Кемеровская область-Кузбасс
Тяжинский муниципальный округ
Администрация Тяжинского муниципального округа

ПОСТАНОВЛЕНИЕ

от 22.12.2022 г. № 330-п

Об утверждении Политики информационной безопасности в администрации Тяжинского муниципального округа

В целях исполнения Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», руководствуясь Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», Приказом ФСТЭК России от 11.02.2013 N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Уставом Тяжинского муниципального округа:

1. Утвердить Политику информационной безопасности в администрации Тяжинского муниципального округа согласно приложению.
2. Постановление вступает в силу со дня его обнародования, путем вывешивания на информационных стендах в зданиях администрации Тяжинского муниципального округа и территориальных отделов, входящих в состав Управления по жизнеобеспечению и территориальному развитию Тяжинского муниципального округа администрации Тяжинского муниципального округа.
3. Контроль за исполнением настоящего постановления возложить на заместителя главы Тяжинского муниципального округа – управляющего делами.

Глава Тяжинского муниципального округа В.Е. Серебров

Панкратов Александр Александрович
тел:28-1-92

Приложение

Утверждена
Постановлением администрации
Тяжинского муниципального округа
от «___»_____2022г. № ____

Политика информационной безопасности в администрации Тяжинского муниципального округа

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая политика информационной безопасности в администрации Тяжинского муниципального округа (далее - Политика) утверждается постановлением администрации Тяжинского муниципального округа и определяет мероприятия, процедуры и правила по защите информации в информационных системах администрации Тяжинского муниципального округа (далее – Администрация).

1.2. Положения настоящей Политики распространяются на все информационные системы Администрации, связанные с обработкой и хранением персональных данных.

1.3. Положения настоящей Политики обязательны к исполнению для всех пользователей информационных систем (далее - Пользователи), а также для администраторов безопасности и системных администраторов (далее - Администраторы).

1.4. В соответствии с указом Президента Российской Федерации № 188 от 6 марта 1997 года к сведениям конфиденциального характера (защищаемой информации) в Администрации:

- 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;
- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);
- служебные сведения, доступ к которым ограничен органами местного самоуправления в соответствии с Гражданским кодексом Российской Федерации, Федеральным законом от 09.02.2009 N 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» и иными федеральными законами;
- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

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.

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 Администрации. Администраторы и Пользователи, допущенные к обработке той или иной защищаемой информации, обязаны производить обработку этой информации в соответствии с соответствующими описаниями технологических процессов обработки информации, приведенных в данном разделе.

2.2. Технологический процесс обработки персональных данных сотрудников Администрации.

2.2.1. Персональные данные следует получать непосредственно у субъекта, либо у законного представителя.

2.2.2. Перед началом обработки персональных данных необходимо получить у субъекта или его законного представителя согласие на обработку персональных данных в письменной форме, в соответствии с утвержденной в Администрации формой такого Согласия.

2.2.3. Информация, представляемая сотрудником при поступлении на работу, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

1) паспорт или иной документ, удостоверяющий личность;

2) трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или сотрудник поступает на работу на условиях совместительства, либо трудовая книжка у сотрудника отсутствует в связи с ее утратой или по другим причинам;

3) страховое свидетельство государственного пенсионного страхования;

4) документы воинского учета – для военнообязанных и лиц, подлежащих воинскому учету;

5) документ об образовании, о квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки;

6) свидетельство о присвоении ИНН (при его наличии у сотрудника).

2.2.4. При заключении муниципального контракта в соответствии со ст. 16 Федерального закона от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации» (далее – ФЗ № 25) лицо, поступающее на работу, предъявляет работодателю:

1) заявление с просьбой о поступлении на муниципальную службу и замещении должности муниципальной службы по форме, утвержденной в Администрации;

2) собственноручно заполненную и подписанную анкету по форме, установленной уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти;

3) паспорт;

4) трудовую книжку и (или) сведения о трудовой деятельности, оформленные в установленном законодательством порядке, за исключением случаев, когда контракт заключается впервые;

5) документ об образовании;

6) документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета, за исключением случаев, когда контракт заключается впервые;

7) свидетельство о постановке физического лица на учет в налоговом органе по месту жительства на территории Российской Федерации;

8) документы воинского учета - для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу;

9) заключение медицинской организации об отсутствии заболевания, препятствующего поступлению на муниципальную службу;

10) сведения о доходах за год, предшествующий году поступления на муниципальную службу, об имуществе и обязательствах имущественного характера;

11) сведения, предусмотренные статьей 15.1 ФЗ № 25;

2.2.5. А также лицо, поступающее на работу, предъявляет работодателю:

1) свидетельство о заключении брака;

2) свидетельство о рождении ребенка;

3) фотографию;

4) заявление на медицинский полис;

5) автобиографию;

6) удостоверения, награды, медали;

7) сертификаты о повышении квалификации, прохождении курсов, тренингов.

8) водительское удостоверение (при необходимости);

9) сведения о лицевом счете в банке.

2.2.6. При оформлении сотрудника в Администрацию сотрудниками, отвечающими за кадровую работу (далее - отдел кадров) заполняется унифицированная форма Т-2 «Личная карточка работника» или Т-2 ГС (МС) «Личная карточка муниципального служащего».

2.2.7. В дальнейшем муниципальные служащие заполняют справку о доходах, расходах, об имуществе и обязательствах имущественного характера.

2.2.8. Часть информации копируется в соответствующую информационную систему.

2.2.9. В отделе кадров Администрации создаются и хранятся следующие группы документов, содержащие персональные данные сотрудников в единичном или сводном виде:

1) документы, содержащие персональные данные сотрудников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении;

2) комплекс материалов по анкетированию, тестированию;

3) проведению собеседований с кандидатом на должность;

4) подлинники и копии приказов по личному составу; личные дела и трудовые книжки сотрудников;

5) дела, содержащие материалы аттестации сотрудников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы);

6) подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Администрации, руководителям структурных подразделений;

7) копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения);

8) документация по работе отделов (регламенты, положения, должностные инструкции сотрудников, приказы Администрации, постановления и распоряжения Администрации);

9) документы по планированию, учету, анализу и отчетности в части работы с персоналом.

