Министерство образования Саратовской области
Государственное автономное профессиональное образовательное учреждение
Саратовской области «Балаковский политехнический техникум»

СОГЛАСОВАНО
Совет ГАПОУ СО «БПТ»
(протокол от 18.03.2026 г. № 4)

УТВЕРЖДЕНО
приказом директора ГАПОУ СО «БПТ»
от «18» марта 2026 г. № 80

ПЭП

Подписан: Никулина Элла Александровна
DN: C=RU, S=Саратовская область, L=Балаково, T=Директор, O="ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САРАТОВСКОЙ ОБЛАСТИ "" БАЛАКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ ТЕХНИКУМ""", СНИЛС=05641551451, ИНН=644106310058, E=balakovopolytech@mail.ru, G=Элла Александровна, SN=Никулина, CN=Никулина Элла Александровна
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: г.Балаково, Саратовской области
Дата: 2026-03-25 11:39:12

ПОЛИТИКА
информационной безопасности

СОГЛАСОВАНО
Юрисконсульт ГАПОУ СО «БПТ»
_____ Троценко О.А.
«18» марта 2026г.

Вступает в законную силу с 18 марта 2026 г. и действует до отмены или принятия новой политики

г. Балаково
2026г.

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Объекты информатизации являются неотъемлемой частью организации основной деятельности ГАПОУ СО «БПТ» (далее – Учреждение). Все объекты информатизации Учреждения подлежат защите в соответствии с их ценностью, и способом, направленным на минимизацию рисков несанкционированного доступа и противоправных действий в отношении их. Учреждение осуществляет постоянное контроль и совершенствование систем информационной безопасности, обеспечивая соответствие законодательству и регуляторным нормам Российской Федерации.

1.2 Политика информационной безопасности ГАПОУ СО «БПТ» (далее – Политика) формулирует и отображает позицию Учреждения в области информационной безопасности, описывает основные принципы построения и эксплуатации, определяющие стратегические цели и задачи обеспечения информационной безопасности Учреждения.

1.3 Политика отражает ключевой вектор развития системы информационной безопасности Учреждения и основные принципы, непосредственно использующиеся для построения и управления информационной безопасностью. Политика предусматривает общие организационно-технические меры, направленные на повышение информационной защищенности и принципы построения информационной безопасности Учреждения.

1.4 Настоящая Политика описывает общую концепцию информационной безопасности Учреждения и не предполагает построения безусловной системы защиты информации, в связи с чем Политикой предполагается и допускается возникновение случаев, несущих потенциальный вред информационной защищенности Учреждения.

1.5 Иные внутренние нормативные документы, регламентирующие общие или частные мероприятия по обеспечению информационной безопасности должны разрабатываться и применяться с учетом положений и требований настоящей Политики. Иные внутренние документы не могут противоречить определениям и положениям, которые определенны данной Политикой.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1 Требования настоящей Политики распространяются на все процессы Учреждения, связанные с применением объектов информатизации, его информационную инфраструктуру и являются обязательными для выполнения всеми работниками Учреждения.

2.2 Требования Политики также распространяются на процессы взаимодействия с внешними, по отношению к Учреждению лицами, услуги и предложения которых связаны с предоставлением доступа, использованием, обработкой посредством использования объектов информатизации, информационных систем и обрабатываемой или используемой в Учреждении информации.

2.3 Требования настоящей Политики распространяются на все структурные подразделения Учреждения. Область применения настоящей Политики покрывает весь жизненный цикл (создание, тестирование, вывод в эксплуатацию, эксплуатация и вывод из эксплуатации) объектов информатизации Учреждения.

2.4 Настоящая Политика также распространяется на все деловые, договорные, финансовые, информационные, публичные или иные взаимодействия Учреждения с третьими лицами или организациями, которые прямо или косвенно могут влиять на процессы, связанные с рисками информационной безопасности.

3. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

3.1. В настоящей Политике применены следующие термины с соответствующими определениями:

Аудит информационной безопасности (далее – Аудит ИБ) – комплекс организационно-технических мер и мероприятий, направленный на получение объективных данных состояния защиты информации объектов информатизации.

