуры направленные на предотвращение и выявление нарушений законодательства. К таким документам в частности относятся:

– положение о защите и обработке персональных данных в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город»;

– правила рассмотрения запросов субъектов персональных данных или их представителей, чьи персональные данные обрабатываются в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город»;

– перечень лиц, допущенных к обработке персональных данных в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город»;

– перечень лиц, допущенных к обработке персональных данных субъектов персональных данных, чьи персональные данные обрабатываются в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город» без использования средств автоматизации»;

– правила обработки персональных данных обрабатываемых в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город» без использования средств автоматизации;

– инструкция администратора безопасности в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город»;

– инструкция ответственного за организацию обработки персональных данных в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город»;

– инструкция по реагированию на инциденты информационной безопасности в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город»;

– положение о контролируемой зоне пользовательского сегмента государственной информационной системы Камчатского края «Сетевой город;

– инструкция пользователя пользовательского сегмента государственной информационной системы Камчатского края «Сетевой город»;

– политика информационной безопасности пользовательского сегмента государственной информационной системы Камчатского края «Сетевой город»;

– план мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город»;

– устранение последствий нарушений законодательства РФ производится в соответствии с действующим законодательством РФ, в соответствии с положением об обработке и защите персональных данных, а также в соответствии с инструкцией администратору безопасности персональных данных;

– внутренний контроль соответствия обработки персональных данных законодательству РФ в данной сфере производится в соответствии с планом внутренних проверок, инструкцией администратора безопасности и положением об обработке и защите персональных данных;

– для ГИС «Сетевой город» разработана модель угроз безопасности персональных данных, в которой при определении опасности угроз проводится оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства;

– для ГИС «Сетевой город» разработано техническое задание на создание системы защиты информации;

– проведена оценка эффективности принимаемых мер по обеспечению безопасности персональных данных;

– правила доступа к персональным данным утверждены в соответствующем положении, технически реализуются с помощью средств защиты информации;

– сотрудники, допущенные к обработке персональных данных, проходят инструктажи по информационной безопасности, подписывают соглашение о неразглашении персональных данных, знакомятся с документами по защите персональных данных под роспись.

9. Заключительные положения

К настоящей Политике обеспечивается неограниченный доступ.

Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года.

Контроль исполнения требований настоящей Политики осуществляется ответственным за организацию обработки персональных данных МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева».

Ответственность должностных лиц МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»

Приложение №13 к приказу
МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»
от 27.09.2019 г. № 100 §1

Правила обработки персональных данных обрабатываемых в пользовательском сегменте государственной информационной системе Камчатского края «Сетевой город» без использования средств автоматизации

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Обработка персональных данных считается осуществленной без использования средств автоматизации (неавтоматизированной), если обработка персональных данных осуществляется без помощи средств вычислительной техники.

1.2. Категории обрабатываемых персональных данных и категории субъектов персональных данных, а также цели обработки персональных данных указаны в утвержденном положении о защите и обработке персональных данных.

1.3. В МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева» (далее - Организация) не обрабатываются биометрические и специальные категории персональных данных.

1.4. Обработка персональных данных без использования средств автоматизации осуществляется на законной и справедливой основе. Обработка персональных данных без использования средств автоматизации не может быть использована Организацией или его работниками в целях причинения материального и морального вреда субъектам персональных данных, затруднения реализации их прав и свобод.

1.5. Настоящие правила обработки персональных данных без использования средств автоматизации (далее – Правила) разработаны и утверждены в целях обеспечения безопасности персональных данных, обрабатываемых в Организации без использования средств автоматизации, и исполнения требований Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.

1.6. Настоящие Правила являются внутренним локальным актом Организации, вступают в силу с момента их утверждения директором Организации и действуют бессрочно до их замены новым документом.

1.7. Все работники Организации, допущенные к неавтоматизированной обработке персональных данных, должны быть ознакомлены с настоящими Правилами под роспись.

1.8. Ответственность за актуализацию настоящих Правил и контроль над выполнением настоящих Правил возлагаются на назначенного директором Организации ответственного за организацию обработки персональных данных.

2. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

2.1. Категории и перечень персональных данных обрабатываемых в Организации без использования средств автоматизации представлен в Перечне персональных данных обрабатываемых в государственной информационной системе Камчатского «Сетевой город».

2.2. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

2.3. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

2.4. К обработке персональных данных без использования средств автоматизации допущены только те работники, которые указаны в утвержденных в Организации перечнях лиц, допущенных к обработке персональных данных без использования средств автоматизации.

2.5. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, подписывают соглашение о неразглашении персональных данных.

2.6. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

– типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с

персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых способов обработки персональных данных;

– типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

– типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

– типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

2.7. Журналы (реестры, книги), содержащие персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию Организации, не ведутся.

2.8. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

– при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

– при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

2.9. Для уничтожения персональных данных на материальных носителях в Организации утвержден состав комиссии по уничтожению персональных данных, а также утверждена форма уничтожения персональных данных.

2.10. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается

техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

3.1. С целью обеспечения безопасности персональных данных при их обработке без использования средств автоматизации приказом директора Организации определены места хранения персональных данных, а также назначены ответственные за обеспечение конфиденциальности персональных данных при их хранении.

3.2. Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях (разные места хранения для разных категорий субъектов персональных данных).

3.3. При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, определены в Положении о защите и обработке персональных данных в МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева».