2.2.10. Материалы дела хранятся в течение трех лет, затем передаются в архив.

2.3. Технологический процесс обработки персональных данных соискателей на вакантные должности в Администрации:

2.3.1. Обработка персональных данных соискателей на замещение вакантных должностей предполагает получение согласия соискателей на замещение вакантных должностей на обработку их персональных данных на период принятия работодателем решения о приеме либо отказе в приеме на работу.

Исключение составляют случаи, когда от имени соискателя действует кадровое агентство, с которым данное лицо заключило соответствующий договор, а также при самостоятельном размещении соискателем своего резюме в Интернете, доступного неограниченному кругу лиц.

2.3.2. В случае получения резюме соискателя по каналам электронной почты, факсимильной связи сотрудник, ответственный за прием и регистрацию входящей почты дополнительно проводит мероприятия, направленные на подтверждение факта направления указанного резюме самим соискателем:

1) приглашение соискателя на личную встречу с уполномоченными сотрудниками работодателя;

2) обратная связь посредством электронной почты;

3) иные мероприятия, не противоречащие законодательству РФ.

2.3.3. При поступлении в адрес работодателя резюме, составленного в произвольной форме, при котором однозначно определить физическое лицо, его направившее, не представляется возможным, данное резюме подлежит уничтожению в день поступления.

2.3.4. В случае если сбор персональных данных соискателей осуществляется посредством типовой формы анкеты соискателя, утвержденной работодателем, то данная типовая форма анкеты должна соответствовать требованиям:

1) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, 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 оператором способов обработки персональных данных;

2) 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;

в) 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;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

А также содержать информацию о сроке ее рассмотрения и принятия решения о приеме либо отказе в приеме на работу.

2.3.5. Типовая форма анкеты соискателя может быть реализована в электронной форме на сайте Администрации, где согласие на обработку персональных данных подтверждается соискателем путем проставления отметки в соответствующем поле, за исключением случаев, когда работодателем запрашиваются сведения, предполагающие получение согласия в письменной форме.

3. ПРАВИЛА И ПРОЦЕДУРЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ, ПОЛИТИКА РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ ИНФОРМАЦИОННЫХ СИСТЕМ

3.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику Администрации, допущенному к работе с ресурсами, информационной системой присваивается уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в информационной системе.

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 информационных системах запрещено.

3.4. Для администратора безопасности, для системных администраторов, для удаленных пользователей (пользователей, работающих с ресурсами информационных систем через внешние телекоммуникационные сети, но являющихся сотрудниками Администрации, для внешних пользователей (пользователей, не являющихся сотрудниками информационных систем) предусмотрена двухфакторная аутентификация в информационных системах.

3.5. Процедура регистрации (создания учетной записи и выдачи при необходимости электронного ключа) пользователя для сотрудника Администрации, и предоставления ему (или изменения его) прав доступа к ресурсам информационных систем инициируется заявкой руководителя подразделения, в

котором работает этот сотрудник. Форма заявки приведена в Приложении № 1 к настоящей Политике. В заявке указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам информационных систем ранее зарегистрированного пользователя);
- должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач);
- заявку визирует администратор безопасности, утверждая тем самым возможность допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных задач ресурсам информационных систем.

3.6. Администратор перед визированием заявки осуществляет верификацию пользователя (подтверждает его личность), а также уточняет его должностные и функциональные обязанности и сопоставляет их с технологическими процессами обработки информации, описанным в разделе 2 настоящей Политики. Допуск Пользователей к обработке информации в информационных системах производится на основании завизированной Администратором заявки, составленной по форме, приведенной в Приложении № 1 к настоящей Политике. При визировании очередной заявки Администратор осуществляет актуализацию следующих документов:

- уровень прав доступа в положении о разграничении прав доступа в информационной системе (при необходимости, Приложение № 2 к настоящей Политике);
- перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами, по форме, приведенной в Приложение № 3 к настоящей Политике. Перечень утверждается (изменяется) распоряжением Администрации.

3.7. После визирования заявки Администратор определяет тип учетной записи (внутренний пользователь, внешний пользователь, системная, учетная запись приложения, временная, гостевая) и производит необходимые настройки СЗИ от НСД и формирует учетную запись, персональный идентификатор и первичный пароль. Дает ознакомиться с инструкцией Пользователя под роспись, сообщает пользователю идентификационные данные и допускает к работе. После допуска к работе, Пользователь самостоятельно формирует пароль доступа к своей учетной записи в соответствии с требованиями раздела 3 Инструкции Пользователя.

3.8. В информационных системах Администрации для учетных записей Пользователей, процессов, приложений, гостевых и временных учетных записей разрешен только один параллельный сеанс доступа к ресурсам. Для привилегированных учетных записей (администратор безопасности и системные администраторы) разрешено не более двух параллельных сеансов доступа к ресурсам с разных устройств. Настройка разрешения параллельных сеансов доступа к ресурсам осуществляется Администратором путем указания соответствующих параметров.

3.9. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания. Исполненная заявка хранится у Администратора и может быть использована для восстановления полномочий пользователей после сбоев в работе информационных систем, а также для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам при разборе инцидентов безопасности.

3.10. Для проведения временных работ в информационных системах сотрудниками сторонних организаций предусмотрена гостевая временная учетная запись «Гость». Данная учетная запись отключена и активируется (наделяется необходимыми полномочиями) только при необходимости. Все работы от имени такой учетной записи проводятся только под контролем Администратора.

