Приложение
к Приказу МБОУ «Гимназия»
от 31.08.2026г. № 347-П

Политика защиты информации

1. Общие положения

1.1. Настоящая Политика защиты информации (далее – Политика) является документом верхнего уровня, закрепляющим основные цели, задачи и принципы по защите информации в Муниципальном бюджетном общеобразовательном учреждении «Гимназия» (далее – Учреждение).

1.2. Политика устанавливает единый подход к организации деятельности по защите информации и управлению указанной деятельностью в Учреждении.

1.3. Политика разработана с учетом требований нормативных правовых актов Российской Федерации, в том числе приказа ФСТЭК России от 11.04.2025 №117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений».

1.4. Управление информационной инфраструктурой Учреждения осуществляется на основании Положения об информационной инфраструктуре, а также иных локальных актов Учреждения.

1.5. Настоящая Политика разработана в целях:

– информирования работников Учреждения о целях, задачах, принципах и требованиях в области защиты информации, а также об их обязанностях при работе с объектами информационной инфраструктуры;

– установления единых целей, задач, принципов и организационных основ деятельности по защите информации в Учреждении;

– обеспечения конфиденциальности, целостности и доступности информации, обрабатываемой в информационной инфраструктуре Учреждения, а также устойчивого функционирования ее объектов;

– обеспечения соблюдения требований законодательства Российской Федерации и локальных актов Учреждения в области защиты информации, в том числе при обработке персональных данных;

– снижения рисков неправомерного доступа к информации, ее изменения, уничтожения, блокирования, нарушения работоспособности объектов информационной инфраструктуры и иных последствий реализации угроз безопасности информации.

1.6. В Политике используются следующие термины и определения:

1) Автоматизированное рабочее место – программно-технический комплекс информационной системы, предназначенный для автоматизации деятельности определенной категории работников или определенного вида деятельности.

2) Информационная инфраструктура — совокупность объектов информатизации, используемых для создания, обработки, хранения, передачи и использования информации в деятельности Учреждения.

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

4) Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

5) Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

6) Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

7) Мониторинг – методика и система наблюдений за состоянием определенного объекта или процесса, дающие возможность наблюдать их в развитии, оценивать, оперативно выявлять результаты воздействия различных внешних факторов;

8) Процесс – устойчивая, повторяющаяся совокупность взаимосвязанных работ, направленная на выполнение функций и предоставление услуг, преобразующая по определенной технологии (регламенту) входы (в форме материалов, ресурсов, требований) для получения намеченного результата – выхода (например, услуги, документа), представляющего ценность для потребителя результатов процесса;

9) Сайт – совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет») по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет»;

10) Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

1.7. Политика обязательна для исполнения всеми работниками Учреждения.

1.8. Положения и требования Политики распространяются на работников Учреждения, а также на иных лиц, имеющих доступ к объектам информационной инфраструктуры Учреждения, в части, их касающейся.

1.9. В отношении иных лиц и организаций, которым предоставляется доступ к объектам информационной инфраструктуры Учреждения, требования по защите информации устанавливаются договорами, соглашениями, техническими заданиями, условиями предоставления доступа и иными документами, регулирующими соответствующие отношения, с учетом положений настоящей Политики.

2. Цели и задачи защиты информации

2.1. Целями защиты информации являются:

– обеспечение конфиденциальности информации;

– обеспечение целостности информации;

– обеспечение доступности информации;

– обеспечение устойчивости функционирования объектов информационной инфраструктуры Учреждения.

2.2. Для достижения указанных целей решаются следующие задачи:

– выявление и анализ угроз безопасности информации;

– разработка и актуализация моделей угроз безопасности информации и нарушителя;

– классификация объектов информационной инфраструктуры Учреждения и определение уровня их защищенности;

– разработка и внедрение организационных и технических мер защиты информации;

– управление доступом к объектам информационной инфраструктуры Учреждения;

– обеспечение идентификации и аутентификации пользователей;

– обеспечение защиты информации от несанкционированного доступа, изменения, уничтожения и блокирования;
– обеспечение регистрации и учета событий безопасности;
– управление уязвимостями и обновлениями программного обеспечения;
– обеспечение антивирусной защиты и защиты от сетевых атак;
– обеспечение резервного копирования и восстановления информации;
– обеспечение непрерывности функционирования информационных систем;
– организация мониторинга информационной безопасности;
– выявление и реагирование на инциденты информационной безопасности;
– обеспечение физической защиты объектов информационной инфраструктуры;
– обеспечение безопасности при взаимодействии с внешними организациями;
– обучение и повышение осведомленности работников Учреждения в области информационной безопасности.

2.3. Реализация задач обеспечения информационной безопасности осуществляется посредством внутренних стандартов и регламентов по защите информации.

3. Принципы защиты информации

3.1. Защита информации в Учреждении осуществляется на основе следующих принципов:
– принцип законности – обеспечение защиты информации осуществляется в соответствии с законодательством Российской Федерации, нормативными правовыми актами и внутренними документами Учреждения;
– принцип комплексности – защита информации обеспечивается совокупностью организационных, технических и программных мер на всех уровнях информационной инфраструктуры;
– принцип непрерывности – защита информации обеспечивается на всех этапах жизненного цикла информационных систем: создания, эксплуатации, модернизации и вывода из эксплуатации;
– принцип минимально необходимого доступа – доступ пользователей к информации и информационным системам предоставляется в объеме, необходимом для выполнения их должностных обязанностей;
– принцип персональной ответственности — каждый пользователь несет ответственность за соблюдение требований информационной безопасности в пределах предоставленных ему прав доступа;
– принцип централизованного управления – управление деятельностью по защите информации осуществляется централизованно в рамках установленной системы управления информационной безопасностью;
– принцип приоритета предотвращения угроз – меры по защите информации направлены на предупреждение реализации угроз безопасности информации, а также своевременное выявление и устранение их последствий;
– принцип контролируемости и проверяемости – процессы обеспечения информационной безопасности подлежат контролю, мониторингу и оценке их эффективности;
– принцип достаточности мер защиты – меры защиты информации определяются с учетом актуальных угроз, значимости информации и уровня возможного ущерба;
– принцип адаптивности – система защиты информации подлежит постоянному совершенствованию с учетом изменений угроз, технологий и нормативных требований;
– принцип сегментации и разграничения – информационная инфраструктура и доступ к ней организуются с учетом разграничения прав доступа и изоляции критически важных компонентов;

– принцип защищенности по умолчанию – информационные системы и средства защиты информации настраиваются с использованием максимально безопасных параметров по умолчанию;

– принцип использования доверенных средств защиты — применяемые средства защиты информации должны соответствовать установленным требованиям безопасности и обеспечиваться поддержкой их производителей.