Приложение №14 к приказу
МАОУ «Средняя школа № 28 им. Г.Ф. Кирдищева»
от 27.09.2019 г. № 100 §1

Перечень персональных данных обрабатываемых в государственной информационной системе Камчатского края «Сетевой город»

В государственной информационной системе Камчатского «Сетевой город» (далее – ГИС «Сетевой город) обрабатываются следующие категории персональных данных:

- ПДн учащихся в организациях общего образования (далее - ООО);
- ПДн родителей/законных представителей учащихся (ООО);
- ПДн сотрудников (ООО).

В ГИС «Сетевой город» обрабатываются следующие категории данных учащихся (ООО):

- Фамилия;
- Имя;
- Отчество;
- Дата рождения;
- Пол;
- Гражданство;
- Имя на экране;
- Имя пользователя;
- Учетная запись Windows;
- Документы, удостоверяющие личности (тип документа, серия, номер, дата выдачи, кем выдан, номер актовой записи);

– Личные достижения;
– Адрес проживания;
– Адрес регистрации;
– Домашний телефон;
– Мобильный телефон;
– Предпочтительный способ связи;
– E-mail;
– Родители;
– Иностранный язык;
– Второй иностранный язык;
– ИНН;
– Группа здоровья (для детей до 18 лет);
– Группа здоровья (для детей старше 18 лет);
– Физ. Группа;
– Заболевания;
– Движение;
– № личного дела;
– Психолого-педагогическая характеристика;
– Дополнительная контактная информация;
– Наличие ПК дома;
– Медицинский полис (серия, № полиса, дата выдачи, организация, выдавшая мед.полис);
– Состав семьи;
– Социальное положение;
– Сертификат доп. Образования (номер, дата выдачи);
– Дополнительное образование;
– Творческие объединения;

– Девиантное поведение;
– Бросил обучение;
– Форма обучения;
– Программа обучения;
– Предметы для ЕГЭ;
– Предметы для ЕГЭ по сокр. программе;
– Тип документа для ЕГЭ;
– Тип ограничения возможностей здоровья;
– Решение комиссии;
– Льгота на питание;
– СНИЛС;
– Малочисленные народы Севера;
– Финансирование обучения (тип);
– Инвалидность (группа инвалидности);
– Место рождения;
– Отказ от предоставления ПДн;
– Горячее питание;
– Нуждается в подвозе к месту обучения;
– Обеспечен подвоз к месту обучения;
– Прикреплённые файлы;
– Комментарий.

В ГИС «Сетевой город» обрабатываются следующие категории данных родителей/законных представителей учащихся (ООО):

– Фамилия;
– Имя;
– Отчество;

– Дата Рождения;
– Пол;
– Гражданство;
– Имя на экране;
– Имя пользователя;
– Учетная запись Windows;
– Документы, удостоверяющие личность (тип документа, серия, номер, дата выдачи, кем выдан, номер актовой записи);
– Личные достижения;
– Адрес проживания;
– Адрес регистрации;
– Домашний телефон;
– Мобильный телефон;
– Предпочтительный способ связи;
– E-mail;
– Дети;
– Степень родства;
– Образование;
– Место работы;
– Должность;
– Рабочий адрес;
– Рабочий телефон;
– Факс;
– Помощь школе;
– Дата и результат обращения за помощью;
– Заявитель на льготу;

– СНИЛС;
– Малочисленные народы Севера.
– Тип законного представителя;
– Документ законного представителя (тип, серия, номер, выдано, дата выдачи);
– Отказ от предоставления ПДн;
– Прикреплённые файлы;
– Комментарий.

В ГИС «Сетевой город» обрабатываются следующие категории данных сотрудников (ООО):

– Фамилия;
– Имя;
– Отчество;
– Дата Рождения;
– Пол;
– Гражданство;
– Имя на экране;
– Имя пользователя;
– Учетная запись Windows;
– Функции пользователя;
– Преподаваемые предметы;
– Документы, удостоверяющие личность (тип документа, серия, номер, дата выдачи, кем выдан, номер актовой записи);
– Личные достижения;
– Адрес проживания;
– Адрес регистрации;
– Домашний телефон;
– Мобильный телефон;

– Предпочтительный способ связи;
– E-mail;
– Табельный №;
– Учебная деятельность (тема самообразования, технология обучения);
– Дата приема на работу и № приказа (№ приказа, дата приказа, дата приема);
– Основная должность (должность, категория, дата последней аттестации);
– Заявка на аттестацию по основной должности (дата аттестации, категория);
– Дополнительная должность;
– Заявка на аттестацию по дополнительной должности (дата аттестации, категория);
– Трудовой стаж, лет, месяцев, дней (общий стаж, педагогический стаж, непрерывный стаж, стаж в занимаемой административной должности, стаж в занимаемой преподавательской должности, стаж в данном учреждении, территориальный стаж);
– Семейное положение;
– Состав семьи;
– ИНН;
– СНИЛС;
– Награды;
– Образование;
– Категория работника;
– Подразделение;
– Наличие ПК дома;
– Декретный отпуск;
– Дата выхода на пенсию;
– Малочисленные народы Севера;
– Воинский учет (звание, годность, запас, состав, номер военного билета, имеет военную подготовку, состоит на специальном учете, наименование отдела ОВК, дата начала службы, дата окончание службы);

– Предыдущее место работы;
– Иностранный язык;
– Второй иностранный язык;
– Рабочий телефон;
– Является экспертом ГАК;
– Прикреплённые файлы;
– Комментарий.