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

3.12. Администратор обеспечивает оперативное обновление и актуальность перечня лиц, их должностей, а также служб и процессов, допущенных к работе с ресурсами и сопоставляемые им роли.

3.13. Перечень помещений, в которых разрешена работа с ресурсами информационных систем, расположены технические средства информационных систем, а также перечень лиц, допущенных в эти помещения, утверждается (изменяется) распоряжением Администрации, по форме приведенной в Приложение № 4 к настоящей Политике. Администратор обеспечивает оперативное обновление и актуальность данного перечня.

3.14. Перечень устройств (стационарных, мобильных, портативных), используемых в информационных системах утверждается (изменяется) распоряжением Администрации, по форме приведенной в приложении № 5 к настоящей Политике. Администратор обеспечивает оперативное обновление и актуальность данного перечня. Идентификация и аутентификация устройств в информационных системах осуществляется по совокупности имени или ID устройства, IP-адреса и MAC-адреса. Идентификация и аутентификация устройств осуществляется с помощью механизмов СЗИ от НСД. В случае выявления посторонних устройств, Администратор оперативно блокирует доступ неустановленного устройства к информационным системам и созывает ГРИИБ, которая в свою очередь устанавливает причины и последствия такого инцидента.

3.15. Идентификация и аутентификация на сетевом оборудовании (коммутаторы, маршрутизаторы, точки доступа и т. д.) разрешена только администраторам безопасности, системным администраторам и сотрудникам сторонней организации, производящим работы в сети Администрации 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.

3.16. Пользователям запрещены любые действия в информационных системах до прохождения процедуры идентификации и аутентификации в системе. Администратору разрешается ряд действий до прохождения идентификации и аутентификации в информационных системах в ряде случаев. Условия, при которых разрешаются такие действия и перечень разрешенных действий для Администратора до прохождения процедуры идентификации и аутентификации в информационных системах перечислены в пункте 5.9 инструкции Администратора:

- 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. ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ПОТОКАМИ

4.1. С целью определения разрешенных маршрутов прохождения информации между пользователями, устройствами, сегментами в рамках информационных систем, а также между информационными системами и при взаимодействии с сетью Интернет устанавливаются правила и процедуры управления информационными потоками.

4.2. С целью управления информационными потоками внутри периметра защищаемой сети Администрации на всех сетевых устройствах (включая сетевые адаптеры АРМ Пользователей и серверов) прописываются статические маршруты в список статистических сетевых маршрутов в информационных системах, по форме приведенной в Приложении 5 к настоящей Политике. Список утверждается (изменяется) распоряжением Администрации.

4.3. Администратор осуществляет контроль неизменности статических маршрутов, а также добавляет необходимые маршруты в случае необходимости и документирует изменения.

4.4. Контроль и фильтрация информационных потоков между информационными системами и внешними телекоммуникационными сетями осуществляется с помощью межсетевых экранов ViPNet Client, ViPNet Coordinator.

4.5. Для контроля и фильтрации информационных потоков между информационными системами 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».

4.6. С целью реализации политики контроля и фильтрации информационных потоков между информационными системами и внешними телекоммуникационными сетями «Блокировать все, кроме явно разрешенного» утверждается (изменяется) на основании распоряжения Администрации список разрешающих правил взаимодействия с внешними телекоммуникационными сетями, по форме приведенной в Приложении № 6 к настоящей Политике.

Данный список может быть дополнен на основании служебной записки Администратору с указанием обоснования добавления того или иного ресурса/сайта/протокола/порта в список разрешенных.

4.7. Администратор обеспечивает соответствие настроек межсетевых экранов ViPNet Client, ViPNet Coordinator, согласно утвержденному списку разрешённых правил.

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

5.1. В информационных системах 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 утверждается (изменяется) распоряжением Администрации, по форме приведенной в Приложении № 7 к настоящей Политике.

5.3. Установка программного обеспечения, его компонент, утилит и драйверов осуществляется только системными администраторами или администратором безопасности в соответствии с Перечнем разрешенного программного обеспечения. Пользователям запрещена установка любого ПО в информационных системах.

5.4. Пользователь имеет право подать заявку в виде служебной записки на включение в список разрешенного в информационных системах 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 информационных системах списку разрешенного ПО. В случае выявления постороннего программного обеспечения, созывается группа реагирования на инциденты информационной безопасности, 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 информационных системах для хранения и обработки защищаемой информации. Исходя их этого, защита машинных носителей информации (как в стационарных АРМ и серверах, так и мобильных/съемных) является ключевым звеном политики информационной безопасности Администрации.

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 Администрации учету подлежат:

- съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные подобные устройства);
- портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности 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, использование которых разрешено за пределами контролируемой зоны и информационной системы и делает соответствующую отметку в журнале. Использование немаркированного соответствующим образом носителя информации за пределами контролируемой зоны и/или информационной системы является инцидентом информационной безопасности и расследуется в установленном порядке.

6.7. Использование неучтенных съемных носителей и/или портативных устройств (в том числе личных) в информационных системах 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 информационных системах. 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 информационных системах, 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 информационных систем и комплектности технических средств.

6.11. К устройствам ввода относятся: клавиатуры, мыши, сканеры. К устройствам ввода допущены все легальные пользователи информационной системы. Допуск к тем или иным устройствам ввода организовывается Администратором, в зависимости от выполняемых пользователем должностных обязанностей. Дополнительный контроль устройств ввода не осуществляется.

6.12. К интерфейсам ввода/вывода относятся: USB-порты, LPT-порты, COM-порты, порты вывода видеоизображения (VGA, DVI, HDMI), сетевые адаптеры (порт RJ45).

6.13. Сетевой трафик контролируется межсетевыми экранами ViPNet Client, ViPNet Coordinator в соответствии с установленными настоящей Политикой правилами.