4. Объекты защиты информации

4.1. Перечни объектов защиты информации приведены в Приложении 1 к настоящей Политике.

4.2. Конкретный состав объектов защиты информации определяется и поддерживается в актуальном состоянии в соответствующих учетных сведениях об объектах информационной инфраструктуры Учреждения.

5. Организационная система управления деятельностью по защите информации

5.1. Общие положения

5.1.1. Организационная система управления деятельностью по защите информации включает следующие подсистемы:

– подсистема управления деятельностью по защите информации;

– подсистема обеспечения защиты информации;

– подсистема управления обработкой персональных данных.

5.1.2. Подсистемы организационной системы управления деятельностью по защите информации объединяют категории лиц, участвующих в защите информации, в соответствии с выполняемыми ими обязанностями (функциями), полномочиями и ответственностью.

5.1.3. Обязанности (функции), полномочия и ответственность категорий лиц, участвующих в защите информации, устанавливаются настоящей Политикой, внутренними стандартами и регламентами по защите информации, должностными инструкциями работников, договорами и иными локальными актами Учреждения.

5.1.4. Категории лиц, участвующих в защите информации, обязаны обеспечивать выполнение требований законодательства Российской Федерации, настоящей Политики и иных документов по защите информации в пределах возложенных на них обязанностей (функций) и предоставленных полномочий.

5.1.5. Взаимодействие категорий лиц, участвующих в защите информации, осуществляется в соответствии с организационной системой управления деятельностью по защите информации, установленной настоящей Политикой.

5.1.6. Категории лиц осуществляют предоставленные им полномочия в пределах компетенции, установленной законодательством Российской Федерации, настоящей Политикой и локальными актами Учреждения.

5.1.7. Конкретное распределение обязанностей (функций), полномочий и ответственности между категориями лиц определяется положениями о структурных подразделениях, должностными инструкциями работников, внутренними стандартами и регламентами по защите информации.

5.1.8. Схема взаимодействия элементов организационной системы управления деятельностью по защите информации приведена в Приложении 2 к настоящей Политике.

5.2. Подсистема управления деятельностью по защите информации

5.2.1. Управление деятельностью по защите информации в Учреждении осуществляет руководитель Учреждения.

5.2.2. Подсистема управления деятельностью по защите информации осуществляет общее руководство деятельностью по защите информации, а также обеспечивает:

– определение целей, задач и основных направлений деятельности по защите информации;

– организацию функционирования системы защиты информации;

– распределение обязанностей (функций), полномочий и ответственности между участниками деятельности по защите информации;

– координацию деятельности участников защиты информации;

– принятие управленческих решений по вопросам защиты информации;

– контроль деятельности по защите информации;

– рассмотрение результатов контрольных мероприятий, проверок, аудитов и оценок состояния защиты информации;

– принятие решений по совершенствованию деятельности по защите информации.

5.2.3. Подсистема управления деятельностью по защите информации обладает следующими полномочиями:

– утверждение документов по защите информации;

– издание распорядительных документов по вопросам защиты информации;

– назначение ответственных лиц в области защиты информации;

– создание управленческих коллегиальных органов в области защиты информации;

– запрос информации, необходимой для принятия управленческих решений;

– выдача обязательных для исполнения поручений по вопросам защиты информации в пределах компетенции;

– инициирование контрольных мероприятий, проверок и оценок состояния защиты информации;

– рассмотрение результатов контрольных мероприятий, проверок, аудитов и оценок состояния защиты информации, а также принятие решений по их результатам.

5.2.4. Для решения отдельных задач в области защиты информации руководителем Учреждения могут создаваться управленческие коллегиальные органы, состав, полномочия и порядок деятельности которых определяются отдельными локальными актами либо распорядительными документами Учреждения.

5.3. Подсистема обеспечения защиты информации

5.3.1. Подсистема обеспечения защиты информации состоит из следующих категорий лиц:

– работники Учреждения, на которых возложены обязанности по защите информации;

– работники Учреждения, которым для исполнения должностных (трудовых) обязанностей предоставляется автоматизированное рабочее место (далее — Пользователи информационной инфраструктуры).

5.3.2. Подсистема обеспечения защиты информации обеспечивает практическую реализацию деятельности по защите информации и осуществляет:

– выполнение мероприятий по защите информации;

– обеспечение безопасного функционирования информационных систем и объектов информационной инфраструктуры;

– применение и эксплуатацию средств защиты информации;

– соблюдение требований по защите информации;

– выявление и информирование о событиях, угрозах и инцидентах информационной безопасности;

– участие в предупреждении, выявлении и устранении нарушений требований по защите информации;

– участие в реализации решений, принимаемых в рамках деятельности по защите информации.

5.3.3. Подсистема обеспечения защиты информации обладает следующими полномочиями:

– получение доступа к информационным системам, информационным ресурсам и средствам защиты информации в пределах предоставленных прав;

– получение информации, необходимой для выполнения возложенных обязанностей (функций);

– участие в рассмотрении вопросов, связанных с защитой информации;

– подготовка и направление предложений по совершенствованию деятельности по защите информации;

– инициирование рассмотрения вопросов, связанных с устранением выявленных нарушений требований по защите информации.

5.3.4. Работники Учреждения, на которых возложены обязанности по защите информации, обеспечивают реализацию мероприятий по защите информации, организуют выполнение требований настоящей Политики и иных документов по защите информации, а также осуществляют контроль соблюдения работниками установленных требований в пределах предоставленных полномочий.

5.3.5. Пользователи информационной инфраструктуры при работе с информационными системами, информационными ресурсами и иными объектами информационной инфраструктуры Учреждения обязаны соблюдать требования настоящей Политики, Правила работы пользователя информационной инфраструктуры (Приложение 3 к настоящей Политике), а также иных локальных актов Учреждения в области защиты информации в части, касающейся выполнения ими должностных (трудовых) обязанностей.

5.3.6. При предоставлении Пользователю информационной инфраструктуры доступа к информационной системе, информационному ресурсу либо иному объекту информационной инфраструктуры Учреждения он приобретает статус пользователя соответствующего объекта в объеме, необходимом для исполнения своих должностных (трудовых) обязанностей.

5.3.7. Пользователь информационной инфраструктуры при работе с информационными системами и информационными ресурсами на автоматизированных рабочих местах обязан соблюдать требования информационной безопасности, установленные в отношении указанных информационных систем и ресурсов, в части, касающейся выполнения им своих должностных обязанностей.

5.3.8. При наличии отдельной инструкции пользователя информационной системы и (или) информационного ресурса Пользователь информационной инфраструктуры до начала работы с соответствующим объектом подлежит ознакомлению с такой инструкцией.

