СОГЛАСОВАНО
Председатель профсоюзного комитета
МАОУДО «ДЮЦ «Импульс»
_____ / Сухорослова С.В.
Протокол «17» 08 2026 г. № 0166

УТВЕРЖДЕНО
Директор
МАОУДО «ДЮЦ «Импульс»
_____ / Хабибьянова Д.С.
приказ от 17 августа 2026 № 156

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика информационной безопасности (далее — Политика) муниципального автономного образовательного учреждения дополнительного образования «Детско-юношеский центр «Импульс» (далее — Учреждение) является основополагающим документом Учреждения в области обеспечения информационной безопасности и определяет цели, задачи, принципы и основные направления деятельности Учреждения в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн).

1.2. Политика определяет порядок работы пользователей и администраторов ИСПДн, сотрудников, ответственных за техническое обеспечение, а также администратора информационной безопасности, в части обеспечения безопасности ПДн при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ИСПДн, порядок проверки электронного журнала обращений к ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в помещения ИСПДн, порядок создания резервных копий ИСПДн, правила хранения и регистрации носителей информации а также порядок обезличивания ПДн.

1.3. Настоящая Политика является обязательной для исполнения всеми работниками Учреждения независимо от занимаемой должности и формы трудовых отношений, а также контрагентами и третьими лицами, получающими доступ к информационным активам Учреждения.

1.4. Положения Политики должны быть доведены до сведения всех работников Учреждения под подпись.

1.5. Политика вступает в силу с момента её утверждения директором Учреждения и действует до её отмены либо замены новой редакцией.

2. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

В настоящей Политике используются термины в значениях, установленных Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», ГОСТ Р 53114-2008, а также следующие термины и определения:

Информационная безопасность (ИБ) — состояние защищённости информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий, способных нанести неприемлемый ущерб субъектам информационных отношений.

Конфиденциальность — обязательное для соблюдения требование не допускать несанкционированного ознакомления с информацией лиц, не имеющих на это права.

Целостность — состояние информации, при котором отсутствует любое её изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Доступность — состояние информации, при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно.

Угроза безопасности информации (УБИ) — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, целостности или доступности информации.

Уязвимость — свойство информационной системы, обуславливающее возможность реализации угроз безопасности информации.

Инцидент информационной безопасности — одно или серия нежелательных либо непредвиденных событий информационной безопасности, которые со значительной степенью вероятности приводят к реализации угроз безопасности информации и создают риски для информационных активов Учреждения.

Мера защиты информации — комплекс организационных, технических, правовых и физических действий, направленных на противодействие угрозам безопасности информации.

Контролируемая зона (КЗ) — пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и транспортных средств.

Средство защиты информации (СЗИ) — техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные либо используемые для защиты информации.

Средство криптографической защиты информации (СКЗИ) — средство защиты информации, реализующее алгоритмы криптографического преобразования информации.

Информационная система (ИС) — совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств.

Информационная система персональных данных (ИСПДн) — информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Критическая информационная инфраструктура (КИИ) — объекты информатизации, функционирующие в сферах, определённых Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Персональные данные (ПДн) — любая информация, относящаяся прямо или косвенно к определённому или определяемому физическому лицу (субъекту персональных данных).

Оператор персональных данных — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки, состав обрабатываемых данных и действия, совершаемые с ними.

Сокращения, используемые в Политике:

АРМ — автоматизированное рабочее место;

ГИС — государственная информационная система;

ЗО КИИ — значимый объект критической информационной инфраструктуры;

ИАФ — идентификация и аутентификация;

ИБ — информационная безопасность;

ИС — информационная система;

ИСПДн — информационная система персональных данных;

КИИ — критическая информационная инфраструктура;

КЗ — контролируемая зона;

МФА — многофакторная аутентификация;

НПА — нормативный правовой акт;

НСД — несанкционированный доступ;

ОРД — организационно-распорядительная документация;

ПДн — персональные данные;

РКН — Роскомнадзор;

СЗИ — средство защиты информации;

СКЗИ — средство криптографической защиты информации;

УБИ — угроза безопасности информации;

УЗ — уровень защищённости;

ФСБ — Федеральная служба безопасности Российской Федерации;

ФСТЭК — Федеральная служба по техническому и экспортному контролю.

3. ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Основной целью Политики является создание и поддержание условий, обеспечивающих защиту информации от случайных или преднамеренных воздействий, которые могут привести к нарушению её конфиденциальности, целостности или доступности, а также соблюдение требований законодательства Российской Федерации в области защиты информации.

3.2. Для достижения указанной цели решаются следующие задачи:

- обеспечение конфиденциальности, целостности и доступности информации, обрабатываемой в информационных системах Учреждения;

- предотвращение несанкционированного доступа к защищаемой информации и её неконтролируемого распространения;

- выполнение требований действующего законодательства Российской Федерации, в том числе по защите персональных данных, государственной и служебной тайны;

- защита деловой репутации Учреждения и прав её клиентов, партнёров и работников;

- своевременное выявление, оценка и нейтрализация актуальных угроз безопасности информации;

- мониторинг событий информационной безопасности и обнаружение инцидентов на ранних стадиях;

- реагирование на инциденты информационной безопасности с минимизацией ущерба;

- обеспечение непрерывности деятельности Учреждения при реализации инцидентов ИБ и внештатных ситуациях;

- совершенствование подходов к обеспечению информационной безопасности на основе анализа текущего состояния и лучших отраслевых практик;

- поддержание уровня осведомлённости работников в области информационной безопасности.

4. ОБЛАСТЬ ПРИМЕНЕНИЯ И ОБЪЕКТЫ ЗАЩИТЫ

4.1. Настоящая Политика применяется ко всем видам информации, обрабатываемой в Учреждении, в том числе:

- информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (включая служебную, коммерческую, банковскую тайну);

- персональным данным работников, клиентов, контрагентов и иных субъектов;

- информации, составляющей врачебную, адвокатскую, нотариальную или иную профессиональную тайну (при применимости к деятельности Учреждения);

- сведениям об интеллектуальной собственности и ноу-хау Учреждения;

- общедоступной информации, целостность и доступность которой критичны для функционирования Учреждения.

4.2. Объектами защиты в рамках настоящей Политики являются:

4.2.1. Информационные активы:

- защищаемая информация в любом виде представления (электронные документы, базы данных, файлы, сообщения, бумажные носители, устные сообщения);

- информационные ресурсы и базы данных, эксплуатируемые Учреждением;

- документированная информация в составе организационно-распорядительной документации.

4.2.2. Технические средства и инфраструктура:

- автоматизированные рабочие места и серверное оборудование;

- системы и средства обработки, хранения и передачи информации;

- информационные системы, включая ИСПДн, ГИС, ЗО КИИ (при наличии);

- телекоммуникационное оборудование и каналы связи;

- средства защиты информации, в том числе СЗИ от НСД, межсетевые экраны, антивирусное программное обеспечение, системы обнаружения вторжений, средства криптографической защиты информации;

- носители информации, включая съёмные и отчуждаемые носители, резервные копии, архивы.

4.2.3. Программное обеспечение:

- системное и прикладное программное обеспечение;

- средства защиты информации;

- собственные разработки Учреждения.

4.2.4. Помещения и физическая среда:

- помещения, в которых размещаются технические средства обработки информации и средства защиты;

- помещения, в которых осуществляется хранение носителей информации;

- контролируемая зона Учреждения.

4.3. Политика распространяется на всех работников Учреждения, стажёров, практикантов, а также на сотрудников Учреждения, партнёров, контрагентов и иных третьих лиц, допущенных к обработке защищаемой информации на основании заключённых договоров.

5. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Обеспечение информационной безопасности в Учреждении базируется на следующих принципах:

Принцип законности — соответствие всех мер защиты требованиям действующего законодательства Российской Федерации и международных соглашений, участником которых является Российская Федерация.