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

Информация – совокупность данных (в электронной, письменной или устной форме), которая обрабатывается в Учреждении, а также используется для поддержки процессов Учреждения.

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

Достоверность – свойства соответствия предусмотренному поведению и результатам.

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

Информационная безопасность (далее – ИБ) – сохранение конфиденциальности, целостности и доступности информации.

Информационная система (далее – ИС) – комплекс программного обеспечения, услуг или других компонентов для обработки информации.

Инцидент ИБ – 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.

Конфиденциальность – недоступность для неавторизованных лиц, объектов или процессов.

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

Оценка риска – процесс, охватывающий идентификацию риска, анализа риска и оценивание риска.

Подлинность – свойство, определяющее, что фактический субъект или объект совпадает с заявленным.

Применение риска – обоснованное решение о принятии риска.

Пользователь – работник Учреждения, имеющий в установленном порядке доступ к информационным ресурсам Учреждения в объеме, необходимом для надлежащего выполнения должностных обязанностей.

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

Риск ИБ – событие информационной безопасности, наступившее в результате реализации одного или нескольких факторов операционного риска, и повлекшее или способное повлечь за собой прямые потери и/или косвенные потери.

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

3.2. В настоящей Политике приняты следующие сокращения:

ИБ	–	информационная безопасность;
ИС	–	информационная система;
ИСПДн	–	информационная система персональных данных;
ПД	–	персональные данные;
ПЭВМ	–	персональная электронно-вычислительная машина;
НСД	–	несанкционированный доступ;
СЗИ	–	система защиты информации;
СКЗИ	–	система криптографической защиты информации;
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю.

4. НОРМАТИВНЫЕ ДОКУМЕНТЫ

4.1. Настоящая Политика разработана в соответствии с требованиями действующего законодательства Российской Федерации, требованиями регуляторов в области информационной безопасности, а также с учетом требований иных нормативных и организационно-распорядительных документов Учреждения в области информационной безопасности:

– Конституция Российской Федерации;

– Национальный стандарт Российской Федерации информационные технологии методы и средства обеспечения безопасности свод норм и правил применения мер обеспечения информационной безопасности ГОСТ Р ИСО/МЭК 27002-2021;

– Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федеральный закон от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи»;

– Указ Президента Российской Федерации от 17.03.2008 г. № 358 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

– Постановление Правительства РФ от 15 сентября 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119;

– Методический документ. Методика оценки угроз безопасности информации, утвержденный ФСТЭК России от 05.02.2021.

5. ЦЕЛИ И ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Цель настоящей Политики – это минимизация рисков ИБ, которым подвержена информационная инфраструктура Учреждения.

Поставленная цель достигается посредством обеспечения следующих задач:

– поддержка процессов Учреждения посредством обеспечения конфиденциальности, достоверности, доступности и подлинности, обрабатываемой в Учреждении информации;

– обеспечение снижения риска нарушения конфиденциальности, достоверности, доступности и подлинности информации путем организации правил использования информации и информационных систем;

– обеспечение информацией об общих правилах ИБ среди работников Учреждения и сторонних лиц, которая определяет обязанности, ответственность и роль каждого работника;

– обеспечение соблюдения требованиям законодательства Российской Федерации, Регуляторов и иных внутренних нормативных актов;

– управление ИБ, в частности определение ролей и обязанностей в области ИБ всех работников Учреждения;

– проведение оценки рисков ИБ;

– обеспечение информационной безопасности объектов информатизации Учреждения;

– мониторинг событий ИБ и управление инцидентами ИБ;

– регулярный аудит состояния ИБ;

– постоянное совершенствование систем обеспечения ИБ Учреждения.

