ПРИКАЗ

«16» сентября 2019 г. №9/20

О защите информации, содержащейся в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город» (Сегмент № 211)

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 старшего воспитателя Пастушенко И.А.

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 МБДОУ «Детский сад №12 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 старшего воспитателя Пастушенко И.А.

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 МБДОУ «Детский сад №12» 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:

– Хилобокая С.Я. - заведующая

– Пастушенко И.А. старший воспитатель

– Прохорова Е.А. - заведующий хозяйством

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 старшего воспитателя Пастушенко И.А.

19. К работе с СКЗИ допускать только пользователей (далее – Пользователи), прошедших предварительное обучение работе с СКЗИ согласно перечню сотрудников МБДОУ «Детский сад №12» допущенных к работе с СКЗИ в пользовательском сегменте государственной информационной системы Камчатского края «Сетевой город».

20. Определить в качестве мест хранения персональных данных в архивном шкафу в методическом кабинете МБДОУ «Детский сад №12» Ответственным за соблюдение конфиденциальности персональных данных при их хранении назначить старшего воспитателя Пастушенко И.А.

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 МБДОУ «Детский сад №12» 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 МБДОУ «Детский сад №12», 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.

И.о.заведующий «Детский сад № 12 присмотра и оздоровления» И.А. Пастушенко

Приложение №8 к приказу
МБДОУ «Детский сад №12»
от 16.09.2019 г. № 9/20

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 МБДОУ «Детский сад №12» и определяет мероприятия, процедуры и правила по защите информации в информационных системах МБДОУ «Детский сад №12»

1.2. Положения настоящей Политики распространяются на пользовательский сегмент государственной информационной системы Камчатского края «Сетевой город» (далее – ГИС «Сетевой город») принадлежащий МБДОУ «Детский сад №12»МБДОУ «Детский сад №12».

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 МБДОУ «Детский сад №12» 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 МБДОУ «Детский сад №12». 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 МБДОУ «Детский сад №12»:

– пользовательский сегмент ГИС «Сетевой город» состоит из 1 автоматизированного рабочего места. 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 МБДОУ «Детский сад №12», 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 МБДОУ «Детский сад №12» 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 МБДОУ «Детский сад №12» 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 МБДОУ «Детский сад №12».

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 МБДОУ «Детский сад №12» 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. МБДОУ «Детский сад №12» 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;

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 МБДОУ «Детский сад №12» 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 МБДОУ «Детский сад №12» 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 МБДОУ «Детский сад №12» 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 МБДОУ «Детский сад №12» 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 МБДОУ «Детский сад №12» 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 МБДОУ «Детский сад №12».

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 заведующей МБДОУ «Детский сад №12», 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 МБДОУ «Детский сад №12», 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 МБДОУ «Детский сад №12» от 16.09.2019 г. № 9/20

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.