5.3.9. При отсутствии отдельной инструкции пользователя информационной системы и (или) информационного ресурса Пользователь информационной инфраструктуры обязан руководствоваться Правилами работы пользователя информационной инфраструктуры как документом, определяющим общие правила безопасной и допустимой работы в информационной инфраструктуре Учреждения.

5.4. Подсистема управления обработкой персональных данных

5.4.1. К подсистеме управления обработкой персональных данных относится лицо, ответственное за организацию обработки персональных данных.

5.4.2. Подсистема управления обработкой персональных данных обеспечивает организацию деятельности по обработке персональных данных и осуществляет:

– организацию внутреннего контроля соблюдения требований законодательства Российской Федерации о персональных данных;

– участие в организации мероприятий по защите персональных данных;
– организацию рассмотрения обращений и запросов субъектов персональных данных и их представителей;
– доведение до работников требований законодательства Российской Федерации о персональных данных и локальных актов по вопросам обработки персональных данных;
– участие в предупреждении, выявлении и устранении нарушений законодательства Российской Федерации о персональных данных;
– подготовку предложений по совершенствованию деятельности в области обработки и защиты персональных данных.

5.4.3. Подсистема управления обработкой персональных данных обладает следующими полномочиями:
– получение информации, необходимой для осуществления внутреннего контроля;
– участие в рассмотрении вопросов обработки и защиты персональных данных;
– подготовка и направление предложений по совершенствованию деятельности в области обработки и защиты персональных данных;
– инициирование рассмотрения вопросов, связанных с устранением выявленных нарушений законодательства Российской Федерации о персональных данных;
– взаимодействие с работниками Учреждения по вопросам обработки и защиты персональных данных в пределах компетенции.

5.5. Взаимодействие с подрядными организациями

5.5.1. Для выполнения отдельных работ и (или) оказания услуг в области информационных технологий и защиты информации Учреждением могут привлекаться подрядные организации.

5.5.2. Доступ к объектам информационной инфраструктуры Учреждения может предоставляться подрядным организациям, а также иным лицам и организациям в случаях, предусмотренных законодательством Российской Федерации, договорами, соглашениями, условиями предоставления доступа и иными документами, регулирующими соответствующие отношения.

5.5.3. Обязанности (функции), полномочия, ответственность и порядок взаимодействия подрядных организаций, иных лиц и организаций с Учреждением устанавливаются договорами, соглашениями, техническими заданиями, условиями предоставления доступа и иными документами, регулирующими соответствующие отношения, с учетом положений настоящей Политики.

6. Ответственность работников за нарушение требований о защите информации и установленных правил обработки информации

6.1. Каждый работник Учреждения несет ответственность за соблюдение требований по защите информации при работе с информацией и объектами информационной инфраструктуры, к которым ему предоставлен доступ, в пределах возложенных на него обязанностей и предоставленных полномочий.

6.2. Работники Учреждения, а также иные лица, имеющие доступ к информации и объектам информационной инфраструктуры, несут ответственность за нарушение требований настоящей Политики, внутренних стандартов и регламентов по защите информации в соответствии с законодательством Российской Федерации.

6.3. Ответственность за обеспечение соблюдения требований информационной безопасности возлагается:

– на руководителей структурных подразделений — в части организации работы с информацией и обеспечения соблюдения требований информационной безопасности подчиненными работниками;

– на работников — в части соблюдения установленных требований при работе с информацией и информационными системами;

6.4. Лица, виновные в нарушении требований информационной безопасности, могут быть привлечены к дисциплинарной, административной, гражданско-правовой и иной ответственности в соответствии с законодательством Российской Федерации.

6.5. Требования к обработке персональных данных, а также ответственность за их нарушение, устанавливаются отдельным документом — Положением об обработке персональных данных.

6.6. Нарушение требований Правил работы пользователя информационной инфраструктуры рассматривается как нарушение требований настоящей Политики.

Приложение 1
к Политике защиты информации

Перечни объектов защиты информации

Настоящие Перечни определяют категории объектов защиты информации, используемых в информационной инфраструктуре Муниципального бюджетного общеобразовательного учреждения «Гимназия» (далее – Учреждение) и подлежащих защите в соответствии с законодательством Российской Федерации и Политикой защиты информации.

Конкретный состав объектов защиты информации определяется и поддерживается в актуальном состоянии в учетных сведениях об объектах информационной инфраструктуры Учреждения.

Указанные ниже категории объектов защиты информации применяются при организации деятельности по защите информации, определении мер защиты информации, ведении учета объектов информационной инфраструктуры Учреждения, проведении контрольных мероприятий и актуализации локальных актов Учреждения.

1. Перечень информации

1.1. Информация, создаваемая, обрабатываемая, хранимая и передаваемая посредством объектов информационной инфраструктуры Учреждения, доступ к которой ограничен законодательством Российской Федерации, в том числе персональные данные:

– работников Учреждения;
– обучающихся, их законных представителей;
– иных субъектов персональных данных.

1.2. Информация, создаваемая, обрабатываемая, хранимая и передаваемая посредством объектов информационной инфраструктуры Учреждения, необходимость защиты которой определяется Учреждением самостоятельно.

1.3. Общедоступная информация, размещаемая на официальном сайте Учреждения и иных информационных ресурсах, в части обеспечения ее целостности, доступности и защиты от неправомерного изменения, уничтожения и блокирования.

2. Информационные системы и информационные ресурсы

2.1. Информационная система, используемая для организации, проведения, обеспечения и контроля проведения государственной итоговой аттестации.

2.2. Государственные, муниципальные и иные информационные системы, не эксплуатируемые Учреждением, доступ к которым предоставлен Учреждению и его работникам для исполнения полномочий, функций, прав и обязанностей, в том числе для предоставления информации, получения информации и участия в информационном обмене.

2.3. Официальный сайт Учреждения, используемый для размещения информации о деятельности Учреждения.

3. Программное обеспечение

3.1. Операционные системы, драйверы, системные утилиты и иное системное программное обеспечение, используемое для обеспечения функционирования, настройки и сопровождения серверного оборудования, автоматизированных рабочих мест и иных средств вычислительной техники Учреждения.

3.2. Прикладное программное обеспечение, в том числе офисное программное обеспечение, используемое на автоматизированных рабочих местах, серверном оборудовании

и иных средствах вычислительной техники Учреждения для обеспечения деятельности Учреждения.

3.3. Программные средства защиты информации.

3.4. Программные средства криптографической защиты информации.

4. Программно-аппаратные и технические средства

4.1. Автоматизированные рабочие места, используемые работниками Учреждения для создания, обработки, хранения, передачи и использования информации.