6. ОСНОВНЫЕ ТРЕБОВАНИЯ, ПРАВИЛА, ПРИНЦИПЫ, РОЛИ И ОТВЕТСТВЕННОСТЬ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Настоящая Политика предусматривает следующие основополагающие принципы и правила обеспечения ИБ объектов информатизации:

– в целях снижения потенциальных рисков возникновения инцидентов ИБ Учреждение систематически проводит инструктажи и обучение работников нормам ИБ;

– работники Учреждения и сторонние лица, имеющие доступ к информации или информационной инфраструктуре Учреждения должны обеспечивать надлежащий уровень ИБ при осуществлении своих должностных обязанностей и несут персональную ответственность за его нарушение в рамках действующего законодательства Российской Федерации и внутренними нормативными документами Учреждения;

6.2. Политика предусматривает применение Учреждением следующих мер по обеспечению ИБ:

– определяет объекты информатизации, обеспечивающие планомерность и беспрерывность процессов деятельности Учреждения и требующих надлежащей защиты;

– определяет инструкции, регламенты и процедуры классификации и оперативного реагирования на инциденты ИБ;

– определены правила доступа и распределение доступа к информационным ресурсам, ИС, АРМ и обрабатываемой в Учреждении информации;

– обеспечивает систему защиты обрабатываемой информации на объектах информатизации;

– обеспечивает криптографическую защиту информации;

– обеспечивает защиту локальной сети Учреждения;

– обеспечивает порядок доступа в помещения Учреждения, в которых обрабатывается информация;

– разрабатывает и поддерживает актуальность требований по защите ИБ, определенных во внутренней нормативной документации в области информационной безопасности Учреждения.

6.3. Роли и ответственность:

– обеспечение ИБ достигается путем соблюдения требований к ИБ всем структурными подразделениями и работниками Учреждения, а также сторонними лицами, предоставляющих услуги Учреждению во время исполнения которых обеспечивается доступ к информационным ресурсам и информации Учреждения;

– при выполнении своих должностных обязанностей работники Учреждения отвечают за выполнение требований настоящей Политики, законодательных актов Российской Федерации, норм Регуляторов, норм внутренних документов и несут ответственность за невыполнение или нарушение требований согласно действующему законодательству Российской Федерации и внутренним документам Учреждения;

– в Учреждении определены работники, обеспечивающие контроль за соблюдением организационно-технических мер, направленных на поддержание надлежащего уровня ИБ.

7. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Общее руководство обеспечением ИБ осуществляет директор Учреждения.

7.1. Принципы управления информационной безопасностью

7.1.1. Обеспечение информационной безопасности объектов информатизации Учреждения включает в себя ряд организационно-управленческих задач:

– обеспечение наличия и регулярного аудита внутренних руководящих документов в области информационной безопасности;

– обеспечение защищаемых объектов информатизации надлежащим уровнем защиты информации с применением программных и программно-аппаратных средств защиты информации;

– обеспечение доступа к обработке информации на объектах информатизации работников, имеющих на это соответствующие полномочии;

– установление полномочий работников в отношении защищаемых объектов информатизации;

– ограничение и контроль доступа лиц, не имеющих полномочий на обработку информации на защищаемых объектах информатизации;

– ограничение и контроль доступа лиц в помещения, где ведется обработка защищаемой информации;

– регулярный контроль выполнения работниками требований в области информационной безопасности.

7.1.2. Перечисленные задачи применимы для всех защищаемых объектов информатизации в которых осуществляется обработка информации и решается с учетом

индивидуальных особенностей обработки и передачи информации в конкретных ИС и вычислительных сетях.

7.1.3. Процесс обеспечения ИБ на защищаемых объектах информатизации и информационно-вычислительных сетях, эксплуатируемых в Учреждении непосредственно осуществляют:

– директор Учреждения;

– руководитель структурного подразделения по защите информации;

– работники, ответственные за информационную безопасность.

7.2. Директор Учреждения

7.2.1. Директор Учреждения обеспечивает утверждение внутренней нормативно-правовой документации в области информационной безопасности и общее обеспечение ИБ.

7.3. Руководитель структурного подразделения по защите информации

7.3.1. Руководитель структурного подразделения обеспечивает контроль за соблюдением и исполнением требований законодательных актов Российской Федерации, регуляторных норм и норм внутренних нормативно-правовых актов в области информационной безопасности, а также обеспечивает подготовку и поддержание в актуальном состоянии распорядительной и иной внутренней нормативно-правовой документации.

