Министерство образования Московской области

Государственное бюджетное профессиональное образовательное учреждение Московской области «Орехово-Зуевский железнодорожный техникум имени В.И. Бондаренко»

(ГБПОУ МО «ОЗЖТ имени В.И. Бондаренко»)

ПРИКАЗ

27.08.2026г. № 337

Об утверждении Политики защиты информации в ГБПОУ МО «Орехово- Зуевский железнодорожный техникум им. В.И. Бондаренко»

Парамонов Сергей Сергеевич

Подписан: Парамонов Сергей Сергеевич
DN: C=RU, S=Московская область, L=Орехово-Зуево, T=директор, O="ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ МОСКОВСКОЙ ОБЛАСТИ ""ОРЕХОВО-ЗУЕВСКИЙ ЖЕЛЕЗНОДОРОЖНЫЙ ТЕХНИКУМ ИМЕНИ В.И. БОНДАРЕНКО""", СНИЛС=11832280032, ИНН=503500837815, E=ry1oreh@mail.ru, G=Сергей Сергеевич, SN=Парамонов, CN=Парамонов Сергей Сергеевич
Основание: Я являюсь автором этого документа
Местоположение: место подписания
Дата: 2026.08.28 09:19:45+03'00'
Foxit Reader Версия: 10.1.3

В соответствии с Распоряжением Министерства образования Московской области от 03.08.2026 № Р-505 «Об утверждении Политики защиты информации в Министерстве образования Московской области», в целях обеспечения защиты информации в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», приказом Федеральной службы по техническому и экспортному контролю 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»,

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемую Политику защиты информации в ГБПОУ МО «Орехово-Зуевский железнодорожный техникум им. В.И. Бондаренко».
2. Признать утратившим силу Приложение 90 к приказу ГБПОУ МО «ОЗЖТ имени В.И. Бондаренко» от 02.09.2024 № 397 Положение об информационной безопасности ГБПОУ МО «Орехово-Зуевский железнодорожный техникум имени В.И. Бондаренко».
3. Программисту Васильевых Д.Н. разместить утвержденную Политику на официальном сайте техникума в сети Интернет в установленные сроки.
4. Настоящий приказ вступает в силу с 1 сентября 2026 г.

Директор С.С. Парамонов

С приказом ознакомлены:

Приложение
к приказу от 27.08.2026г. № 337

УТВЕРЖДЕНО
приказом по ГБПОУ МО «Орехово-Зуевский железнодорожный техникум им. В.И. Бондаренко»
от 27.08.2026г. № 337

Политика защиты информации в ГБПОУ МО «Орехово- Зуевский железнодорожный техникум им. В.И. Бондаренко»

1. Общие положения

1.1. Политика защиты информации в государственном бюджетном профессиональном образовательном учреждении Московской области «Орехово-Зуевский железнодорожный техникум имени В.И. Бондаренко» (далее – Политика) определяет основные принципы, определяющие задачи и методы обеспечения защиты информации в ГБПОУ МО «Орехово-Зуевский железнодорожный техникум имени В.И. Бондаренко» (далее — Техникум) в целях достижения целей деятельности в области обеспечения защиты информации.

1.2. Иные внутренние документы, описывающие процедуры обеспечения защиты информации в Техникуме, разрабатываются с учетом требований Политики.

2. Область применения политики защиты информации в Техникуме

2.1. Настоящая Политика устанавливает обязательные требования к защите информации в информационных системах Техникума, его ИТ-инфраструктуре, а также в процессах обработки, хранения и передачи информации ограниченного доступа, включая персональные данные и иные информационные активы.

2.2. Требования Политики распространяются на:

информационные системы (далее - ИС) и ИТ-инфраструктуру на всех этапах их жизненного цикла: создание (разработка, внедрение), эксплуатация, вывод из эксплуатации;

работников Техникума (далее - сотрудники).

2.3. Требования Политики также распространяются на взаимоотношения Техникума с внешними организациями, включая:

поставщиков товаров и услуг;

подрядчиков, выполняющих работы по созданию, модернизации, обслуживанию или сопровождению ИС и ИТ-инфраструктуры;

иных контрагентов, услуги которых связаны с использованием, обработкой или доступом к информации или информационным активам Техникума.

Сотрудники Техникума при взаимодействии с внешними организациями в целях обеспечения информационной безопасности обязаны обеспечить:

ознакомление с настоящей Политикой и принятие её положений в качестве обязательных условий взаимодействия;

включение в договоры, контракты и соглашения с Техникумом пунктов об обязательствах по защите информации, порядке реагирования на инциденты защиты информации и ответственности за нарушение требований безопасности. 2.4. Контроль за соблюдением требований настоящей Политики осуществляется инженером по защите информации Техникума (далее — инженер).

3. Термины и определения

Авторизация – процесс предоставления пользователю прав доступа к определенным ресурсам, функциям или данным системы после успешной аутентификации.

Анализ угроз – процесс изучения природы и характера угроз информационной безопасности.

Атака – попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к ИТ-активу или его несанкционированного использования.

Аудит – систематический, независимый и задокументированный процесс, предназначенный для получения свидетельств аудита и объективной оценки аудиторами степени соблюдения критериев аудита.

Аутентификация – обеспечение гарантии того, что заявленные характеристики субъекта или объекта подлинные.

Аутентификационная информация – информация, используемая при аутентификации субъекта доступа или объекта доступа (в том числе – пароль пользователя).