Принцип комплексности — одновременное использование правовых, организационных, технических, физических и криптографических мер защиты информации, обеспечивающее взаимное дополнение и компенсацию ограничений отдельных мер.

Принцип непрерывности — постоянное поддержание необходимого уровня информационной безопасности на всех этапах жизненного цикла информационных систем и информации.

Принцип минимально необходимых привилегий (Least Privilege) — предоставление работникам минимально необходимых прав доступа к информационным ресурсам, исключительно в объёме, требуемом для исполнения должностных обязанностей.

Принцип разделения обязанностей (Separation of Duties) — распределение критичных функций между разными работниками для предотвращения несанкционированных действий одного лица.

Принцип эшелонированной защиты (Defense in Depth) — применение многоуровневой защиты, при которой преодоление одного уровня не приводит к компрометации системы в целом.

Принцип адекватности и соразмерности — соответствие применяемых мер защиты уровню актуальных угроз и стоимости защищаемых информационных активов.

Принцип риск-ориентированного подхода — принятие решений в области ИБ на основе оценки рисков с учётом вероятности и потенциального ущерба.

Принцип персональной ответственности — закрепление за каждым работником личной ответственности за соблюдение требований информационной безопасности в зоне его ответственности.

Принцип прозрачности и подотчётности — документирование действий с защищаемой информацией, ведение журналов событий безопасности, возможность последующего аудита.

Принцип непрерывного совершенствования — регулярный пересмотр и улучшение системы защиты информации на основе выявленных инцидентов, результатов аудитов и изменений в угрозах.

6. РОЛИ И ОТВЕТСТВЕННОСТЬ

6.1. Директор Учреждения:

- утверждает настоящую Политику и иные документы в области ИБ;
- определяет стратегию обеспечения информационной безопасности;
- назначает ответственных в Учреждении по защите информации;
- обеспечивает финансирование мероприятий по защите информации;
- принимает решения по результатам инцидентов ИБ и аудитов.

6.2. Ответственный за обеспечение информационной безопасности:

- организует разработку, внедрение и поддержание системы управления информационной безопасностью;
- обеспечивает разработку и актуализацию организационно-распорядительной документации в области ИБ;
- организует обучение и повышение осведомлённости работников;
- расследует инциденты информационной безопасности;
- готовит отчётность о состоянии ИБ для администрации Учреждения.

6.3. Администратор безопасности информационных систем:

- реализует технические меры защиты информации;
- управляет средствами защиты информации;
- обеспечивает контроль настроек безопасности ИС;
- ведёт учёт инцидентов и событий безопасности;
- участвует в реагировании на инциденты.

6.4. Администратор информационных систем (системный администратор):

- обеспечивает настройку и эксплуатацию ИС в соответствии с требованиями ИБ;
- управляет учётными записями пользователей;
- обеспечивает резервное копирование и восстановление данных;
- взаимодействует с администратором безопасности при реализации мер защиты.

6.5. Работники Учреждения:

- выполняют требования настоящей Политики и иных документов в области ИБ;
- обеспечивают сохранность выданных им технических средств, учётных данных и паролей;
- немедленно сообщают о выявленных инцидентах информационной безопасности;
- проходят обязательное обучение в области ИБ в установленные сроки.

7. КЛАССИФИКАЦИЯ ИНФОРМАЦИИ И ИНФОРМАЦИОННЫХ АКТИВОВ

7.1. Вся информация, обрабатываемая в Учреждения, подлежит классификации с целью определения адекватного уровня защиты.

7.2. Для целей настоящей Политики устанавливаются следующие категории информации по уровню ограничения доступа:

Общедоступная информация — сведения, свободно распространяемые и не требующие специальных мер защиты конфиденциальности, при этом подлежащие защите от несанкционированного изменения и уничтожения.

Информация для внутреннего пользования — сведения, доступ к которым ограничен работниками Учреждения, но не подпадающие под категории тайны, установленные законодательством.

Конфиденциальная информация — сведения, составляющие коммерческую, служебную или иную профессиональную тайну, защищаемые в соответствии с требованиями законодательства Российской Федерации.