7.3.2. Руководитель структурного подразделения находится в непосредственном подчинении директора Учреждения, а также обеспечивает контроль за работой работников, ответственных за информационную безопасность.

7.3.3. Руководитель структурного подразделения контролирует наличие у 30% работников структурного подразделения образования в области ИБ и/или обеспечивает своевременное переподготовку работников в области ИБ.

7.4. Работники, ответственные за информационную безопасность

7.4.1. Работники, ответственные за информационную безопасность (далее – Ответственные за ИБ) назначаются приказом директора Учреждения и находятся в непосредственном подчинении руководителя структурного подразделения по защите информации.

7.4.2. Ответственные за ИБ обеспечивают ряд следующих задач:

– разработка внутренних нормативно-правовых документов в области информационной безопасности Учреждения;

– планирование работ по ИБ;

– обеспечение контроля за соблюдением требований в области информационной безопасности работниками Учреждения;

– обеспечение ИБ при эксплуатации объектов информатизации и сетевой инфраструктуры;

– обеспечение программных и программно-аппаратных средств защиты информации на объектах информатизации и/или сетевой инфраструктуры;

– обеспечение целостности, безотказной работы и восстановление штатной (ожидаемо нормальной) работы ИС и сетевой инфраструктуры;

– поддержание требуемого уровня защиты информации в программных и программно-аппаратных средствах защиты информации на протяжении всего жизненного цикла объекта информатизации, путем контроля функционирования и настройки механизмов безопасности;

– обеспечение доступа работников к информационным ресурсам объектов информатизации;

– проведение обучения, инструктажей и регулярного информирования работников Учреждения о требованиях законодательных, регуляторных и внутренних норм по обеспечению ИБ.

8. ОБЪЕКТЫ ЗАЩИТЫ

Объектами защиты информации в Учреждении являются:

– информационные ресурсы, содержащие конфиденциальную информацию, информацию ограниченного доступа, в том числе персональные данные физических лиц, коммерческую тайну, а также иную информацию, необходимую для бесперебойной работы Учреждения;

– информационная инфраструктура Учреждения, включая информационные системы (в том числе ИСПДн), системы информационного взаимодействия, технические и программные средства обработки и передачи информации, каналы информационного обмена и телекоммуникаций, средства защиты информации, объекты и помещения, в которых размещена информационная инфраструктура.

9. МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.1. Модель угроз и модель нарушителя безопасности информации является определяющим документом, оценивающим потенциальные риски ИБ и является необходимым документом при сопровождении информационной инфраструктуры Учреждения в течение всего жизненного цикла.

9.2. Сведения об объектах информатизации, уровнях защищенности, субъектах доступа, потенциальные негативные последствия реализации угроз ИБ, возможные объекты воздействия, источники угроз ИБ, оценка способов реализации угроз ИБ, а также актуальные угрозы безопасности информации определяются документом «Модель угроз и модель нарушителя безопасности информации в информационных системах персональных данных ГАПОУ СО «БПТ».

10. ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.1. Общие требования по обеспечению информационной безопасности

Требования ИБ формулируются для следующих областей:

– назначение и распределение ролей доступа работников к ИС;

– стадий жизненного цикла ИС;

– защиты от НСД, управления доступом и регистрацией в ИС;

– антивирусной защиты;

– использования Интернет-ресурсов;

– использования средств криптографической защиты информации;

– защиты информационных технологических процессов.

10.2. Требования по обеспечению информационной безопасности при назначении и распределении ролей доступа работников к ИС Учреждения

10.2.1. Уровень и роли доступа работников в ИС Учреждения назначаются и определяются приказом директора Учреждения в соответствии с выполняемыми работниками должностными обязанностями.

Каждая утвержденная за работником роль соответствует своей персонифицированной учетной записи для доступа к элементам и компонентам информационной инфраструктуры.

10.2.2. Контроль для выполнением работниками требований ИБ осуществляется ответственными за информационную безопасность.

10.3. Требования по обеспечению информационной безопасности при работе в ИСПДн

10.3.1. Назначение и доступ работников к ИСПДн осуществляется на основании приказа директора Учреждения.