Информация – совокупность данных (в электронной, письменной или устной форме), которая обрабатывается в Техникуме, а также используется для

поддержки процессов Техникума. Информация, которая создается третьими лицами от имени Техникума и информация, на которую Техникум владеет авторскими правами, также относится к информации Техникума.

Документированная информация – информация, которая должна управляться и поддерживаться Техникумом, в том числе носитель, содержащий такую информацию.

Достоверность – свойства соответствия предусмотренному поведению и результатам.

Доступность – свойство, определяющее возможность использования объекта авторизованным субъектом по запросу.

Защищаемый объект информации — объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем её защищённости.

Защита информации или Информационная безопасность – сохранение конфиденциальности, целостности и доступности информации.

Информационная система – набор приложений, услуг, информационно-технических активов или других компонентов для обработки информации.

Инцидент информационной безопасности – одно или несколько нежелательных или неожиданных событий информационной безопасности, которые с высокой степенью вероятности могут привести к компрометации в бизнес-процессах и создают угрозы для информационной безопасности.

ИТ-актив - элемент инфраструктуры организации, который имеет ценность для процессов организации в сфере информационных технологий.

Конфиденциальность – недоступность для неавторизованных лиц, объектов или процессов.

Мера обеспечения информационной безопасности – мера, направленная на снижение угрозы информационной безопасности.

Мониторинг – определение состояния системы, процесса или вида деятельности.

Обеспечение непрерывности информационной безопасности – процессы и процедуры, гарантирующие непрерывность операций по обеспечению информационной безопасности.

Процесс – набор взаимосвязанных или взаимодействующих мероприятий, в результате которых исходные ресурсы преобразуются в конечный продукт.

Руководство деятельностью по обеспечению информационной безопасности – система, с помощью которой контролируется и управляется деятельность Техникума в области обеспечения информационной безопасности.

Событие информационной безопасности – выявленное состояние системы, услуги или сети, указывающее на возможное нарушение политики обеспечения информационной безопасности или сбой мер обеспечения информационной безопасности, или ранее неизвестная ситуация, которая может иметь отношения к вопросам безопасности.

Средства обработки информации – совокупность автономных устройств сбора, накопления, передачи, обработки и представления информации.

Угроза – совокупность условий и факторов, создающих опасность нарушения информационной безопасности как отдельно взятому активу, так и Техникуму в целом.

Управление доступом – обеспечение санкционированного доступа к активам в соответствии с бизнес-требованиями и требованиями безопасности.

Уязвимость информационной безопасности – слабое место актива или меры обеспечения информационной безопасности, которое может быть использовано одной или несколькими угрозами.

Целостность – свойство сохранения правильности и полноты активов.

4. Нормативные документы

4.1. Политика разработана с учетом требований следующих нормативных правовых актов:

1) Конституция Российской Федерации.

2) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3) Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

4) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

5) Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности».

6) Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

7) Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера».

8) Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

9) Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

10) Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

11) Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

12) Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

13) Приказ 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».

14) Приказ ФСО России от 07.09.2016 № 443 «Об утверждении положения о российском государственном сегменте информационно-телекоммуникационной сети «Интернет».

15) ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

16) ГОСТ Р 59407-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных».

17) ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

18) ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности. Общие положения».

19) ГОСТ Р 59453.3-2025 «Защита информации. Формальная модель управления доступом. Часть 3. Рекомендации по разработке».

20) Иные нормативные правовые акты Российской Федерации и нормативные документы уполномоченных в области обеспечения безопасности информации органов государственной власти.

5. Цели и задачи защиты информации

5.1. В соответствии с действующим законодательством Российской Федерации в области защиты информации и обеспечения безопасности, настоящей Политикой определены следующие цели защиты информации:

обеспечение корректности и непрерывности осуществления функций в рамках возложенных на Техникум полномочий;

обеспечение (защита) прав граждан, установленных законодательством Российской Федерации в области защиты информации, а также реализация прав граждан и организаций на получение, распространение и использование информации;

обеспечение органов, организаций и граждан достоверной, полной и своевременной информацией, необходимой для принятия решений, а также предотвращение нарушений целостности и незаконного использования информационных ресурсов Техникума.

5.2. Достижение установленных целей защиты информации обеспечивается посредством реализации мероприятий, направленных на обеспечение следующих ключевых свойств информации:

конфиденциальность информации;

целостность информации;

доступность информации.

5.3. Реализация указанных целей достигается за счет решения следующих задач:

управление информационной безопасностью, в том числе определение ролей и обязанностей в области информационной безопасности всех сотрудников;

определение защищаемых ресурсов (информации, информационных систем и сервисов, оборудования и иных ресурсов);

определение защищаемых ИТ-активов;

классификация информационных активов;

определение критических процессов деятельности;

определение актуальных для критических процессов угроз информационной безопасности;

обеспечение безопасности информационных активов в соответствии с категорией их классификации и оценкой актуальных угроз информационной безопасности;

мониторинг событий информационной безопасности, реагирование на них и управление инцидентами информационной безопасности;

организация и контроль обеспечения безопасного управления жизненным циклом информационных систем и ресурсов;

обеспечение непрерывности функциональных процессов;

снижение риска нарушения конфиденциальности, целостности и доступности информации путем определения правил использования информации и информационных систем;

распространение информации об общих правилах информационной безопасности среди сотрудников Техникума и третьих лиц, которая определяет обязанности, ответственность и роли каждого сотрудника;

обеспечение соответствия Политики действующему законодательству Российской Федерации, в том числе в области защиты информации, а также требованиям регуляторов.