6.14. Порты вывода видеоизображения дополнительному контролю в информационных системах не подлежат.

6.15. USB, LPT и COM порты контролируются с помощью СЗИ от НСД Secret Net Studio. К работе с данными интерфейсами вывода допущены пользователи в соответствии с политикой учета съемных носителей информации.

6.16. Вывод информации на печать дополнительно не контролируется.

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

- возвращения учтенного съемного носителя информации Администратору;
- кого 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.

6.18. 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.

6.19. 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.

6.20. 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.

6.21. В случаях уничтожения информации способами, описанными в пунктах 6.19 и 6.20 настоящей Политики, Администратор фиксирует факт уничтожения информации, а также факт контроля уничтожения информации в Журнале учета мероприятий по защите информации в информационных системах.

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

6.23. В случае физического уничтожения машинного носителя информации, составляется акт уничтожения. Акт уничтожения машинных носителей подписывается созданной на основании распоряжения Администрации комиссией по уничтожению персональных данных и по форме утвержденного акта уничтожения персональных данных.

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

7.1. В Администрации осуществляется взаимодействие с внешними информационными системами.

7.2. Администратор обеспечивает доступ пользователей внешних информационных систем к ресурсам информационных систем Администрации в соответствии с правилами и процедурами, описанными в разделе 3 настоящей Политики.

7.3. Администратор обеспечивает управление информационными потоками при взаимодействии с внешними информационными системами в соответствии с правилами и процедурами, описанными в разделе 4 настоящей Политике.

7.4. Администратор составляет список прикладного программного обеспечения, доступного для конкретного перечня пользователей внешних информационных систем в соответствии с формой, приведенной в Приложении №

8 к настоящей Политике с указанием целей предоставления такого доступа. Список утверждается (изменяется) на основании распоряжения Администрации.

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

7.6. В Администрации взаимодействие с внешними информационными системами 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 ОБЕСПЕЧЕНИЯ ДОВЕРЕННОЙ ЗАГРУЗКИ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

8.1. В Администрации применяется модуль доверительной загрузки (далее - МДЗ).

8.2. Для работы с ресурсами информационных систем выбираются такие технические средства, базовая система ввода-вывода которых (BIOS/UEFI) позволяет отключить возможность выбора источника загрузки в обход настроек BIOS/UEFI (вызов вариантов источников загрузки одной из функциональных клавиш).

8.3. Администратор контролирует работоспособность МДЗ в соответствии с планом периодических мероприятий по контролю защищенности информации. По результатам проверки делается запись в журнал периодического тестирования средств защиты информации.

8.4. В случае некорректной работы средства доверенной загрузки на техническом средстве, такое техническое средство изымается из информационной системы на время проведения ремонта/замены средства доверенной загрузки. В случае необходимости продолжения работы на техническом средстве, применяются следующие компенсирующие меры:

- опечатываются USB-порты, входы для SD/Micro-SD и других карт памяти, CD/DVD/Blu-Ray-приводы и сами технические средства;
- устанавливается пароль администратора на вход в BIOS/UEFI и отключается возможность вызова источника загрузки нажатием функциональной клавиши (F1-F12) при загрузке;
- устанавливается усиленный визуальный контроль за техническим средством.

8.5. В проектной документации на систему защиты информации в информационных системах обосновано применение компенсирующих мер, нейтрализующих угрозы безопасности информации, связанные с недоверенной загрузкой технических средств.

9. ПРАВИЛА И ПРОЦЕДУРЫ ПРИМЕНЕНИЯ УДАЛЕННОГО ДОСТУПА

9.1. В Администрации для достижения некоторых целей и задач применяются технологии удаленного доступа к информационным системам.

9.2. Удаленный доступ к информационным системам предоставляется только тем Пользователям, которым это необходимо для выполнения своих должностных обязанностей, либо внешним пользователям, не являющимся работниками Администрации, которым такой доступ необходим для обновления, установки, разработки программного обеспечения (и других действий в информационной системе) в соответствии с договором.

9.3. Удаленный доступ к информационным системам запрещен от имени привилегированных учетных записей (учетные записи системных администраторов, администраторов безопасности и т. д.).

9.4. Удаленный доступ к информационным системам предоставляется на основании утвержденного списка, по форме приведенной в Приложении № 9 к настоящей Политике, в котором указываются: ФИО сотрудника, доступные ресурсы, цель или основание предоставления удаленного доступа, учетная запись для удаленного доступа, сроки и время предоставления удаленного доступа. Утверждение (изменение) списка осуществляется на основании распоряжения Администрации.

9.5. Администратор осуществляет мониторинг и контроль удаленного доступа на предмет выявления установления несанкционированного соединения технических средств (устройств) с информационной системой. В случае выявления несанкционированного доступа Администратор созывает ГРИИБ, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

9.6. С целью упрощения контроля за удаленными подключениями Администратор обеспечивает минимальное количества точек удаленного доступа к информационным системам.

9.7. Администратор обеспечивает защиту канала связи при удаленном доступе с помощью средств криптографической защиты «ViPNet Coordinator». Администратор обеспечивает невозможность получения удаленного доступа к информационным системам, если на удаленном АРМ Пользователя не установлен (или отключен) ViPNet Client.

9.8. Администратор обеспечивает отсутствие возможности удаленного доступа к информационным системам по уязвимым протоколам (ftp, telnet и т. д.).

9.9. Перед предоставлением удаленного доступа к информационным системам, Администратор проводит инструктаж Пользователей по вопросам информационной безопасности.