4.2. Серверное оборудование, системы хранения данных и иные средства вычислительной техники, используемые для обеспечения функционирования серверного сегмента информационной инфраструктуры Учреждения.

4.3. Сетевое, телекоммуникационное и коммутационное оборудование, используемое для обеспечения функционирования сетевого сегмента информационной инфраструктуры Учреждения.

4.4. Устройства печати, сканирования, копирования и иные периферийные устройства, используемые при обработке информации.

5. Перечень объектов информационно-телекоммуникационной сети

5.1. Телекоммуникационные розетки, используемые для подключения средств вычислительной техники и иных объектов информационной инфраструктуры Учреждения к информационно-телекоммуникационной сети Учреждения.

5.2. Кабельные линии информационно-телекоммуникационной сети Учреждения, используемые для передачи информации и соединения объектов информационной инфраструктуры Учреждения.

5.3. Точки консолидации информационно-телекоммуникационной сети Учреждения, используемые для соединения кабельных линий между собой и (или) с активным сетевым оборудованием.

5.4. Коммутационные центры и телекоммуникационные комнаты, в которых размещаются точки консолидации, коммутационные панели, сетевое, телекоммуникационное и иное оборудование информационно-телекоммуникационной сети Учреждения.

5.5. Точки разграничения информационно-телекоммуникационной сети Учреждения с информационно-телекоммуникационными сетями иных организаций, в том числе точки наружного подключения зданий.

5.6. Точки беспроводного доступа, являющиеся точками сопряжения проводной и беспроводной частей информационно-телекоммуникационной сети Учреждения.

6. Учетные записи, права доступа и средства аутентификации

6.1. Учетные записи Пользователей информационной инфраструктуры Учреждения, используемые для доступа к объектам информационной инфраструктуры Учреждения.

6.2. Учетные записи привилегированных Пользователей информационной инфраструктуры Учреждения, используемые работниками Учреждения, которым предоставлены полномочия по администрированию, сопровождению, настройке либо управлению объектами информационной инфраструктуры Учреждения.

6.3. Групповые учетные записи, используемые в случаях, обусловленных особенностями соответствующих объектов информационной инфраструктуры Учреждения.

6.4. Учетные записи, используемые лицами, не являющимися работниками Учреждения, которым предоставлен доступ к объектам информационной инфраструктуры Учреждения.

6.5. Права доступа, роли, полномочия и иные параметры разграничения доступа к информационным системам, информационным ресурсам, программным средствам и иным объектам информационной инфраструктуры Учреждения.

6.6. Средства аутентификации, используемые Пользователями информационной инфраструктуры и иными лицами при доступе к объектам информационной инфраструктуры Учреждения, в том числе пароли, ключевые носители, токены, сертификаты, одноразовые коды и иные аналогичные средства.

7. Машинные носители информации и резервные копии

7.1. Машинные носители информации, используемые в составе автоматизированных рабочих мест, серверного оборудования и иных средств вычислительной техники Учреждения.

7.2. Внешние машинные носители информации, используемые для хранения и (или) передачи информации.

7.3. Резервные копии информации и машинные носители, на которых они размещаются.

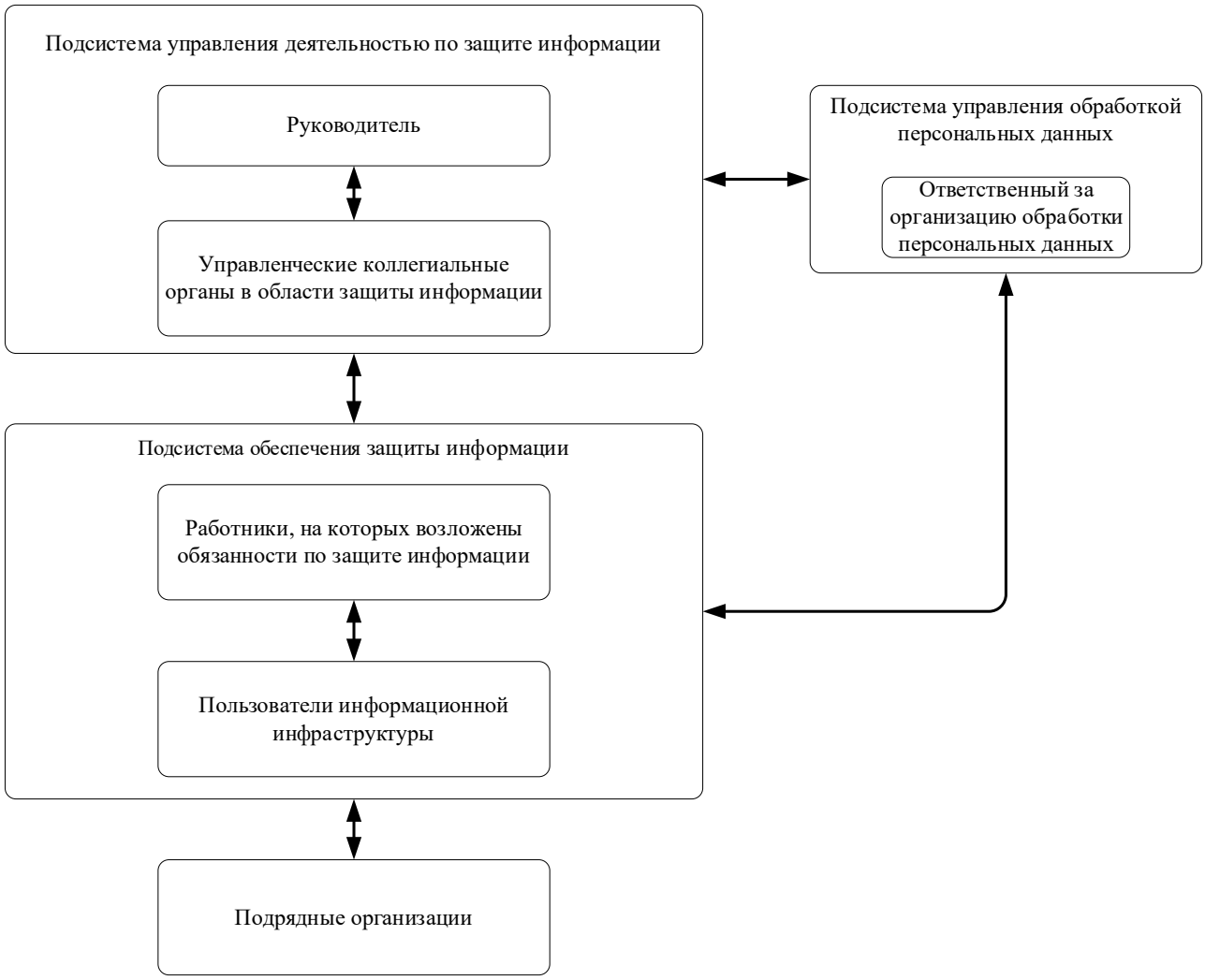
8. Помещения и места размещения объектов информационной инфраструктуры

8.1. Помещения, в которых размещаются серверное, сетевое, телекоммуникационное и иное оборудование, обеспечивающее функционирование информационной инфраструктуры Учреждения.