Персональные данные — сведения, относящиеся к физическим лицам, защищаемые в соответствии с Федеральным законом № 152-ФЗ и подзаконными актами.

Информация с признаками государственной тайны — сведения, защищаемые в особом порядке в соответствии с Законом Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» (если применимо к деятельности Учреждения).

7.3. Для информационных систем, обрабатывающих защищаемую информацию, определяется класс защищённости или уровень защищённости в соответствии с: — приказом ФСТЭК России от 11.02.2013 № 17 — для государственных информационных систем (до перехода на приказ № 117); — приказом ФСТЭК России № 117 — для государственных информационных систем (вступил в силу с 01.03.2026); — приказом ФСТЭК России от 18.02.2013 № 21 и Постановлением Правительства РФ от 01.11.2012 № 1119 — для информационных систем персональных данных; — приказом ФСТЭК России от 25.12.2017 № 239 — для значимых объектов критической информационной инфраструктуры.

7.4. Классификация и категорирование информационных систем оформляется отдельными организационно-распорядительными документами и является основанием для выбора конкретного набора мер защиты.

8. УПРАВЛЕНИЕ ДОСТУПОМ

8.1. Управление доступом к информационным ресурсам Учреждения осуществляется на основании принципа минимально необходимых привилегий и ролевой модели.

8.2. В Учреждении применяется многоуровневая идентификация и аутентификация:

- однофакторная (по паролю) — для систем с невысоким уровнем защищённости;
- многофакторная (пароль + токен / смарт-карта / биометрия / одноразовый код) — для привилегированных учётных записей, для ИС с высоким классом защищённости, для удалённого доступа.

8.3. Предоставление, изменение и отзыв прав доступа осуществляются по письменным заявкам, согласованным с руководителем подразделения работника и ответственным за ИБ.

8.4. Учётные записи уволенных работников блокируются в день увольнения. Учётные записи работников, уходящих в длительный отпуск или командировку, блокируются по заявке их руководителя.

8.5. Не реже одного раза в шесть месяцев проводится ревизия прав доступа на соответствие должностным обязанностям. Результаты ревизии оформляются актом.

8.6. Привилегированные учётные записи (администраторы систем и средств защиты) выделяются в отдельный контур управления: персональная аутентификация, обязательная МФА, расширенное логирование, отдельная парольная политика с повышенными требованиями, запрет использования для выполнения ежедневных рабочих задач.

8.7. Удалённый доступ к информационным ресурсам Учреждения разрешается только через защищённые каналы с применением СКЗИ и МФА, с обязательной регистрацией всех подключений.

9. ЗАЩИТА ОТ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

9.1. Для защиты от угроз безопасности информации в Учреждения разрабатывается и поддерживается в актуальном состоянии Модель угроз безопасности информации, оформляемая отдельным документом в соответствии с «Методикой оценки угроз безопасности информации», утверждённой ФСТЭК России 05.02.2021.

9.2. Модель угроз разрабатывается с использованием Банка данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), содержащего описание угроз (УБИ) и уязвимостей.

9.3. На основе модели угроз определяется состав применимых мер защиты информации в соответствии с применимыми нормативными актами (приказы ФСТЭК России № 17, 21, 117, 239 — в зависимости от типа информационной системы). Базовый перечень мер защиты приведён в Приложении 2.

9.4. Применяются следующие группы мер защиты:

Организационные меры:

- разработка и поддержание в актуальном состоянии организационно-распорядительной документации;
- назначение ответственных лиц;
- инструктажи и обучение работников;
- контроль соблюдения требований ИБ.

Технические меры:

- идентификация и аутентификация (ИАФ);
- управление доступом к информационным ресурсам (УПД);
- защита машинных носителей информации (ЗНИ);
- регистрация событий безопасности (РСБ);
- антивирусная защита (АВЗ);
- обнаружение и предотвращение вторжений (СОВ);
- контроль (анализ) защищённости (АНЗ);
- обеспечение целостности информационной системы (ОЦЛ);
- обеспечение доступности информации (ОДТ);
- защита среды виртуализации (ЗСВ);
- защита технических средств (ЗТС);
- защита информационной системы, её средств, систем связи и передачи данных (ЗИС).