10.3.2. Для каждой ИСПДн должен быть разработан и утверждён технический паспорт (формуляр) ИСПДн в соответствии с регуляторными нормами, определен требуемый уровень защищенности информации, определены категории, количество и принадлежность обрабатываемых ПД, а также выделены актуальные угрозы ИБ.

10.3.3. Каждая ИСПДн должна комплектоваться средством защиты информации от НСД и средством антивирусной защиты информации. СЗИ от НСД и средство антивирусной защиты информации могут быть объединены в один программно-аппаратный комплекс для каждой ПЭВМ, входящей в состав ИСПДн, в случае наличия соответствующих

сертификатов соответствия требованиям к СЗИ. Средства защиты информации, их компоненты и модули должны быть постоянно включены и регулярно обновляться.

10.3.4. Полный состав программно-аппаратного, технического обеспечения и сетевой инфраструктуры должен быть указан в техническом паспорте (формуляре) ИСПДн.

10.4. Требования по обеспечению программно-аппаратной защиты информации

10.4.1. Все ПЭВМ, находящиеся в стадии фактической эксплуатации в Учреждении должны включать в состав программного обеспечения сертифицированное средство защиты информации (средство антивирусной защиты).

10.4.2. Установка, обновление, мониторинг и контроль за состоянием средств защиты информации осуществляется работниками, ответственными за информационную безопасность в соответствии с локальными нормативно-правовым актами Учреждения в области ИБ.

10.4.3. На всех ПЭВМ, находящихся в стадии фактической эксплуатации в Учреждении настраивается автоматическая проверка наличия обновлений компонентов и модулей средств защиты информации.

10.4.4. Работники, имеющие доступ к ПЭВМ Учреждения должны соблюдать требования и инструкции по антивирусной защите информации и несут ответственность за невыполнение таких требований.

10.5. Требования по обеспечению информационной безопасности при использовании ресурсов информационно-телекоммуникационной сети «Интернет»:

10.5.1. Предоставление доступа Учреждению к сетям общего доступа и международного обмена, в том числе к информационно-телекоммуникационной сети «Интернет» обеспечивается Поставщиком услуг на основании государственного контракта на оказание государственным и муниципальным образовательным организациям услуг по предоставлению с использованием единой сети передачи данных доступа к информационно-телекоммуникационной сети «Интернет», а также на основании иных договоров на представление услуг по предоставлению доступа к информационно-телекоммуникационной сети «Интернет».

10.5.2. Взаимодействие и использование ресурсов информационно-телекоммуникационной сети «Интернет» необходимо для получения, обработки и распространения информации, связанной с деятельностью Учреждения. Работники, имеющие доступ к информационно-телекоммуникационной сети «Интернет» должны выполнять такое взаимодействие только в целях выполнения своих должностных и функциональных обязанностей.

10.5.3. Порядок и правила взаимодействия работников Учреждения с ресурсами информационно-телекоммуникационной сети «Интернет» регламентируются документами «Правила безопасной работы сотрудников ГАПОУ СО «БПТ» при осуществлении эксплуатации информационных систем и интернет-сервисов с использованием информационно-телекоммуникационной сети «Интернет», «Порядок предоставления пользователям доступа из информационных систем в телекоммуникационную сеть «Интернет» и контроля ее использования», а также иными внутренними нормативными актами, определяющими порядок работы и взаимодействия работников с ресурсами, доступ к которыми осуществляется посредством информационно-телекоммуникационной сети «Интернет».

10.6. Требования по обеспечению информационной безопасности при работе со средствами криптографической защиты информации

10.6.1. Помещения, в которых располагаются компоненты СКЗИ обязательно оборудуются дверьми и запирающими механизмами. Помещение должно быть оборудовано системой охранной сигнализации, снятие и постановка на которую должно документально фиксироваться при каждом таком событии.

10.6.2. Доступ работников Учреждения, осуществляющих работу с СКЗИ, в помещения, в которых располагаются компоненты СКЗИ определяется на основании

соответствующего приказа директора Учреждения. Присутствие иных лиц, не осуществляющих работу с СКЗИ, в помещения, где располагаются компоненты СКЗИ возможно только под постоянным контролем ответственных работников на протяжении всего периода нахождения лица в помещении, где располагаются компоненты СКЗИ.