8.2. Помещения, в которых размещаются автоматизированные рабочие места и иные средства вычислительной техники, используемые для обработки информации.

Приложение 2
к Политике защиты информации

Схема взаимодействия элементов организационной системы управления деятельностью по защите информации



Приложение 3
к Политике защиты информации

Правила работы пользователя информационной инфраструктуры

1. Общие положения

1.1. Настоящие Правила работы пользователя информационной инфраструктуры (далее — Правила) определяют единые требования безопасной и допустимой работы работников Муниципального бюджетного общеобразовательного учреждения «Гимназия» (далее – Учреждение) при использовании объектов информационной инфраструктуры Учреждения.

1.2. Правила разработаны в целях реализации требований законодательства Российской Федерации, Политики защиты информации Учреждения и иных локальных актов Учреждения в области защиты информации.

1.3. Требования настоящих Правил являются обязательными для исполнения всеми работниками Учреждения, которым для исполнения должностных (трудовых) обязанностей предоставляется автоматизированное рабочее место.

1.4. Настоящие Правила применяются совместно с Политикой защиты информации, иными локальными актами Учреждения в области защиты информации, инструкциями пользователей информационных систем, эксплуатационной документацией, а также иными документами, регламентирующими обработку информации и использование объектов информационной инфраструктуры Учреждения.

1.5. Пользователь информационной инфраструктуры обязан соблюдать требования настоящих Правил в течение всего периода использования предоставленных ему объектов информационной инфраструктуры Учреждения.

1.6. Несоблюдение требований настоящих Правил рассматривается как нарушение требований Политики защиты информации Учреждения и может повлечь применение мер ответственности, предусмотренных законодательством Российской Федерации, локальными актами Учреждения, трудовым договором и иными документами, регулирующими трудовые отношения.

2. Статус Пользователя информационной инфраструктуры

2.1. Статус Пользователя информационной инфраструктуры возникает у работника Учреждения с момента предоставления ему автоматизированного рабочего места для исполнения должностных (трудовых) обязанностей.

2.2. Предоставление работнику Учреждения автоматизированного рабочего места является основанием для применения к нему требований настоящих Правил, Политики защиты информации и иных локальных актов Учреждения, регулирующих использование объектов информационной инфраструктуры.

2.3. Пользователь информационной инфраструктуры осуществляет использование предоставленных ему объектов информационной инфраструктуры исключительно в пределах полномочий, необходимых для исполнения должностных (трудовых) обязанностей.

2.4. При предоставлении Пользователю информационной инфраструктуры доступа к отдельным информационным системам, информационным ресурсам либо иным объектам информационной инфраструктуры Учреждения он приобретает статус пользователя соответствующих объектов и обязан соблюдать требования локальных актов, регулирующих порядок их использования.

2.5. Пользователю информационной инфраструктуры предоставляются только те права доступа, программные средства, информационные ресурсы и иные объекты

информационной инфраструктуры, которые необходимы для исполнения его должностных (трудовых) обязанностей.

2.6. Пользователь информационной инфраструктуры не вправе использовать предоставленные ему объекты информационной инфраструктуры для выполнения действий, не связанных с исполнением должностных (трудовых) обязанностей, за исключением случаев, предусмотренных локальными актами Учреждения.

2.7. Статус Пользователя информационной инфраструктуры прекращается при прекращении предоставления ему автоматизированного рабочего места, в том числе при прекращении трудовых отношений либо в иных случаях, предусмотренных локальными актами Учреждения.

3. Предоставление автоматизированного рабочего места

3.1. Автоматизированное рабочее место предоставляется работнику Учреждения для исполнения должностных (трудовых) обязанностей в соответствии с локальными актами Учреждения.

3.2. До начала использования автоматизированного рабочего места работник Учреждения должен быть ознакомлен с настоящими Правилами и иными обязательными для него локальными актами Учреждения в области защиты информации.

3.3. Работнику Учреждения предоставляются только те программные средства, средства вычислительной техники, средства аутентификации, информационные системы, информационные ресурсы и иные объекты информационной инфраструктуры, использование которых необходимо для исполнения его должностных (трудовых) обязанностей.

3.4. Пользователь информационной инфраструктуры обязан использовать предоставленные ему объекты информационной инфраструктуры исключительно по их назначению и в пределах предоставленных полномочий.

3.5. Передача автоматизированного рабочего места, средств вычислительной техники, носителей информации и иных материальных объектов информационной инфраструктуры другому лицу осуществляется в порядке, установленном локальными актами Учреждения.

3.6. В случае изменения должностных (трудовых) обязанностей Пользователя информационной инфраструктуры, предоставленные ему права доступа, состав используемых информационных систем, программных средств и иных объектов информационной инфраструктуры подлежат приведению в соответствие с новыми должностными (трудовыми) обязанностями.

3.7. При прекращении использования автоматизированного рабочего места Пользователь информационной инфраструктуры обязан возвратить предоставленные ему средства вычислительной техники, средства аутентификации, носители информации и иные материальные объекты информационной инфраструктуры в порядке, установленном локальными актами Учреждения.

4. Общие правила работы Пользователя информационной инфраструктуры

4.1. Пользователь информационной инфраструктуры обязан использовать объекты информационной инфраструктуры Учреждения исключительно для исполнения своих должностных (трудовых) обязанностей.

4.2. Пользователь информационной инфраструктуры обязан соблюдать требования законодательства Российской Федерации, Политики защиты информации Учреждения, настоящих Правил, иных локальных актов Учреждения, а также инструкций пользователей отдельных информационных систем, информационных ресурсов и иных объектов информационной инфраструктуры.

4.3. Пользователь информационной инфраструктуры обязан обеспечивать сохранность предоставленных ему средств вычислительной техники, средств аутентификации, носителей информации и иных объектов информационной инфраструктуры Учреждения.

4.4. Пользователь информационной инфраструктуры обязан использовать только предоставленные ему права доступа и не предпринимать действий, направленных на получение доступа к информации, информационным системам, информационным ресурсам либо иным объектам информационной инфраструктуры, доступ к которым ему не предоставлен.