Криптографические меры: — применение сертифицированных СКЗИ для защиты информации, передаваемой по каналам связи и хранимой на носителях, в соответствии с требованиями ФСБ России; — учёт СКЗИ и ключевых документов в соответствии с приказом ФАПСИ от 13.06.2001 № 152.

Физические меры: — Учреждение контролируемой зоны; — применение технических средств охраны и систем контроля и управления доступом; — защита помещений, в которых размещаются ИС и средства защиты.

9.5. Применяемые СЗИ должны иметь действующие сертификаты соответствия ФСТЭК России или ФСБ России (для криптографических средств) в соответствии с

требованиями, установленными для классов и уровней защищённости обрабатываемой информации.

9.6. Эксплуатация средств защиты информации должна осуществляться в соответствии с эксплуатационной документацией и с учётом требований настоящей Политики.

10. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.1. В Учреждения реализуется процесс управления инцидентами информационной безопасности, включающий:

— обнаружение и регистрацию событий и инцидентов ИБ;

— классификацию и приоритизацию инцидентов;

— реагирование и локализацию;

— расследование и установление причин;

— устранение последствий и восстановление;

— пост-инцидентный анализ и внесение изменений в систему защиты.

10.2. Работники Учреждения обязаны немедленно сообщать об инцидентах информационной безопасности ответственному за ИБ посредством (каналов уведомления: e-mail, телефон горячей линии, тикет-система).

10.3. Для типовых инцидентов (компрометация пароля, заражение вредоносным ПО, утечка информации, отказ в обслуживании, несанкционированный доступ) разрабатываются планы реагирования.

10.4. Для значимых объектов КИИ инциденты, подлежащие уведомлению, направляются в Национальный координационный центр по компьютерным инцидентам (НКЦКИ) в сроки, установленные Федеральным законом № 187-ФЗ и подзаконными актами.

10.5. Для операторов персональных данных инциденты, связанные с неправомерной передачей или иным нарушением безопасности ПДн, уведомляются в Роскомнадзор в срок не позднее 24 часов с момента выявления (в соответствии с требованиями Федерального закона № 152-ФЗ в редакции 420-ФЗ от 30.11.2024).

10.6. Все инциденты регистрируются в журнале инцидентов информационной безопасности и подлежат анализу для совершенствования системы защиты.

11. ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА СРЕДЫ ФУНКЦИОНИРОВАНИЯ

11.1. Помещения, в которых размещаются серверное оборудование, средства защиты информации, рабочие места с доступом к защищаемой информации, определяются приказом директора Учреждения и входят в контролируемую зону.

11.2. Доступ в помещения с техническими средствами обработки защищаемой информации ограничивается и контролируется. Допуск посторонних лиц осуществляется только в сопровождении уполномоченных работников с фиксацией в журнале учёта посещений.

11.3. Помещения оборудуются:

— системами видеонаблюдения;

— системами охранно-пожарной сигнализации;

11.4. Вне рабочего времени рабочие места блокируются, съёмные носители информации помещаются в запираемые шкафы или сейфы, бумажные документы с

защищаемой информацией убираются в места ограниченного доступа («политика чистого стола»).

11.5. Утилизация и уничтожение носителей информации, содержащих защищаемую информацию, производятся способами, исключающими восстановление информации, с оформлением актов уничтожения.

12. ОБУЧЕНИЕ И ОСВЕДОМЛЁННОСТЬ РАБОТНИКОВ

12.1. Обучение работников Учреждения в области информационной безопасности является обязательным и включает:

- **вводный инструктаж** — проводится при приёме на работу до допуска к обработке защищаемой информации, включает ознакомление с настоящей Политикой и смежными документами под подпись;
- **ежегодное обучение** — проводится не реже одного раза в год для всех работников, включает вопросы актуальных угроз, социальной инженерии, парольной защиты, правил обращения с защищаемой информацией;
- **повышение квалификации** — для ответственного за обеспечение ИБ не реже одного раза в три года.