10. ПРАВИЛА И ПРОЦЕДУРЫ ОБНАРУЖЕНИЯ (ПРЕДОТВРАЩЕНИЯ) ВТОРЖЕНИЙ

10.1. В информационных системах для выявления преднамеренных и случайных атак на внешней границе сети применяется средство обнаружения вторжений Secret Net Studio. Средство обнаружения вторжений содержит следующие компоненты:

- детекторы сетевых атак:
- сканирование портов;
- ARP-spoofing;
- SYN-FLOOD;
- Аномальный трафик;

- DDoS;
-DOS;
- сигнатурные анализаторы;
- иные компоненты, не запрещенные законодательством РФ.

10.2. С целью снижения нагрузки на Secret Net Studio, система устанавливается за межсетевым экраном, а также отключается проверка ViPNet-трафика.

10.3. При первоначальном развертывании Secret Net Studio Администратор устанавливает пароль учетной записи главного администратора средства обнаружения вторжений в соответствии с утвержденной парольной политикой.

10.4. Администратор осуществляет следующие настройки Secret Net Studio:
- включить детекторы атак - включить;
- блокировка атакующего хоста при обнаружении атак - включено;
- время блокировки - 15 мин;
- используемые сетевые сервисы - по умолчанию;
- сканирование портов - включено;
- период обнаружения - 60 секунд;
- максимальное количество обращений к портам за указанный период - 200;
- ARP-spoofmg - включено;
- время после ARP-запроса, в течении которого ожидается ARP-ответ - 1500 миллисекунд;
- действие с ARP-ответами, полученными без ARP-запросов - активное противодействие APIP-spoofmg;
- SYN-FLOOD - включено;
- время, за которое учитывается полуоткрытое соединения - 30 секунд;
- количество полуоткрытых соединений, после которых хост считается атакующим - 20;
- блокировать пакет, если детектор сработал - включено;
- аномальный трафик - включено;
- блокировать пакет, если детектор сработал - включено;
- DDoS -включено;
- максимальное количество активных удаленных хостов, при превышении которого срабатывает детектор - 1000;
- DoS - включено;
- отрезок времени, за который учитывается обращение к порту - 60 секунд;
- максимальное количество пакетов, при превышении которого будет детектирована атака - 52428;
- максимальный размер данных, при превышении которого будет детектирована атака - 76800 Кб;
- замедлять трафик атакующего хоста - включено;
- сервис - по умолчанию;
- обнаружение вторжений (регистрация событий):
- сработал детектор вторжений - включить;
- СОВ заблокировал удаленный узел - включить;
- обнаружена сигнатура СОВ. Доступ заблокирован - включить;
- СОВ разблокировала удаленный узел - включить.

10.5. Администратор не реже одного раза в сутки изучает отчеты Secret Net Studio. При выявлении аномалий и атак Администратор сам принимает меры по

профилактике и предотвращению несанкционированного доступа к информационным системам, либо созывает ГРИИБ.

11. ПРАВИЛА И ПРОЦЕДУРЫ ВЫЯВЛЕНИЯ, АНАЛИЗА И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

11.1. В Администрации в качестве средства выявления уязвимостей используется сертифицированный сканер уязвимостей.

11.2. Администратор не реже одного раза в месяц проводит полное сканирование системы на выявление уязвимостей. В случае поступления информации из новостных источников об уязвимостях в операционных системах и/или прикладном программном обеспечении применяемых в информационных системах производится внеплановое обновление базы данных сканера уязвимостей и полное сканирование информационной системы.

11.3. Администратор изучает отчеты по результатам сканирования 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 ГРИИБ.

11.4. 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».

11.5. При выявлении уязвимостей, Администратор анализирует системные журналы и журналы средств защиты информации, на предмет выявления эксплуатации выявленной уязвимости в информационной системе и последствий такой эксплуатации.

11.6. В случае невозможности оперативного устранения критичной уязвимости, Администратор уведомляет об этом ответственного за организацию обработки персональных данных.

12. ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ УСТАНОВКИ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

12.1. С целью противодействия эксплуатации известных уязвимостей, в Администрации устанавливаются правила и процедуры контроля установки обновлений системного и прикладного программного обеспечения.

12.2. В программном обеспечении, поддерживающем автоматические обновления, автоматические обновления не отключаются.

12.3. Общесистемное программное обеспечение и основное прикладное программное обеспечение обновляется во внерабочее время. Администратор

перед обновлениями создает образы системы, точки восстановления и резервные копии баз данных.

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

12.5. 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.

12.6. Администратор в соответствии с эксплуатационной документацией на программное обеспечение осуществляет проверку установки обновлений, а также корректность установки обновлений. В Администрации должно применяться только такое программное обеспечение, которое поддерживает проверку целостности файлов обновлений.

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

12.8. Обновление микропрошивок и программного обеспечения BIOS/UEFI производится только при поступлении информации о критичных уязвимостях в таком программном обеспечении, применяемом в Администрации.

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

13.1. Состав технических средств (далее – ТС), программного обеспечения (далее – ПО) и средств защиты информации (далее – СрЗИ) информационных систем фиксируется в техническом паспорте на информационную систему. Технический паспорт является эталоном состава ТС, ПО и СрЗИ, по которому осуществляется периодический контроль.

13.2. В случае добавления новых ТС, ПО и СрЗИ в состав информационных систем или удаления существующих компонентов, на основании акта ввода в эксплуатацию (или акта вывода из эксплуатации) максимально оперативно вносятся изменения в Технический паспорт.

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

13.4. Выявление несоответствия состава ТС, ПО и СрЗИ техническому паспорту информационной системы является инцидентом безопасности. В случае выявления фактов несоответствия Администратор устанавливает причины самостоятельно или созывает ГРИИБ.

13.5. 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.

13.6. 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 ответственному за организацию обработки персональных данных, 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.

14. ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

14.1. Администратор в СЗИ от НСД Secret Net Studio настраивает контроль целостности (осуществляет расчет эталонных контрольных сумм) файлов и директорий прикладного программного обеспечения, операционных систем и средств защиты информации.