6. Принципы защиты информации

6.1. Принципы обеспечения информационной безопасности определяют основные необходимые действия и мероприятия, выполнение которых является обязательным условием построения защищенного рабочего процесса в Техникуме, являются обязательными и соблюдаются всеми сотрудниками, а также иными лицами, которые имеют доступ к информации или информационным системам.

6.2. В Техникуме деятельность по защите информации реализуется на основе следующих принципов информационной безопасности:

Активность: активное использование всех доступных сил и средств для защиты информации, в том числе нестандартных подходов и методов, проактивный подход к выявлению и устранению угроз;

Взаимодействие и координирование работы: обеспечение эффективного взаимодействия и координации усилий между всеми участниками системы защиты информации для достижения общих целей;

Законность: применяемые способы и меры защиты соответствуют требованиям законодательства Российской Федерации в области защиты информации и требованиям регуляторов;

Инновационность: использование новых технологий и подходов, обеспечивающих повышение результативности и эффективности принимаемых организационно-технических мер ИБ;

Квалификация (развитие компетенций и профессионализма): привлечение квалифицированных специалистов и организаций, имеющих соответствующие лицензии и сертификаты, к разработке и внедрению системы защиты информации;

необходимость постоянного развития компетенций и практических навыков специалистов по информационной безопасности в условиях непрекращающегося

изменения рисков ИБ, ландшафта используемых информационных технологий и техник потенциальных нарушителей;

Комплексность: обеспечение многоуровневой защиты всех элементов, связанных с информацией: сотрудников, физических и информационных ресурсов, охватывающей все этапы жизненного цикла информации (создание, хранение, обработка, использование, архивирование, уничтожение);

Непрерывность: постоянное поддержание работоспособности и развитие системы защиты, постоянное совершенствование мер безопасности;

Ответственность: каждый сотрудник Техникума несёт ответственность за надлежащее использование информационных активов;

Повышение культуры информационной безопасности: повышение осведомленности сотрудников Техникума, а также третьих лиц в области информационной безопасности (далее — ИБ), демонстрация профессионального и этичного отношения к деятельности в области ИБ;

Проактивность: применение превентивных мер защиты, а именно мониторинг, анализ и оценка появляющихся, актуальных и будущих угроз информационной безопасности (включая изучение технологий, используемых злоумышленниками) с целью своевременного и осознанного принятия превентивных мер для предупреждения компьютерных атак и недопущения ущерба Техникуму;

Совершенствование информационной безопасности: обеспечение постоянного улучшения существующей практики и совершенствования средств и методов управления и обеспечения информационной безопасности на основе результатов аудитов информационной безопасности, мониторинга функционирования систем информационной безопасности, анализа изменений в методах и средствах компьютерных атак, анализа нормативных требований и существующего передового отечественного и зарубежного опыта в этой области;

Экономическая рациональность: соблюдение баланса между затратами на защиту информации и потенциальным ущербом от нарушения безопасности.

Требования информационной безопасности учитываются на всех этапах жизненного цикла ИТ-актива вне зависимости от уровня конфиденциальности информации, обрабатываемой в ИТ-активе.

Создание программных продуктов в интересах Техникума осуществляется с применением методов безопасной разработки программного обеспечения.

Предпочтительными являются ИТ-активы с наибольшим покрытием требований информационной безопасности встроенными функциями (при прочих равных характеристиках). Встроенные функции по информационной безопасности должны быть настроены и использоваться при эксплуатации ИТ-активов, включая программно-аппаратные средства, автоматизированные системы управления.

Соответствие приобретаемого/внедряемого ИТ-актива требуемому уровню информационной безопасности подтверждается с учетом требований законодательства Российской Федерации.

7. Категории лиц, участвующих в защите информации

7.1. В целях реализации Политики лица, отвечающие за обеспечение информационной безопасности, в том числе сотрудники Техникума или третьей стороны, в соответствии с требованиями законодательства Российской Федерации и локальными нормативными актами Техникума:

Инженер:

с учетом требований законодательства Российской Федерации и требований регуляторов, определяет необходимую квалификацию для лиц, обеспечивающих информационную безопасность, подтверждаемую соответствующим образованием, профессиональной подготовкой (стажировкой/переподготовкой) и/или опытом работы;

обеспечивает систематическое обучение (повышение квалификации) лиц, обеспечивающих информационную безопасность;

осуществляет стратегическое управление деятельностью в области защиты информации;

осуществляет принятие стратегических решений в целях обеспечения защиты информации в Техникуме;

осуществляет организацию мероприятий по защите информации, относящихся ко всем структурным подразделениям Техникума;

осуществляет обеспечение процессов информационной безопасности необходимыми ресурсами;

осуществляет контроль исполнения требований законодательства Российской Федерации и принятых решений в области защиты информации в Техникуме;

осуществляет реализацию технических и организационных мероприятий по защите информации;

осуществляет анализ состояния защищенности информации;

осуществляет анализ угроз информации;

осуществляет разработку проектов организационно-распорядительной и эксплуатационной документации в области защиты информации;

осуществляет организацию и проведение мероприятий по повышению осведомленности сотрудников Техникума в области защиты информации;

осуществляет своевременное реагирование на возникающие угрозы информации;

осуществляет расследование компьютерных инцидентов;

осуществляет подготовку предложений по модернизации защиты информации;

Эффективность процессов обеспечения ИБ Техникума достигается путем полноценного участия инженера на всех этапах деятельности по защите и обеспечению информационной безопасности.

8. Основы деятельности по обеспечению защиты информации

8.1. Инженер планирует, реализует и контролирует деятельность, необходимую для обеспечения защиты информации в Техникуме, а также реализует планы по достижению целей такой деятельности.