12.2. Учреждение проводит мероприятия по повышению осведомлённости работников: регулярные рассылки с напоминаниями о правилах ИБ, проведение учебных фишинговых атак (не менее одного раза в квартал), размещение обучающих материалов на внутреннем портале.

12.3. Результаты обучения документируются и хранятся в личных делах работников.

13. НЕПРЕРЫВНОСТЬ ДЕЯТЕЛЬНОСТИ И ВОССТАНОВЛЕНИЕ ПОСЛЕ ИНЦИДЕНТОВ

13.1. Для обеспечения непрерывности деятельности Учреждение разрабатывает и поддерживает в актуальном состоянии:

- план обеспечения непрерывности деятельности;
- план восстановления после аварий;
- процедуры резервного копирования и восстановления данных.

13.2. Для критичных информационных систем определяются целевые показатели:

- **RTO (Recovery Time Objective)** - максимально допустимое время восстановления;
- **RPO (Recovery Point Objective)** - максимально допустимая потеря данных по времени.

13.3. Резервное копирование осуществляется регулярно в соответствии с утверждённым графиком. Резервные копии хранятся в защищённом месте, физически отделённом от места расположения основных систем, с контролем целостности.

13.4. Не реже одного раза в год проводится тестирование процедур восстановления с оформлением отчёта и внесением корректировок.

14. КОНТРОЛЬ СООТВЕТСТВИЯ И АУДИТ

14.1. Контроль соблюдения требований настоящей Политики осуществляется:

- на уровне Учреждения - ответственным за обеспечение ИБ путём проведения плановых проверок и внутренних аудитов;

- на уровне внешних проверок - путём привлечения сторонних аудиторов для независимой оценки состояния ИБ.

14.2. Внутренний аудит информационной безопасности проводится не реже одного раза в год. Результаты оформляются отчётом, представляемым руководителю Учреждения.

14.3. При необходимости проводятся внеплановые проверки по фактам инцидентов, при изменении законодательства, при существенных изменениях в ИТ-инфраструктуре.

14.4. По результатам аудитов и проверок разрабатываются планы корректирующих действий, исполнение которых контролируется ответственным за ИБ.

14.5. Учреждение обеспечивает возможность проведения проверок уполномоченными государственными органами (ФСТЭК России, ФСБ России, Роскомнадзор) в рамках их компетенции.

15. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ ПОЛИТИКИ

15.1. Нарушение требований настоящей Политики влечёт ответственность в соответствии с законодательством Российской Федерации и локальными нормативными актами Учреждения.

15.2. В отношении работников Учреждения за нарушение требований Политики могут применяться следующие меры:

- **дисциплинарная ответственность** — замечание, выговор, увольнение по соответствующим основаниям в соответствии с Трудовым кодексом Российской Федерации;

- **материальная ответственность** — возмещение прямого действительного ущерба в соответствии со статьёй 238 ТК РФ;

- **административная ответственность** — в случаях, предусмотренных Кодексом Российской Федерации об административных правонарушениях;

- **уголовная ответственность** — в случаях, предусмотренных Уголовным кодексом Российской Федерации (статьи 137, 138, 272, 273, 274, 274.1 УК РФ).

15.3. Ответственность юридического лица за нарушение требований законодательства в области защиты информации установлена, в частности: — статьёй 13.11 КоАП РФ (нарушение законодательства о персональных данных); — статьёй 13.12 КоАП РФ (нарушение правил защиты информации); — Федеральным законом № 420-ФЗ от 30.11.2024 (оборотные штрафы за утечки ПДн).

16. ПОРЯДОК ПЕРЕСМОТРА И АКТУАЛИЗАЦИИ ПОЛИТИКИ

16.1. Настоящая Политика подлежит плановому пересмотру не реже одного раза в год с целью оценки её соответствия текущему состоянию информационной безопасности и актуальным требованиям законодательства.