4.5. Пользователь информационной инфраструктуры обязан использовать только предоставленные либо разрешенные Учреждением программные средства, оборудование, сервисы и иные объекты информационной инфраструктуры.

4.6. Пользователь информационной инфраструктуры обязан принимать разумные меры по предотвращению нарушения конфиденциальности, целостности и доступности защищаемой информации при выполнении своих должностных (трудовых) обязанностей.

4.7. Пользователь информационной инфраструктуры обязан незамедлительно сообщать непосредственному руководителю и работникам Учреждения, на которых возложены обязанности по защите информации, о выявленных нарушениях требований защиты информации, событиях и инцидентах информационной безопасности, а также об обстоятельствах, которые могут привести к их возникновению.

4.8. Пользователю информационной инфраструктуры запрещается совершать действия, способные привести к нарушению работоспособности объектов информационной инфраструктуры Учреждения, нарушению требований защиты информации либо причинению ущерба Учреждению, если такие действия не входят в его должностные (трудовые) обязанности и предоставленные полномочия.

4.9. В случаях возникновения вопросов по безопасному использованию объектов информационной инфраструктуры Пользователь информационной инфраструктуры обязан до совершения соответствующих действий обратиться за разъяснениями к непосредственному руководителю либо работникам Учреждения, на которых возложены обязанности по защите информации.

5. Работа с информацией

5.1. Пользователь информационной инфраструктуры осуществляет обработку информации исключительно в объеме и в целях, необходимых для исполнения своих должностных (трудовых) обязанностей.

5.2. Пользователь информационной инфраструктуры обязан обеспечивать соблюдение установленного Учреждением порядка обработки, использования, хранения, передачи и уничтожения информации в соответствии с требованиями законодательства Российской Федерации и локальных актов Учреждения.

5.3. Пользователь информационной инфраструктуры обязан использовать только достоверную, актуальную и официально полученную информацию, необходимую для выполнения возложенных на него обязанностей.

5.4. Пользователь информационной инфраструктуры не вправе использовать информацию, доступ к которой ему предоставлен в связи с исполнением должностных (трудовых) обязанностей, в личных целях либо в интересах третьих лиц.

5.5. Передача информации другим работникам Учреждения, третьим лицам, государственным органам, организациям и гражданам осуществляется только при наличии соответствующих полномочий и правовых оснований.

5.6. Копирование, тиражирование, публикация, распространение, уничтожение либо иное использование информации осуществляются Пользователем информационной инфраструктуры только в пределах предоставленных ему полномочий.

5.7. Пользователь информационной инфраструктуры обязан принимать меры, исключающие ознакомление посторонних лиц с информацией, доступ к которой ограничен законодательством Российской Федерации либо локальными актами Учреждения.

5.8. В случае ошибочного получения информации, доступ к которой Пользователю информационной инфраструктуры не предоставлен, либо выявления фактов неправомерного доступа к информации Пользователь информационной инфраструктуры обязан прекратить дальнейшее использование такой информации и незамедлительно сообщить об этом непосредственному руководителю либо работникам Учреждения, на которых возложены обязанности по защите информации.

5.9. Пользователь информационной инфраструктуры обязан обеспечивать сохранность информации до момента ее передачи, архивного хранения либо уничтожения в порядке, установленном законодательством Российской Федерации и локальными актами Учреждения.

6. Работа с информационными системами

6.1. Пользователь информационной инфраструктуры осуществляет работу только с теми информационными системами, информационными ресурсами и программными средствами, доступ к которым предоставлен ему для исполнения должностных (трудовых) обязанностей.

6.2. Доступ к информационным системам предоставляется Пользователю информационной инфраструктуры в объеме, необходимом для исполнения его должностных (трудовых) обязанностей, и не может использоваться в иных целях.

6.3. Пользователь информационной инфраструктуры обязан использовать информационные системы в соответствии с их функциональным назначением, эксплуатационной документацией, настоящими Правилами, а также инструкциями пользователей соответствующих информационных систем.

6.4. Пользователь информационной инфраструктуры не вправе изменять настройки информационных систем, средств защиты информации, программного обеспечения и иных объектов информационной инфраструктуры, если такие действия не входят в его должностные (трудовые) обязанности либо ему не предоставлены соответствующие полномочия.

6.5. Пользователь информационной инфраструктуры не вправе самостоятельно устанавливать, удалять, обновлять либо изменять программное обеспечение, если иное не предусмотрено его должностными (трудовыми) обязанностями или локальными актами Учреждения.

6.6. При работе с информационными системами Пользователь информационной инфраструктуры обязан использовать только предоставленные ему учетные записи, в том числе групповые учетные записи в случаях, когда право их использования предоставлено ему в установленном порядке, и не вправе использовать учетные записи, предоставленные другим Пользователям информационной инфраструктуры.

6.7. Передача другим лицам индивидуальных учетных записей, индивидуальных средств аутентификации либо предоставленных прав доступа к информационной системе запрещается.

6.8. При завершении работы Пользователь информационной инфраструктуры обязан корректно завершить работу с информационной системой в соответствии с требованиями эксплуатационной документации либо инструкции пользователя соответствующей информационной системы.

6.9. При обнаружении ошибок в работе информационной системы, подозрений на нарушение ее работоспособности либо признаков нарушения требований защиты информации Пользователь информационной инфраструктуры обязан прекратить выполнение действий, которые могут привести к увеличению последствий нарушения, и незамедлительно сообщить

об этом непосредственному руководителю либо работникам Учреждения, на которых возложены обязанности по защите информации.

6.10. Пользователю информационной инфраструктуры запрещается предпринимать действия, направленные на обход установленных ограничений доступа, средств защиты информации, механизмов регистрации событий безопасности либо иных механизмов обеспечения безопасности информационных систем.

7. Использование автоматизированного рабочего места

7.1. Автоматизированное рабочее место используется Пользователем информационной инфраструктуры исключительно для исполнения должностных (трудовых) обязанностей.

7.2. До начала работы Пользователь информационной инфраструктуры обязан убедиться в исправности автоматизированного рабочего места и отсутствии признаков, свидетельствующих о нарушении его работоспособности либо требований защиты информации.

7.3. Во время работы Пользователь информационной инфраструктуры обязан обеспечивать сохранность автоматизированного рабочего места, средств вычислительной техники, средств аутентификации, носителей информации и иных предоставленных ему объектов информационной инфраструктуры Учреждения.

7.4. При временном отсутствии на рабочем месте Пользователь информационной инфраструктуры обязан принять меры, исключающие возможность использования автоматизированного рабочего места посторонними лицами.