8.2. Инженер выпускает и хранит документированную информацию в объеме, необходимом для организации деятельности по обеспечению защиты информации.

8.3. Инженер управляет запланированными изменениями деятельности по обеспечению защиты информации и анализирует последствия внеплановых изменений, принимая меры по снижению любых неблагоприятных последствий.

8.4. Процессы деятельности по обеспечению защиты информации, осуществляемые с привлечением подрядных организаций, определяются и контролируются инженером.

9. Состав организационной системы управления деятельностью по защите информации

9.1. Управление деятельностью по защите информации представляет собой комплекс мероприятий по планированию, разработке, внедрению, документированию и контролю деятельности по обеспечению защиты информации в Техникуме и является постоянно действующей неотъемлемой частью общей системы управления Техникумом. Основными принципами функционирования системы управления деятельностью по защите информации являются:

надежность;

совместимость;

эффективность использования, в том числе экономическая;

непрерывность.

9.2. Основными этапами создания системы управления деятельностью по защите информации являются:

анализ деятельности и выявление критических процессов организации ИБ, а также информации, использующейся в этих процессах;

выявление и оценка рисков ИБ;

создание внутренней документации в части защиты информации;

выбор и реализация мер по защите информации;

разработка организационно-распорядительной и технической документации;

проведение регулярного контроля деятельности по защите информации.

9.3. Система управления позволяет создать непрерывный цикл процессов защиты информации, состоящий из следующих этапов:

Планирование: анализ текущего состояния информационной безопасности, определение целей и задач системы защиты, разработка/доработка политик и процедур, выявление рисков и угроз, составление плана мероприятий по защите информации;

Действие: внедрение технических средств защиты, обучение персонала, разработка документации, установка процессов мониторинга, проведение контрольных мероприятий;

Проверка: проведение аудита внедрённых мер защиты, оценка эффективности реализованных решений, сбор данных о нарушениях информационной безопасности, анализ инцидентов, проверка на соответствие стандартам;

Улучшение: корректировка выявленных недостатков, обновление политик и процедур, модернизация технических средств, совершенствование процессов управления, повторное планирование с учётом полученного опыта.

10. Перечень объектов защиты

10.1. В своей деятельности сотрудники Техникума обрабатывают (создание/сбор, обработка, использование, уничтожение) следующие виды информации:

персональные данные;

информация ограниченного доступа;

открытые данные.

Сотрудники Техникума обрабатывают вышеуказанную информацию как с помощью технических средств, включая обмен по каналам передачи данных, так и без применения таких средств (в ручном режиме).

Инженер осуществляет деятельность по защите информации в отношении следующих объектов (ИТ-активов):

государственные информационные системы (включая компоненты таких информационных систем и обрабатываемую в них информацию);

аппаратные компоненты информационно-телекоммуникационной инфраструктуры; программные компоненты информационно-телекоммуникационной инфраструктуры;

среды передачи данных (включая сетевое оборудование, средства

криптографической защиты и иное);

базы данных (включая программные компоненты таких баз и данные, содержащиеся в них);

архивные хранилища данных (включая программные компоненты таких баз и данные, содержащиеся в них).

11. Организация и поддержка процессов обеспечения защиты информации

11.1. Сотрудники и лица, выполняющие работу в интересах и под контролем инженера, обязаны ознакомиться:

с Политикой:

с их обязанностями в обеспечении результативности мероприятий по обеспечению информационной безопасности, включая пользу от их вклада в процессы улучшения мероприятий по обеспечению информационной безопасности;

с последствиями несоблюдения требований по обеспечению информационной безопасности.

11.2. Инженером обеспечивается взаимодействие между структурными подразделениями, а также с третьими физическими и юридическими лицами по вопросам, имеющим отношение к процессам обеспечения информационной безопасности, учитывая:

предмет взаимодействия;

период и сроки взаимодействия;

вид субъекта взаимодействия;

роли при взаимодействии;

процедуры осуществления взаимодействия.

11.3. Организация и поддержка процессов обеспечения информационной безопасности Техникума включает:

документационное обеспечение процессов и мер в соответствии с законодательством Российской Федерации и требованиями регуляторов в соответствующей области применения;

документационное обеспечение, определяемое инженером как необходимое для обеспечения результативности процессов информационной безопасности.

11.4. Для управления документационным обеспечением инженер осуществляет:

распространение, обеспечение доступа, поиск и использование информации;

хранение и обеспечение сохранности информации;

архивное хранение и уничтожение информации.

12. Основные требования к обеспечению защиты информации в Техникуме

12.1. Требования по обеспечению защиты информации формируются для следующих областей:

управление доступом;

физическая безопасность и защита от воздействий окружающей среды;

области, ориентированные на конечного пользователя (информационные активы, передача информации, дистанционная работа, ограничения в работе);

резервное копирование;

защита от вредоносного кода (антивирусная защита);

управление техническими уязвимостями;

криптография;

безопасность коммуникаций;

конфиденциальность и защита персональных данных;

взаимодействие с контрагентами.

13. Управление доступом

13.1. Пользователи ИТ-активов по согласованию с инженером определяют соответствующие правила управления доступом, права доступа и ограничения для конкретных ролей сотрудников Техникума по отношению к своим активам с уровнем детализации и набором мер, отражающих риски, связанные с обеспечением информационной безопасности.