16.2. Внеплановый пересмотр Политики проводится в следующих случаях:

- принятие новых либо изменение действующих нормативных правовых актов в области информационной безопасности;

- существенные изменения в ИТ-инфраструктуре Учреждения (внедрение новых информационных систем, изменение архитектуры);

- результаты внутренних и внешних аудитов, выявившие несоответствия; — реализация значительного инцидента информационной безопасности;

- реорганизация Учреждения либо изменение его основной деятельности.

16.3. Пересмотр Политики осуществляется ответственным за обеспечение ИБ с участием руководителей заинтересованных подразделений. Новая редакция Политики согласовывается и утверждается в порядке, аналогичном утверждению первоначальной редакции.

16.4. С каждой новой редакцией Политики работники Учреждения знакомятся под подпись.

Приложение 1
к Политике информационной безопасности

ПЕРЕЧЕНЬ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ

При разработке настоящей Политики использованы следующие нормативные правовые акты:

Федеральные законы:

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

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

3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

4. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

5. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;

6. Федеральный закон от 30.11.2024 № 420-ФЗ (оборотные штрафы за утечки персональных данных);

7. Трудовой кодекс Российской Федерации (статьи 85–90 о защите персональных данных работника).

Постановления Правительства Российской Федерации:

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

9. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Приказы ФСТЭК России:

10. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (до перехода на приказ № 117);

11. Приказ ФСТЭК России № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, а также в информационных системах, функционирующих на объектах критической информационной инфраструктуры» (вступил в силу с 01.03.2026);

12. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания Учреждения информационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

13. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

14. Методика оценки угроз безопасности информации (утверждена ФСТЭК России 05.02.2021).

Приказы ФСБ России:

15. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания Учреждения информационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации»;

16. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об Учреждения и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

ГОСТы:

17. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;

18. ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в Учреждения. Основные термины и определения»;

19. ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых операций. Базовый состав информационных и технических мер»;

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

21. ГОСТ Р ИСО/МЭК 27002-2021 «Информационная технология. Методы и средства обеспечения безопасности. Свод правил для мер обеспечения информационной безопасности».

Приложение 2
к Политике информационной безопасности

ПЕРЕЧЕНЬ БАЗОВЫХ МЕР ЗАЩИТЫ ПО ПРИКАЗАМ ФСТЭК РОССИИ

Базовый состав групп мер защиты информации (адаптируется под конкретный класс/уровень защищённости информационной системы):

Группа	Наименование группы мер	Приказ № 21	Приказ № 117 (ГИС)	Приказ № 239 (КИИ)

		(ИСПДн)		
ИАФ	Идентификация и аутентификация	✓	✓	✓
УПД	Управление доступом к ИС	✓	✓	✓
ОПС	Ограничение программной среды	✓	✓	✓
ЗНИ	Защита машинных носителей информации	✓	✓	✓
РСБ	Регистрация событий безопасности	✓	✓	✓
АВЗ	Антивирусная защита	✓	✓	✓
СОВ	Обнаружение вторжений	✓	✓	✓
АНЗ	Контроль (анализ) защищённости	✓	✓	✓
ОЦЛ	Обеспечение целостности ИС и информации	✓	✓	✓
ОДТ	Обеспечение доступности информации	✓	✓	✓
ЗСВ	Защита среды виртуализации	✓	✓	✓
ЗТС	Защита технических средств	✓	✓	✓
ЗИС	Защита ИС, её средств, систем связи	✓	✓	✓
ИНЦ	Выявление инцидентов и реагирование на них	✓	✓	✓
УКФ	Управление конфигурацией ИС	✓	✓	✓

Конкретный перечень мер с идентификаторами (например, ИАФ.1–ИАФ.7, УПД.1–УПД.17) устанавливается отдельным документом «Модель угроз и перечень мер защиты информационной системы» на основании результатов моделирования угроз и категорирования ИС.