14.2. На АРМ в информационных системах контролю целостности подлежат следующие файлы и директории: - C:\Windows\system32 - C:\Program Files\Secret Net Studio\Client - C:\Program Files(x86)\Kaspersky Lab - C:\Program Files(x86)\InfoTeCS - C:\Program FilesWGate

14.3. Нарушение целостности программного обеспечения является инцидентом информационной безопасности. В случае выявления таких инцидентов, Администратор принимает меры по их устранению самостоятельно или в составе ГРИИБ.

14.4. В информационных системах запрещено использование средств разработки и отладки программ.

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

15.1. Резервирование информационных ресурсов (программного обеспечения, баз данных, средств защиты информации) информационных систем осуществляется в соответствии с инструкцией администратора безопасности информации и в соответствии порядком резервирования, утвержденным по форме приведенной в Приложением № 10 к настоящей Политике. Утверждение (изменение) порядка резервирования осуществляется на основании распоряжения Администрации.

15.2. Администратор осуществляет с периодичностью, установленной в плане мероприятий по обеспечению режима защиты информации проверку работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий. По результатам проверки делается запись в журнале учета мероприятий по контролю за соблюдением режима защиты информации. В случае выявления проблем с системой резервирования, принимаются меры по восстановлению ее работоспособности. После восстановления работоспособности системы резервирования осуществляется внеплановое резервное копирование всех информационных ресурсов информационных систем.

15.3. Резервирование технических средств осуществляется в соответствии с проектной документацией (эскизным проектом) на систему защиты информации информационных систем.

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

15.5. Нештатными ситуациями являются:

1) разглашение информации ограниченного доступа сотрудниками администрации Тяжинского муниципального округа, имеющими к ней право доступа, в том числе:
2) разглашение информации лицам, не имеющим права доступа к защищаемой информации;
3) передача информации по незащищенным каналам связи;
4) обработка информации на незащищенных технических средствах обработки информации;
5) опубликование информации в открытой печати и других средствах массовой информации;
6) передача носителя информации лицу, не имеющему права доступа к ней;
7) утрата носителя с информацией.
8) неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:
9) несанкционированное изменение информации;
10) несанкционированное копирование информации;
11) несанкционированный доступ к защищаемой информации:
12) несанкционированное подключение технических средств к средствам и системам информационной системы;
13) использование закладочных устройств;
14) использование злоумышленником легальных учетных записей пользователей для доступа к информационным ресурсам информационной системы;
15) использование злоумышленником уязвимостей программного обеспечения информационной системы;
16) использование злоумышленником программных закладок;
17) заражение информационной системы злоумышленником программными вирусами;
18) хищение носителей информации;
19) нарушение функционирования технических средств обработки информации;

20) блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;
21) дефекты, сбои, отказы, аварии технических средств и систем;
22) дефекты, сбои, отказы программного обеспечения информационной системы;
23) сбои, отказы и аварии систем обеспечения информационной системы;
24) природные явления, стихийные бедствия:
25) термические, климатические факторы (аномально низкие или аномально высокие температуры воздуха, пожары, наводнения, снегопады и т. д.);
26) механические факторы (повреждения зданий, землетрясения и т. д.);
27) электромагнитные факторы (отключение электропитания, скачки напряжения, удары молний и т. д.).

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

15.7. Порядок оповещения должностных лиц и сроки выполнения мероприятий при нештатных ситуациях определены в Плане обеспечения непрерывности функционирования информационной системы в Приложении № 11 настоящей Политики.

15.8. 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.

15.9. 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 ГРИИБ, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

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

1) корректное отключение технических средств информационной системы до истощения ресурса источников бесперебойного питания, перегрева технических средств и до наступления других негативных последствий;
2) предпринимаются меры по устранению причин, вызвавших сбои, отказы и аварии средств и систем, а также меры по замене/ремонту вышедших из строя средств и систем;
3) в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации, Администратор восстанавливает их из резервных копий.

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

1) Пользователи корректно отключают и обесточивают свои рабочие места;

2) системные администраторы корректно отключают и обесточивают серверы и сетевое оборудование;

3) Администратор предпринимает меры к эвакуации носителей информации и носителей резервных копий;

4) в случае нарушения корректной работы технических средств в информационной системе в результате стихийных бедствий или природных явлений принимаются меры по ремонту/замене вышедшего из строя оборудования;

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

6) в случае стихийных действий/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.

16. ПРАВИЛА ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТЫ И ЗАЩИТЫ ОТ СПАМА

16.1 В настоящей Политике приведены только правила использования электронной почты, касающиеся вопросов информационной безопасности.

16.2. Пользователи при работе с электронной почтой руководствуются положениями раздела 4 инструкции Пользователя.

16.3. Администратор настраивает блокирование потенциально опасных вложений в электронные письма на уровне почтового сервера. Блокировке подлежат как минимум следующие типы файлов: исполняемые файлы, файлы установщиков, файлы скриптов, файлы MS Office с макросам, архивы (в том числе и многотомные).

16.4. Администратор на уровне почтового сервера настраивает черные и белые списки адресатов и отправителей.

16.5. Пользователям информационных систем Администрации, в том числе привилегированным запрещено рассылать спам через почтовый сервер организации.

16.6. Администратор не реже одного раза в месяц проводит занятия с Пользователями на тему фишинговых писем, новых методов социальной инженерии и потенциально опасных вложений в электронных письмах.

17. ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ МОБИЛЬНОГО КОДА

17.1. В информационных системах разрешено использование следующих технологий мобильного кода: PDF, JavaScript, ActiveX. Использование иных технологий мобильного кода в информационных системах запрещено.

17.2. Администратор устанавливает доступ к использованию разрешенных технологий мобильного кода только тем сотрудникам, которым это необходимо для выполнения их служебных (должностных) обязанностей.