13.2. В Техникуме учитываются:

требования безопасности функциональных приложений;

политики распространения информации и авторизации;

законодательные и любые договорные обязательства, касающиеся ограничения доступа к данным или сервисам;

управление правами доступа в распределенных средах и сетях, которые допускают все типы соединений;

разделение ролей по управлению доступом, например, запрос доступа, авторизация доступа, администрирование доступа;

требования к формальной авторизации результатов запросов доступа;

требования к периодическому пересмотру прав доступа;

аннулирование прав доступа;

логирование записей всех значимых событий, касающихся использования и управления идентификаторами пользователей и закрытой аутентификационной информацией.

13.3. В отношении использования сетей и сетевых сервисов учитываются:

сети и сетевые сервисы, к которым разрешен доступ;

процедуры авторизации для определения ролей и разрешений доступа к сетям и сетевым сервисам;

меры управления и процедуры для защиты доступа к сетевым соединениям и сетевым сервисам;

средства, используемые для доступа к сетям и сетевым сервисам VPN или беспроводным сетям;

требования к аутентификации и авторизации пользователя для доступа к различным сетевым сервисам;

мониторинг использования технических средств, программного обеспечения, сетевых сервисов и ресурсов.

13.4. Процесс управления идентификаторами сотрудников Техникума включает:

использование уникальных идентификаторов пользователей, позволяющих фиксировать несанкционированные действия пользователей;

своевременное отключение или удаление идентификаторов уволенных сотрудников;

выявление и удаление/блокирование избыточных идентификаторов пользователей;

исключение возможности передачи идентификаторов пользователей другим пользователям и третьим лицам;

безопасное хранение учетных записей пользователей;

требования к парольной защите.

13.5. Процесс предоставления или аннулирования прав доступа и регламентированных действий для идентификаторов пользователей включает:

получение разрешения от владельца информации, информационной системы или сервиса на использование этой информации, информационной системы или сервиса;

проверку предоставления уровня доступа соответствующего политикам доступа;

недопущение активации права доступа (в том числе поставщикам/поставщикам услуг) до завершения процедур аутентификации;

ведение централизованной регистрации прав доступа к информационным системам и сервисам, связываемым с идентификатором пользователя;

корректировку прав доступа пользователей, у которых поменялись роли или задачи;

периодический контроль, а при необходимости пересмотр прав доступа совместно с владельцами информационных систем или сервисов.

При пересмотре прав доступа учитываются:

пересмотр прав доступа как через определенные интервалы времени, так и после любых изменений статуса сотрудников (таких как повышение или понижение в должности, или увольнение);

регулярные проверки назначенных пользовательских привилегий.

13.6. Сотрудники Техникума ознакамливаются:

о необходимости тайного хранения закрытой аутентификационной информации в целях исключения ее компрометации;

о недопустимости открытого хранения записей закрытой аутентификационной информации (например, на бумаге, в файле программного обеспечения или на мобильном устройстве), кроме тех случаев, когда эти записи могут быть надежно сокрыты, а способ хранения согласован с подразделением, ответственным за обеспечение информационной безопасности;

о необходимости изменять закрытую аутентификационную информацию всякий раз, когда есть какие-либо подозрения или признаки ее возможной компрометации;

о необходимости использования уникальных, сложных паролей с регламентированной минимальной длиной в качестве закрытой аутентификационной информации;

о недопустимости использования идентичного набора символов пароля, используемого для доступа к информационным системам и сервисам Техникума, в личных целях;

о недопустимости использования ведомственных ресурсов в личных целях.

14. Физическая безопасность и защита от воздействия окружающей среды

14.1. Инженер предпринимает исчерпывающие меры по физической защите конфиденциальной информации, а также средств хранения и обработки такой информации. В Техникуме определяются периметры безопасности зон обработки и хранения конфиденциальной информации, а также зон расположения автоматизированных средств хранения и обработки такой информации.

14.2. В целях обеспечения физической защиты конфиденциальной информации реализуются следующие меры (но не ограничиваясь перечисленным):

разработка комплекта организационно-распорядительной документации по физической защите информации и средств ее обработки и хранения;

определение периметров безопасности с учетом расположения и степени защиты каждого из них, зависящие от требований безопасности активов в пределах периметра и с учетом рисков;

организация пропускного и внутриобъектового режима;

периметровое видеонаблюдение;

предоставление доступа в помещения Техникума только авторизованному персоналу.

15. Защита конечного пользователя

15.1. Сотрудники Техникума и внешние пользователи, использующие или имеющие доступ к ИТ-активам Техникума, должны быть осведомлены о требованиях информационной безопасности, относящихся к информации, ИТ-активам Техникума, связанным с информацией, средствам и ресурсам обработки информации, об ответственности за неправомерное использование ими любых ресурсов обработки информации и любое подобное использование, осуществляемое в зоне их ответственности.

В Техникуме применяется политика «чистого стола» в отношении бумажных документов и сменных носителей информации, а также политика «чистого экрана» для средств обработки информации.

Политика «чистого стола» и «чистого экрана» учитывает категории информации, законодательные и договорные требования, а также соответствующие риски и требования работы с информацией, предусмотренные Политикой.

15.2. Меры обеспечения информационной безопасности, которым необходимо следовать при использовании средств связи для передачи информации, учитывают: процедуры, предназначенные для защиты передаваемой информации
от копирования, модификации и уничтожения;

процедуры обнаружения и защиты от вредоносных программ, которые могут передаваться с использованием электронных средств связи;

процедуры для защиты информации ограниченного доступа в электронном виде, передаваемой в форме вложения;

процедуры, определяющие допустимое использование средств связи;

обязанности сотрудников и третьих лиц не предпринимать действий, ставящих под угрозу интересы Техникума;

использование криптографических методов, в том числе для защиты конфиденциальности, целостности, доступности и аутентичности информации;

процедуры, определяющие сроки хранения и утилизации информации, учитывающие нормы и требования законодательства Российской Федерации;

ограничения, связанные с использованием средств связи, включая сервис электронной почты;

рекомендации персоналу о мерах предосторожности во избежание раскрытия конфиденциальной информации.