7.5. По окончании работы Пользователь информационной инфраструктуры обязан завершить работу информационных систем, выполнить действия, предусмотренные эксплуатационной документацией, и принять меры, исключающие возможность несанкционированного использования автоматизированного рабочего места.

7.6. Пользователь информационной инфраструктуры обязан обеспечивать сохранность предоставленных ему средств вычислительной техники и не вправе перемещать, разукомплектовывать, подключать либо отключать оборудование без соответствующих полномочий, если иное не предусмотрено локальными актами Учреждения.

7.7. Подключение к автоматизированному рабочему месту оборудования, устройств и иных технических средств осуществляется только в случаях, предусмотренных локальными актами Учреждения либо по согласованию с работниками, на которых возложены обязанности по защите информации или сопровождению информационной инфраструктуры Учреждения.

7.8. Пользователь информационной инфраструктуры обязан поддерживать автоматизированное рабочее место в состоянии, обеспечивающем его безопасную эксплуатацию, а также незамедлительно сообщать о выявленных неисправностях, повреждениях и иных обстоятельствах, препятствующих его безопасному использованию.

7.9. Самостоятельное вскрытие, ремонт, модернизация, изменение конфигурации либо иное вмешательство в конструкцию средств вычислительной техники допускаются только лицами, уполномоченными на выполнение соответствующих работ.

8. Использование внешних информационных ресурсов и сервисов

8.1. Пользователь информационной инфраструктуры вправе использовать сеть Интернет, электронную почту, средства обмена сообщениями, облачные сервисы, сервисы видеоконференцсвязи и иные внешние информационные ресурсы исключительно в пределах предоставленных полномочий и для исполнения должностных (трудовых) обязанностей.

8.2. Использование внешних информационных ресурсов и сервисов осуществляется с соблюдением требований законодательства Российской Федерации, Политики защиты информации, настоящих Правил и иных локальных актов Учреждения.

8.3. Пользователь информационной инфраструктуры обязан проявлять разумную осторожность при получении информации из внешних информационных ресурсов, открытии ссылок, загрузке файлов, использовании электронных сообщений, а также при взаимодействии с внешними информационными сервисами.

8.4. Пользователь информационной инфраструктуры не вправе размещать во внешних информационных ресурсах и сервисах информацию, распространение которой ограничено законодательством Российской Федерации либо локальными актами Учреждения.

8.5. Передача информации посредством электронной почты, средств обмена сообщениями, сервисов видеоконференцсвязи либо иных внешних информационных сервисов осуществляется только при наличии соответствующих полномочий и с соблюдением установленного порядка обмена информацией.

8.6. Пользователь информационной инфраструктуры не вправе использовать внешние информационные сервисы, если их использование запрещено законодательством Российской Федерации либо локальными актами Учреждения.

8.7. При возникновении сомнений в безопасности электронного сообщения, интернет-ресурса либо иного внешнего информационного сервиса Пользователь информационной инфраструктуры обязан воздержаться от совершения соответствующих действий и обратиться к работникам Учреждения, на которых возложены обязанности по защите информации либо сопровождению информационной инфраструктуры.

9. Использование внешних носителей и мобильных устройств

9.1. Подключение к объектам информационной инфраструктуры Учреждения внешних устройств, носителей информации и иных технических средств осуществляется только в случаях, предусмотренных локальными актами Учреждения либо при наличии соответствующих полномочий.

9.2. Пользователь информационной инфраструктуры обязан использовать только исправные и предназначенные для выполнения служебных задач внешние устройства и носители информации.

9.3. Пользователь информационной инфраструктуры не вправе использовать внешние устройства и носители информации, происхождение, содержание либо техническое состояние которых ему неизвестно или вызывает сомнения.

9.4. Использование личных внешних устройств и носителей информации допускается только в случаях, предусмотренных локальными актами Учреждения либо по согласованию с работниками, на которых возложены обязанности по защите информации или сопровождению информационной инфраструктуры.

9.5. Пользователь информационной инфраструктуры обязан обеспечивать сохранность предоставленных ему внешних устройств, носителей информации и иных технических средств, исключая возможность их утраты, повреждения либо использования посторонними лицами.

9.6. Передача внешних устройств и носителей информации другим лицам допускается только в порядке, установленном локальными актами Учреждения.

9.7. При обнаружении неисправности, повреждения, утраты либо признаков несанкционированного использования внешнего устройства или носителя информации Пользователь информационной инфраструктуры обязан незамедлительно сообщить об этом непосредственному руководителю либо работникам Учреждения, на которых возложены обязанности по защите информации.

9.8. Пользователь информационной инфраструктуры не вправе самостоятельно изменять конструкцию, технические характеристики, программное обеспечение либо режим работы предоставленных ему внешних устройств и носителей информации, если такие действия не входят в его должностные (трудовые) обязанности.

10. Использование средств аутентификации

10.1. Средства аутентификации предоставляются Пользователю информационной инфраструктуры для использования при доступе к объектам информационной инфраструктуры Учреждения в пределах предоставленных ему полномочий.

10.2. Пользователь информационной инфраструктуры обязан обеспечивать сохранность предоставленных ему индивидуальных средств аутентификации и использовать их только лично.

10.3. Пользователь информационной инфраструктуры не вправе передавать средства аутентификации, а также сведения, необходимые для их использования, другим лицам.

10.4. Пользователь информационной инфраструктуры обязан принимать меры, исключающие возможность компрометации средств аутентификации.

10.5. При возникновении подозрения на компрометацию средства аутентификации, его утрату, повреждение либо несанкционированное использование Пользователь информационной инфраструктуры обязан незамедлительно прекратить его использование и сообщить об этом непосредственному руководителю либо работникам Учреждения, на которых возложены обязанности по защите информации.

10.6. Изменение, восстановление, замена либо прекращение действия средств аутентификации осуществляются в порядке, установленном локальными актами Учреждения.

10.7. Использование индивидуальных средств аутентификации, предоставленных другим Пользователям информационной инфраструктуры, запрещается.

10.8. Пользователь информационной инфраструктуры обязан использовать только предоставленные ему средства аутентификации и только в пределах предоставленных полномочий.

10.9. В случае использования пароля в качестве средства аутентификации пароль должен соответствовать следующим требованиям:

– длина пароля — не менее 10 символов;

– пароль должен содержать символы не менее чем из трех следующих групп: строчные буквы, прописные буквы, цифры, специальные символы;

– пароль не должен состоять из общеизвестных слов, фамилий, имен, дат, номеров телефонов, наименований организаций, простых последовательностей символов либо иной информации, которая может быть легко угадана;

– пароль не должен совпадать с логином, именем учетной записи либо иными идентификаторами Пользователя информационной инфраструктуры;

– один и тот же пароль не должен использоваться Пользователем информационной инфраструктуры для служебных и личных учетных записей.