17.3. Регистрация событий, связанных с несанкционированным использованием технологий мобильного кода, осуществляется антивирусным средством, средствами обнаружения вторжений и средством защиты от несанкционированного доступа.

17.4. В случае регистрации инцидентов информационной безопасности, связанных с использованием технологий мобильного кода созывается ГРИИБ, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

Приложение № 1
к Политике информационной безопасности
в администрации Тяжинского муниципального округа

Администратору безопасности информации

_____
(фамилия и инициалы исполнителя)

Произвести изменения в списках пользователей

Глава Тяжинского муниципального округа

В. Е. Серебров

«___» _____ 20__ г.

ЗАЯВКА
на внесение изменений в списки пользователей
и наделение пользователей полномочиями доступа к ресурсам информационных систем администрации Тяжинского муниципального округа

Прошу зарегистрировать пользователя (исключить из списка пользователей, изменить полномочия пользователя) информационной системы (указывается наименование информационной системы):
(нужное подчеркнуть)

_____
(должность с указанием подразделения)

_____
(фамилия имя и отчество сотрудника)

предоставив ему полномочия, необходимые (лишив его полномочий, необходимых)
(нужное подчеркнуть)

для решения задач:

_____
(список задач согласно формуляров задач)

_____

Начальник

_____
(наименование заказывающего подразделения)

«___» _____ 20__ г. _____ _____
(подпись) (фамилия)

Согласовано Администратор безопасности

«___» _____ 20__ г. _____ _____
(подпись) (фамилия)

Обратная сторона заявки

ЗАДАНИЕ
на внесение изменений в списки пользователей

Присвоено **имя** _____ (персональный идентификатор) и предоставлены полномочия, необходимые для решения следующих задач:

Наименование задач

Администратор безопасности _____ / _____/.

Имя учетной записи, персональный идентификатор и начальное значение пароля получил, о порядке смены пароля при первом входе в систему проинструктирован, с инструкцией Пользователя информационными системами ознакомлен

Пользователь

_____
(подпись, фамилия)

«___» _____ 20__ года

Приложение № 2
к Политике информационной безопасности
в администрации Тяжинского муниципального округа

Положение о разграничении прав доступа к работе в информационных системах администрации Тяжинского муниципального округа

I. Общие положения

1. Настоящее Положение определяет права и привилегии субъектов доступа, описывает разграничение доступа субъектов доступа к объектам доступа на основе совокупности правил разграничения доступа, установленных в информационных системах персональных данных (далее - ИСПДн), а также контроль соблюдения этих правил в администрации Тяжинского муниципального округа (далее – Администрация).

2. Разграничение прав осуществляется на основании "Модели угроз безопасности персональных данных при их обработке в ИСПДн", а также исходя из характера и режима обработки персональных данных в ИСПДн.

3. Уровень прав доступа представлен в таблице. Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИСПДн, осуществляется в соответствии с их должностными обязанностями. Доступ к объектам доступа с учетом разделения полномочий (ролей) обеспечивается в соответствии с матрицей субъектов доступа по отношению к защищаемым информационным ресурсам в ИСПДн (далее - матрица доступа).

Таблица. Уровень прав доступа (матрица).

Роль	**Описание параметров доступа к ресурсам информационных систем для данной роли**
Администратор безопасности	Полный доступ к ресурсам, настройкам ОС и СЗИ. Полный доступ к системным журналам, журналам средств защиты информации и другим электронным журналам сообщений.
Системный администратор	Полный доступ к ресурсам за исключением доступа к настройкам СЗИ и к журналам средств защиты информации.
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.
Сертифицированный сканер уязвимостей	Доступ на чтение к системному реестру Windows. Доступ на чтение файловой структуры и папок на жестких дисках. Доступ на запись во временную директорию %SystemRoot%\Temp.

4. Доступ в помещения, в которых расположены технические средства ИСПДн (далее - Помещения), осуществляется в соответствии с перечнем лиц, утверждаемым распоряжением Администрации.

II. Правила разграничения доступа

5. В ИСПДн реализуется:

1) управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей,

возлагается на администратора путем функций, в соответствии с инструкцией администрация безопасности, утвержденной распоряжением Администрации.

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

Заведение временных учетных записей осуществляется на основании подписанного администратором и ответственным за обработку и защиту персональных данных соответствующего Акта, содержащего цель, место, наименование и сроки;

2) дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа - списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа. Типы доступа должны включать операции по чтению, записи, удалению, выполнению и иные операции, разрешенные к выполнению пользователем (группой пользователей).

Правила разграничения доступа реализуются на основе матрицы доступа и обеспечивают управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к ТС, устройствам (в том числе внешним), объектам файловой системы, запускаемым и исполняемым модулям, объектам СУБД, параметрам настройки СЗИ, в том числе внутри виртуальных машин, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации.

В ИСПДн правила разграничения доступа должны обеспечивать:

а) управление доступом субъектов при входе в ИСПДн;

б) управление доступом субъектов к ТС, устройствам, внешним устройствам;

в) управление доступом субъектов к объектам, создаваемым общесистемным (общим) ПО;

г) управление доступом субъектов внутри виртуальной инфраструктуры.

3) в ИСПДн осуществляется управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы, включающее:

а) фильтрацию информационных потоков в соответствии с установленными правилами управления потоками;

б) разрешение передачи информации в ИСПДн только по установленному маршруту;

в) изменение (перенаправление) маршрута передачи информации в случаях необходимости, по согласованию с администратором.

4) права и привилегии, назначаемые пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование ИСПДн, являются минимально необходимыми для выполнения ими своих должностных обязанностей (функций);

5) ограничение неуспешных попыток входа в ИСПДн (доступа к ИСПДн), равное 5 (пяти), при этом обеспечивается блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в ИСПДн (доступа к ИСПДн) не менее чем на 5 (пять) минут;

6) блокирование сеанса доступа в ИСПДн, после 10 минут времени бездействия (неактивности) пользователя или по его запросу.