16. Резервное копирование

16.1. В рамках мероприятий по обеспечению восстановления информационных систем и ресурсов после сбоев, инженер реализует мероприятия по резервному копированию обрабатываемой информации, которые направлены на достижение следующих целей:

обеспечение безопасности данных в случае наступления случайных или преднамеренных угроз, таких как сбои оборудования, вирусные или хакерские атаки, естественные бедствия;

гарантия доступности информации в случае ее утраты или повреждения, обеспечение скорейшего восстановления ресурсов и минимизации простоев;

соответствие требованиям законодательства Российской Федерации и стандартам информационной безопасности;

защита от потери информации, позволяющая предотвратить потерю важных данных, в том числе из-за случайного удаления, ошибок пользователя или неисправностей оборудования;

обеспечение непрерывности процессов за счет регулярного создания резервных копий и разработки стратегий восстановления данных.

16.2. Резервные копии информации и программного обеспечения создаются на регулярной основе с помощью средств резервного копирования, обеспечивающие возможность восстановления всей важной информации и программного обеспечения после аварии, сбоя носителя или иного инцидента.

При выполнении резервного копирования учитываются следующие меры:

ведется точный и полный учет резервных копий, а также документирование процедур восстановления;

объем (например, полное или частичное резервное копирование) и частота резервного копирования соответствуют требованиям функциональных процессов деятельности, требованиям безопасности, а также важности информации для непрерывной работы;

резервированная информация имеет соответствующий уровень защиты, как физической, так и от угроз окружающей среды;

носители резервных копий регулярно проверяются, процедура проверки совмещается с процедурой восстановления;

тестирование возможности восстановления данных из резервной копии

выполняется на выделенных для этого ресурсах;

резервные копии, содержащие информацию конфиденциального характера, защищаются с помощью шифрования.

16.3. Эксплуатационные процедуры контролируют выполнение резервного копирования и обрабатывают результаты в ходе запланированного резервного копирования, чтобы обеспечить полноту и результативность резервного копирования в соответствии с политикой резервного копирования, при разработке которой необходимо учитывать требования настоящей Политики.

17. Защита от вредоносного кода

17.1. Инженер реализует меры защиты от вредоносного кода, реализуя меры обеспечения информационной безопасности, связанные с обнаружением, предотвращением и восстановлением ИТ-инфраструктуры, в сочетании с соответствующим информированием пользователей.

Защита от вредоносных программ основывается на применении ПО для обнаружения вредоносных программ, осведомленности сотрудников в части требований информационной безопасности, соответствующих мерах контроля доступа к информационным системам Техникума и управлении изменениями.

17.2. Применяются следующие меры:

запрет на использование неавторизованного программного обеспечения;

реализация мер информационной безопасности, направленных на предотвращение или обнаружение использования неавторизованного программного обеспечения;

внедрение мер обеспечения информационной безопасности, которые предотвращают или обнаруживают обращение к известным или предполагаемым вредоносным веб-сайтам;

реализация процедур защиты от рисков, связанных с получением вредоносных файлов и программного обеспечения из внешних сетей или через них, либо иными способами;

минимизация прав пользователей;

применение двухфакторной аутентификации;

своевременный мониторинг инфраструктуры на предмет уязвимостей, в том числе с использованием официальных источников соответствующей информации;

выявление уязвимостей с использованием специализированного ПО через определенные временные интервалы;

проведение регулярных проверок программного обеспечения и содержимого систем, поддерживающих критические бизнес-процессы;

регулярное обновление программного обеспечения;

создание и поддержание в актуальном состоянии резервных копий защищаемой информации и активов.

18. Управление уязвимостями

18.1. В соответствии с принципами обеспечения информационной безопасности, инженер определяет и внедряет процесс управления уязвимостями информационных активов. Процесс управления уязвимостями представляет собой комплексный, непрерывный и циклический процесс выявления, оценки и устранения слабых мест в информационных активах Техникума.

Для эффективного управления уязвимостями требуется комплексная информация: сведения о производителях и версиях программного обеспечения, данные о текущем развёртывании ПО (с указанием конкретных систем, где оно установлено), а также информация о доступе, конфигурации и компонентах информационных систем Техникума.

18.2. Целью процесса управления уязвимостями является минимизация вероятности эксплуатации уязвимостей, снижение потенциального ущерба от инцидентов, обеспечение непрерывной и проактивной защиты, предотвращение появления новых уязвимостей.

Процесс управления уязвимостями состоит из следующих этапов:

идентификация уязвимостей;

анализ уязвимостей;

устранение уязвимости;

мониторинг и повторное сканирование.

Информация о технических уязвимостях, актуальных для используемых информационных систем, своевременно получается и обрабатывается.

Инженером оценивается подверженность Техникума техническим уязвимостям и для принятия соответствующих мер в отношении связанных с этим рисков информационной безопасности.