10.6.3. Доступ работников Учреждения к работе с компонентами СКЗИ определяется соответствующим приказом директора Учреждения.

10.6.4. Каждый компонент и/или экземпляр СКЗИ, эксплуатируемый в Учреждении подлежит документальному учету в целях минимизации возможностей копирования компонентов и/или экземпляров СКЗИ на иные ПЭВМ.

10.6.5. Порядок работы работников Учреждения с СКЗИ регламентируется документом «Порядок работы со средствами криптографической защиты информации» и иными внутренними нормативными актами, выполнение требований которых обязательно для всех работников Учреждения, осуществляющих работу с СКЗИ.

11. АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

11.1. Порядок и периодичность проведения аудита ИБ Учреждения, а также отдельных его структурных подразделений, определяется подразделением, ответственным за информационную безопасность на основании потребности в такой деятельности.

11.2. Внешняя оценка безопасности информации при ее обработке в ИСПДн осуществляются внешними, по отношению к Учреждению независимыми организациями, имеющими лицензию на проведение работ и услуг в области оценки и контроля защищенности информации.

11.2.1. Организации, предоставляющие работы и услуги Учреждению по оценке соответствия требованиям по защите информации должны иметь действующую лицензию на проведение работ и услуг по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации.

11.2.2. Внешняя оценка безопасности информации инициируется на основании приказа директора Учреждения.

11.3. Внутренний аудит ИБ на соответствие требованиям по защите информации проводится Комиссией по защите персональных данных или рабочей группой

12. ПОРЯДОК ПЕРЕСМОТРА ПОЛИТИКИ

12.1. Политика подлежит пересмотру в случае изменения в целом или частично требований законодательных актов Российской Федерации и/или регуляторных норм в области информационной безопасности, а также в случае изменения целей, задач, основных принципов, требований ИБ, функций структурных подразделений и ответственных за ИБ в Учреждении.

12.2. Пересмотр Политики должен включать:

– оценку эффективности действия Политики, в соответствии с произошедшими/не произошедшими инцидентами ИБ;

– соответствие Политики требованиям законодательных актов Российской Федерации и/или регуляторных норм в области ИБ;

– соответствие Политики действительному (текущему на момент пересмотра Политики) состоянию развития информационных технологий в области ИБ и организационных способов обеспечения ИБ.

12.3 Подготовку предложений по внесению изменений в настоящую Политику организуют работники, ответственные за ИБ.

13. ОТВЕТСТВЕННОСТЬ РУКОВОДСТВА И РАБОТНИКОВ

13.1. Администрация Учреждения отвечает за состояние ИБ в Учреждении и обеспечивает регулярный контроль соблюдения требований настоящей Политики, актуализацию и выделение организационных, технических и иных ресурсов необходимых для обеспечения ИБ.

13.2. Работники, ответственные за ИБ несут ответственность за обеспечение ИБ объектов защиты информационной инфраструктуры Учреждения.

13.3. Руководители структурных подразделений несут ответственность за:

– соблюдение работниками структурного подразделения нормам ИБ, утвержденных в Учреждении;

– соответствие полномочий работников структурного подразделения по доступу к конфиденциальной информации, объектам информатизации и сетевой инфраструктуре Учреждения.

13.4. Работники Учреждения обязаны:

– соблюдать требования настоящей Политики и иных нормативных и организационно-распорядительных документов Учреждения в области ИБ;

– использовать информационную инфраструктуру Учреждения исключительно для выполнения своих должностных обязанностей;

– информировать работников, ответственных за информационную безопасность о выявленных и/или произошедших инцидентах ИБ.

13.5. Нарушение требований настоящей Политики и иных нормативных и организационно-распорядительных документов Учреждения в области ИБ, а также сокрытие фактов произошедших инцидентов ИБ работниками Учреждения запрещается.

13.6. Работники Учреждения, наущающие и/или не выполняющие требования настоящей Политики и/или требования иных организационно-распорядительных документов Учреждения в области ИБ, несут ответственность, установленную действующим законодательством Российской Федерации.