10.10. Пользователь информационной инфраструктуры обязан обеспечивать конфиденциальность пароля и не вправе сообщать его другим лицам, записывать в открытом виде, размещать на рабочем месте, сохранять в незащищенных файлах либо передавать с использованием незащищенных каналов связи.

10.11. Временный пароль используется только для первоначального предоставления доступа либо восстановления доступа и должен быть изменен Пользователем информационной инфраструктуры при первом входе, если такая возможность предусмотрена соответствующей информационной системой.

10.12. Пароль подлежит изменению при наличии признаков его возможной компрометации, а также в иных случаях, предусмотренных локальными актами Учреждения либо требованиями соответствующей информационной системы.

10.13. Периодичность плановой смены пароля устанавливается локальными актами Учреждения, требованиями соответствующей информационной системы либо ее настройками.

10.14. При вводе пароля Пользователь информационной инфраструктуры обязан принимать меры, исключающие возможность его просмотра посторонними лицами или фиксации техническими средствами.

10.15. При использовании группового пароля Пользователи информационной инфраструктуры, которым предоставлено право использования соответствующей групповой учетной записи, обязаны обеспечивать его конфиденциальность, не передавать его другим лицам и использовать соответствующую учетную запись только в пределах предоставленных полномочий.

10.16. При изменении состава Пользователей информационной инфраструктуры, которым предоставлен групповой пароль, а также при наличии признаков его возможной компрометации Пользователь информационной инфраструктуры, которому предоставлен групповой пароль, обязан сообщить об этом непосредственному руководителю либо работникам Учреждения, на которых возложены обязанности по защите информации.

11. Реагирование на события и инциденты информационной безопасности

11.1. При обнаружении событий, способных привести к нарушению конфиденциальности, целостности или доступности информации либо нарушению работоспособности объектов информационной инфраструктуры Учреждения, Пользователь информационной инфраструктуры обязан действовать в соответствии с требованиями настоящего раздела.

11.2. К событиям, требующим реагирования Пользователя информационной инфраструктуры, относятся, в том числе:

– утрата либо повреждение средств вычислительной техники, носителей информации или средств аутентификации;

– получение информации, доступ к которой Пользователю информационной инфраструктуры не предоставлен;

– попытки получения сведений ограниченного доступа посторонними лицами;

– обнаружение признаков несанкционированного доступа к объектам информационной инфраструктуры Учреждения;

– нарушение работоспособности информационных систем;

– получение подозрительных электронных сообщений, файлов, ссылок либо иных информационных материалов;

– иные события, способные привести к нарушению требований защиты информации.

11.3. При возникновении событий, указанных в пункте 11.2 настоящих Правил, Пользователь информационной инфраструктуры обязан:

– прекратить выполнение действий, способных увеличить последствия произошедшего события;

– по возможности обеспечить сохранность имеющейся информации о произошедшем событии;

– незамедлительно сообщить непосредственному руководителю либо работникам Учреждения, на которых возложены обязанности по защите информации;

– выполнять дальнейшие действия в соответствии с полученными указаниями.

11.4. Пользователю информационной инфраструктуры запрещается самостоятельно предпринимать действия, направленные на устранение последствий событий и инцидентов информационной безопасности, если выполнение таких действий не входит в его должностные (трудовые) обязанности.

11.5. Пользователь информационной инфраструктуры обязан содействовать проведению мероприятий по установлению причин произошедшего события либо инцидента информационной безопасности в пределах предоставленных ему полномочий.

11.6. Сокрытие событий и инцидентов информационной безопасности, несвоевременное сообщение о них либо умышленное воспрепятствование их расследованию не допускается.

12. Прекращение статуса Пользователя информационной инфраструктуры

12.1. Статус Пользователя информационной инфраструктуры прекращается при прекращении предоставления ему автоматизированного рабочего места, прекращении трудовых отношений с Учреждением, а также в иных случаях, предусмотренных локальными актами Учреждения.

12.2. Прекращение или изменение доступа Пользователя информационной инфраструктуры к отдельным информационным системам, информационным ресурсам либо иным объектам информационной инфраструктуры Учреждения не прекращает его статус Пользователя информационной инфраструктуры, если предоставленное ему автоматизированное рабочее место сохраняется.

12.3. При прекращении статуса Пользователя информационной инфраструктуры работник Учреждения обязан:

– прекратить использование предоставленных ему объектов информационной инфраструктуры;

– возвратить средства вычислительной техники, средства аутентификации, носители информации и иные материальные объекты информационной инфраструктуры, находящиеся в его пользовании;

– передать находящуюся в его ведении информацию, документы и материалы в порядке, установленном локальными актами Учреждения;

– сообщить о ставших ему известными обстоятельствах, способных повлиять на обеспечение защиты информации после прекращения его полномочий.

12.4. При изменении должности, структурного подразделения либо должностных (трудовых) обязанностей Пользователя информационной инфраструктуры предоставленные ему права доступа и состав используемых объектов информационной инфраструктуры подлежат приведению в соответствие с новыми должностными (трудовыми) обязанностями.

12.5. После прекращения статуса Пользователя информационной инфраструктуры обязанность соблюдать требования законодательства Российской Федерации, трудового договора, соглашений и локальных актов Учреждения о защите конфиденциальной информации сохраняется в случаях, предусмотренных законодательством Российской Федерации и указанными документами.

13. Ответственность Пользователя информационной инфраструктуры

13.1. Пользователь информационной инфраструктуры несет ответственность за соблюдение требований по защите информации при работе с информацией и объектами информационной инфраструктуры, к которым ему предоставлен доступ, в пределах возложенных на него обязанностей и предоставленных полномочий.

13.2. Пользователь информационной инфраструктуры несет ответственность за действия (бездействие), совершенные при использовании предоставленных ему автоматизированного рабочего места, учетной записи, средств аутентификации и иных объектов информационной инфраструктуры, в порядке, установленном законодательством Российской Федерации, трудовым договором и локальными актами Учреждения.

13.3. Нарушение Пользователем информационной инфраструктуры требований настоящих Правил является основанием для проведения проверки обстоятельств нарушения и применения мер ответственности в порядке, установленном законодательством Российской Федерации, трудовым договором и локальными актами Учреждения.

13.4. В случае причинения Учреждению ущерба вследствие виновных действий (бездействия) Пользователя информационной инфраструктуры вопрос о привлечении его к ответственности решается в соответствии с законодательством Российской Федерации.

13.5. Применение мер ответственности к Пользователю информационной инфраструктуры не освобождает его от обязанности устранить допущенные нарушения, если такое устранение возможно и входит в его полномочия.