18.3. Для создания эффективного процесса управления техническими уязвимостями инженер придерживается следующих принципов:

определяются роли и обязанности, связанные с управлением техническими уязвимостями, включая их мониторинг, оценку риска, исправление ошибок, отслеживание активов и принимаются необходимые меры по координации данного процесса;

идентифицируются информационные ресурсы, которые используются для выявления соответствующих технических уязвимостей;

определяются сроки реагирования на уведомления о потенциально значимых

технических уязвимостях;

при выявлении потенциальной технической уязвимости определяются связанные с ней риски и предпринимаются соответствующие действия к ее устранению. Такие действия включают применение пакетов исправлений к уязвимым системам либо набор компенсирующих мер обеспечения информационной безопасности;

определяются и регламентируются процедуры реагирования на инциденты информационной безопасности;

в случае наличия официального исправления оцениваются риски, связанные с его установкой (риски, связанные с уязвимостью, сравниваются с рисками, которые могут возникнуть вследствие установки исправления);

пакеты исправлений проверяются и оцениваются до их установки в продуктивные среды.

18.4. В случае невозможности установки исправлений или при отсутствии исправлений рассматриваются иные меры устранения или митигации актуальных угроз и рисков, такие как (но не ограничиваясь перечисленным):

отключение сервисов и возможностей, связанных с уязвимостью;

настройка или добавление мер контроля доступа, в том числе межсетевых экранов на границах сети;

усиление мониторинга для выявления реальных атак;

повышение осведомленности об уязвимостях;

журналирование предпринятых действий;

учет систем с высоким уровнем риска.

19. Применение криптографических средств защиты информации

19.1. В целях защиты информации инженер применяет средства криптографической защиты информации (далее — СКЗИ) в соответствии с действующим законодательством Российской Федерации. При работе с СКЗИ учитывается следующее:

подход к управлению ИТ-активами с применением СКЗИ, на которых должна быть основана защита конфиденциальной информации и иной охраняемой законом тайны;

определенный, на основе оценки риска, уровень защиты с учетом типа, стойкости и качества требуемого алгоритма шифрования;

использование шифрования для защиты информации, передаваемой с помощью носителей, а также иных каналов связи;

меры к управлению ключами, в том числе методы по защите криптографических ключей и восстановлению зашифрованной информации

в случае утери, компрометации или повреждения ключей;

роли и обязанности ответственных за направление СКЗИ;

требования законодательства и регуляторов, стандартов, регулирующих деятельность, связанную с использованием СКЗИ;

влияние использования зашифрованной информации на меры обеспечения информационной безопасности, которые базируются на проверке содержимого (например, обнаружение вредоносного ПО).

19.2. Регламентация процессов, связанных с криптографической защитой в Техникуме, учитывает следующие ключевые меры:

обеспечение конфиденциальности при использовании шифрования для защиты информации ограниченного доступа как при хранении, так и при передаче;

обеспечение целостности и аутентичности при использовании электронных подписей или кодов аутентификации сообщений для проверки подлинности или целостности информации ограниченного доступа при ее передаче и хранении;

обеспечение неотказуемости при использовании криптографических методов с целью подтверждения наличия (или отсутствия) события или действия;

использование криптографических методов для аутентификации и авторизации пользователей и других системных объектов.

20. Обеспечение защиты сред передачи данных

20.1. При осуществлении деятельности по защите сред передачи данных инженер руководствуется следующими принципами:

организационное обеспечение защиты;

применение аппаратных средств защиты;

применение программных средств защиты;

применение криптографических средств защиты;

применение средств физической защиты.

20.2. В целях реализации мер по защите сред передачи данных могут использоваться следующие ключевые способы обеспечения защиты (но не ограничиваясь перечисленным):

процедуры защиты регламентированы и оформлены;

ведение постоянного мониторинга и регистрации событий с целью обнаружения действий, которые могут повлиять на информационную безопасность; прохождение пользователями процедуры аутентификации и авторизации для доступа к системам и сетям Техникума;

наличие ограничений на подключение систем к корпоративным сетям;

идентификация механизмов обеспечения безопасности, уровней обслуживания и требований к управлению для всех сетевых сервисов;

разделение в сети групп информационных сервисов, пользователей и информационных систем.

21. Защита персональных данных

21.1. Конфиденциальность и защита персональных данных обеспечиваются в строгом соответствии с требованиями законодательства Российской Федерации и требованиями регуляторов.

21.2. За обработку и обеспечение безопасности персональных данных назначаются ответственные сотрудники исходя из принципа минимально необходимого круга лиц, принимаются технические и организационные меры для защиты персональных данных.

21.3. Порядок работы с персональными данными регулируется приказом директора Техникума.

22. Защита информации при взаимодействии с третьими лицами

22.1. При осуществлении взаимодействия с третьими лицами инженер предъявляет требования, направленные на снижение рисков, связанных с доступом третьих лиц к ИТ-активам Техникума. Условия и порядок такого взаимодействия согласовываются и оформляются документально.

22.2. В Техникуме определены соответствующие меры обеспечения информационной безопасности в отношении доступа третьих лиц к информации Техникума, учитывающие процессы и процедуры, которые должны выполняться сотрудниками Техникума, а также те процессы и процедуры, которые требуется выполнять со стороны третьих лиц, учитывая следующие требования:

определение и документирование типов поставщиков (например, ИТ-услуги, поставщики компонентов ИТ-инфраструктуры, пользователи сервисов, поставщики информации и т.д.), которым будет предоставлен доступ к активам и/или информации Техникума;

стандартизация процесса и жизненного цикла процессов для управления отношениями с поставщиками;

определение типов доступа к информации, которые будут предоставлены третьим лицам, а также мониторинг и контроль доступа;

применение необходимых требований по информационной безопасности для каждой категории информации и типа доступа, учитывающих потребности и требования Политики, а также учет рисков, которые будут служить основой для соглашений с конкретным контрагентом;

правильность и полнота мер обеспечения информационной безопасности для

обеспечения целостности информации или обработки информации, проводимой любой из сторон;

применение обязательств при взаимодействии с третьими лицами с целью защиты информации Техникума;

выполнение обязательств при взаимодействии с третьими лицами;

условия, при которых требования и меры обеспечения информационной безопасности будут учитываться при заключении договорных обязательств обеими сторонами;

определение порядка обработки, хранения информации и ее передачи.