Блокирование сеанса доступа пользователя в ИСПДн обеспечивает временное приостановление работы пользователя со СВТ или с виртуальной машиной, с которого осуществляется доступ к ИСПДн (без выхода из ИСПДн).

Для заблокированного сеанса осуществляется блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса. Блокирование сеанса доступа пользователя в ИСПДн сохраняется до прохождения им повторной идентификации и аутентификации;

7) запрет всех действий пользователей до прохождения процедур идентификации и аутентификации в ИСПДн (кроме необходимых для прохождения процедур идентификации и аутентификации).

Администратору ИБ разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования ИСПДн в случае сбоев в работе или выхода из строя отдельных ТС (устройств).

Приложение № 3
к Политике информационной безопасности
в администрации Тяжинского муниципального округа

Перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами информационных систем

Настоящий Перечень устанавливает перечень лиц, должностей и процессов, допущенных к работе с ресурсами информационных систем. Для каждого элемента списка в таблице обязательно указываются ФИО (Имя службы или процесса для неодушевленных субъектов доступа), должность (только для одушевленных субъектов доступа), имя присвоенной учетной записи и роль (в соответствии с Положением о разграничении прав доступа к работе в информационных системах администрации Тяжинского муниципального округа). Тип и серийный номер выданного идентификатора указываются только при выдаче пользователю электронного ключа. Роспись о получении электронного ключа ставится только при выдаче пользователю такого ключа.

В настоящем Перечне не отражены вопросы, связанные с использованием средств криптографической защиты информации (СКЗИ). Перечни пользователей СКЗИ, а также иные учетный данные, связанные с СКЗИ приведены в других журналах и перечнях.

№ п/п	ФИО сотрудника / Имя службы или процесса	Должность	Имя присвоенной учетной записи	Роль	Выдан эл. ключ	Роспись о получении эл. ключа
1.						
2.						
3.						
4.						
5.						
6.						
7.						

Приложение № 4
к Политике информационной безопасности
в администрации Тяжинского муниципального округа

Перечень помещений, в которых разрешена работа с ресурсами информационных систем, в которых размещены технические средства информационных систем, а также перечень лиц, допущенных в эти помещения

№ п/п	Название/номер помещения	Наименование информационной системы	Техническое средство информационной системы						Сотрудники, допущенные в помещение	
			Тип	Модель	Учетный № (серийный, инвентарный)	Сетевое имя	IP-адрес	MAC-адрес	ФИО	Должность
1.										
2.										
3.										
4.										
5.										
6.										
7.										

Приложение № 5
к Политике информационной безопасности
в администрации Тяжинского муниципального округа

Перечень статических сетевых маршрутов в информационных системах

№ п/п	Наименование информационной системы	Сеть	Маска подсети	Шлюз по умолчанию	Метрика	Где применяется

Приложение № 6
к Политике информационной безопасности
в администрации Тяжинского муниципального округа

Список разрешающих правил взаимодействия с внешними телекоммуникационными сетями в информационных системах

№ п/п	IP/URL ресурса или подсеть	Обоснование разрешения	Правило	Время действия правила	Учетные записи, устройства, процессы, для которых действует правило
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					

Приложение № 7
к Политике информационной безопасности
в администрации Тяжинского муниципального округа

Список разрешенного программного обеспечения в информационных системах

№ п/п	Наименование информационной системы	Наименование ПО	Тип ПО	Цель применения ПО в информационной системе	Место установки компонентов ПО
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					

Приложение № 8
к Политике информационной безопасности
в администрации Тяжинского муниципального округа

Список прикладного программного обеспечения информационных систем, доступного пользователям внешней информационной системы

№ п/п	Наименование информационной системы	Наименование ПО	Тип ПО	Цель допуска к ПО внешних пользователей	Пользователи внешних систем, допущенный к работе с ПО
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					

Приложение № 9
к Политике информационной безопасности
в администрации Тяжинского муниципального округа

Список пользователей информационных систем и внешних пользователей, которым в соответствии с должностными обязанностями предоставлен удаленный доступ к информационной системе

№ п/п	ФИО	Является ли сотрудником организации	Ресурсы, к которым предоставляется удаленный доступ к информационной системе	Обязанности, в связи с которыми предоставляется удаленный доступ или основание для предоставления удаленного доступа	Учетная запись, от имени которой предоставляется удаленный доступ	Время, на которое предоставляется удаленный доступ
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						
14.						
15.						

Приложение № 10
к Политике информационной безопасности
в администрации Тяжинского муниципального округа

Порядок резервирования информационных ресурсов в информационных системах

№ п/п	Наименование информационного ресурса	Место размещения ресурса в системе	Вид резервного копирования	Ответственный за резервное копирование	Место хранения резервной копии	Частота резервного копирования
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						

Приложение № 11
к Политике информационной безопасности
в администрации Тяжинского муниципального округа

План обеспечения непрерывности функционирования информационных систем

№ 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
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 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

№ 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
9.	Маскировка под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
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
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

№ 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
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
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 обнаружения инцидента	Администратору сразу после обнаружения инцидента	20 минут	1 день
22.	Дефекты, сбои, отказы, аварии ТС, программных средств и систем	Сбой ТС и систем	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	1 час	2 дня
		Отказ ТС и систем, 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

№ 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
		Отказ ТС и систем, затронувший работу одного пользователя	Администратору сразу после обнаружения инцидента	Администратору в первый рабочий день после инцидента	1 час	2 дня
		Авария ТС и систем	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	1 день
23.	Сбои, отказы и аварии систем обеспечения	Сбой систем обеспечения	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, 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, 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-техническое обеспечение, Администратору сразу после обнаружения инцидента	Ответственному за материально-техническое обеспечение, 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
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