23. Оценка результативности мероприятий по обеспечению защиты информации

23.1. Инженер оценивает деятельность по обеспечению защиты информации, а также результативность такой деятельности и хранит документированную информацию в качестве свидетельства результатов мониторинга и оценки защищенности информации. При этом инженер определяет:

объекты мониторинга и оценки защищенности, включая процессы и меры обеспечения информационной безопасности;

методы проведения мониторинга, оценки защищенности, анализа и оценивания, обеспечивающие уверенность в достоверности результатов;

время проведения мониторинга и оценки защищенности;

сотрудников, осуществляющих мониторинг и оценку защищенности;

периодичность анализа результатов мониторинга и оценки защищенности;

сотрудников, осуществляющих реализацию мероприятий, принятых по результатам мониторинга и оценки защищенности.

23.2. Инженер проводит внутренние аудиты с целью определения:

соответствия мер по обеспечению информационной безопасности требованиям законодательства Российской Федерации и регуляторов и собственным требованиям к такой деятельности;

эффективной реализации и поддержки деятельности по обеспечению информационной безопасности.

23.3. При проведении аудитов инженер:

планирует, разрабатывает, реализует и поддерживает программу(ы) аудита, включая определение периодичности и методов проведения аудита, ответственных лиц, требования к планированию и предоставлению отчетности аудита, учитывая значимость проверяемых процессов и результаты предыдущих аудитов;

определяет критерии и область проведения каждого аудита;

осуществляет подбор аудиторов и сопровождает проведение аудитов для обеспечения уверенности в объективности и беспристрастности процесса аудита.

23.4. Инженер проводит проверку деятельности по обеспечению информационной безопасности через запланированные интервалы времени в целях обеспечения ее приемлемости, актуальности и результативности. По результатам проверок инженер принимает решения, направленные на совершенствование деятельности по обеспечению информационной безопасности Техникума.

24. Модернизация процессов обеспечения информационной безопасности

24.1. При выявлении несоответствий процессов обеспечения информационной безопасности требованиям действующего законодательства Российской Федерации и/или регуляторов в данной области, инженер:

реагирует на несоответствия и предпринимает необходимые действия, направленные на устранение несоответствий или их последствий;

оценивает необходимость корректирующих действий по устранению причин несоответствий, с целью минимизации риска их повторения или появления при других потенциальных сценариях, посредством:

анализа несоответствия;

определения причин появления несоответствия;

определения наличия подобных несоответствий или потенциальных возможностей их возникновения.

организует мероприятия по корректировке процессов обеспечения информационной безопасности;

анализирует результативность предпринятых корректирующих действий;

вносит, при необходимости, изменения в процессы обеспечения информационной безопасности.

При необходимости реализации корректирующих действий применяются меры, адекватные последствиям выявленных несоответствий.

24.2. Инженер хранит документированную информацию в качестве свидетельства о характере несоответствий и любых последующих предпринимаемых действиях, а также результатах всех корректирующих действий. Инженер постоянно улучшает приемлемость, адекватность и результативность деятельности по обеспечению информационной безопасности.

25. Проведение контрольных мероприятий по защите информации

25.1. Контроль информационной безопасности является одним из основных средств оценки организационных и программнотехнических мер защиты информации, реализуемых в Техникуме и взаимодействующих с ним организациях.

25.2. Контроль осуществляется в следующей форме:

внутренний контроль - проводится инженером в отношении собственных процессов и систем;

25.3. На основании результатов контрольных мероприятий принимаются решения:

по повышению уровня обеспечения информационной безопасности в Техникуме и при взаимодействии с иными организациями;

по модернизации системы информационной безопасности;

по устранению недостатков и уязвимостей, выявленных в ходе контроля.

26. Ответственность за нарушения в области защиты информации

26.1. Ответственность за ненадлежащую организацию и неосуществление контроля исполнения требований настоящей Политики возложена на инженера.

26.2. Ответственность за ненадлежащую организацию деятельности в области информационной безопасности несет инженер.

26.3. Нарушение требований информационной безопасности может являться предметом служебного расследования и сопровождаться применением мер в соответствии с законодательством Российской Федерации, а также локальными нормативными актами Техникума.

26.4. Сотрудники третьих лиц, использующие ИТ-активы Техникума, а также предоставленную информацию, несут ответственность в соответствии с договорными отношениями, а также законодательством Российской Федерации.

27. Заключительные положения

27.1. В случае изменения действующего законодательства и иных нормативных актов Политика и изменения к ней применяются в части, не противоречащей вновь принятым документам.

27.2. Разработка настоящей Политики и внесение в нее изменений осуществляется инженером.

27.3. Внесение изменений в настоящую Политику осуществляется на периодической и/или внеплановой основе. Периодическое внесение изменений осуществляется не реже одного раза в 24 месяца. Внеплановое внесение изменений может производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер

обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий, а также в случае изменения действующего законодательства Российской Федерации в области защиты информации.