ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
РЕСПУБЛИКИ КАРЕЛИЯ
«УЧЕБНО-МЕТОДИЧЕСКИЙ ЦЕНТР ПО ГРАЖДАНСКОЙ ОБОРОНЕ И ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ»
(ГКУ ДПО РК «УМЦ по ГОЧС»)

№ 5 от 20.05.2026
ГКУ ДПО РК
«УМЦ по ГОЧС»

УТВЕРЖДАЮ
Директор
И.В. Крисанов
«20» 05 2026 года

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Петрозаводск 2026

ОГЛАВЛЕНИЕ

Введение

Данная политика информационной безопасности (далее – Политика) представляет собой фундаментальный документ, определяющий всесторонний подход к обеспечению информационной безопасности во всех сферах деятельности ГКУ ДПО РК «УМЦ по ГОЧС» (далее – УМЦ). Политика не просто перечисляет правила, а формирует целостное мировоззрение, направленное на защиту ценных информационных активов. Она устанавливает стратегические цели и задачи по защите информации, задавая вектор развития системы управления информационной безопасностью и описывая принципы её построения. Успешная реализация уставных задач организации напрямую зависит от эффективного обеспечения информационной безопасности, что является одним из ключевых факторов её жизнеспособности и развития.

Под обеспечением информационной безопасности в рамках данной Политики понимается комплекс мероприятий, направленных на защиту информационных ресурсов организации, включая всевозможные данные, программное обеспечение, базы данных, а также всей сопутствующей инфраструктуры: компьютерной техники, сетей связи, систем хранения данных и т.д. Это комплексный подход, охватывающий все автоматизированные системы, телекоммуникационные сети и информационные потоки, которыми владеет и пользуется организация. Политика распространяется на все уровни доступа к информации – от работников до внешних контрагентов, взаимодействующих с информационными системами организации.

Важно подчеркнуть, что Политика исходит из принципиального понимания невозможности достижения абсолютной защищенности информации при использовании изолированных средств защиты. Безопасность учреждения достигается лишь путём комплексного и системного подхода, где все элементы СУИБ тесно взаимосвязаны и работают согласованно. Это требует тщательного анализа рисков, выбора оптимальных технических и организационных мер защиты, постоянного мониторинга и адаптации системы к изменяющимся угрозам. Разработка и внедрение любых элементов информационной системы должны рассматриваться в контексте общей архитектуры безопасности, как неотъемлемая часть единой, защищённой информационной среды. При этом необходимо стремиться к оптимальному балансу между уровнем защищенности, финансовыми затратами и операционной эффективностью. Политика предусматривает технические и организационные меры. К организационным мерам относятся разработка и утверждение внутренних нормативных актов, регламентирующих порядок доступа к информации,

обработку персональных данных, использование информационных ресурсов и т.д.

Обязательным элементом является обучение работников вопросам информационной безопасности, повышение их осведомлённости о возможных угрозах и правилах безопасного поведения. Помимо этого, регулярные аудиты и проверки системы безопасности позволяют оценить эффективность и своевременно выявлять уязвимости.

Важным аспектом является взаимодействие с внешними организациями и партнёрами. Политика должна регламентировать порядок обмена информацией с внешними субъектами, обеспечивая защиту конфиденциальности и целостности данных. Это включает в себя установление правил доступа, использование криптографических средств защиты и контроль за соблюдением договорных обязательств в сфере информационной безопасности.

Таким образом, политика информационной безопасности организации – это не просто набор правил, а стратегический документ, определяющий всеобъемлющий подход к защите информационных ресурсов. Её успешная реализация требует постоянного внимания, инвестиций в технологии и обучение персонала, а также постоянной адаптации к эволюционирующим угрозам в сфере информационной безопасности. Только системный, комплексный подход, учитывающий все аспекты – технические, организационные и человеческий фактор – позволит организации обеспечить необходимый уровень защищенности информации и гарантировать успешное выполнение своих уставных задач. Реализация Политики требует постоянного мониторинга, анализа и совершенствования системы защиты для обеспечения устойчивости к современным и будущим киберугрозам.

Термины и определения

1. **Авторизация** – процесс предоставления доступа к ресурсам на основе проверенной аутентификации.

2. **Аутентификация** – процесс проверки подлинности пользователя или устройства.

3. **Доступность** – обеспечение доступа к информации и связанным с ней активам авторизованным пользователям в нужное время.

4. **Информационная безопасность (ИБ)** – состояние информации, при котором обеспечивается её конфиденциальность, целостность и доступность.

5. **Инцидент информационной безопасности** – событие, которое может привести к нарушению конфиденциальности, целостности или доступности информации.

6. **Конфиденциальность** – обеспечение доступа к информации только авторизованным пользователям.

7. **Межсетевой экран (брандмауэр)** – система, предназначенная для защиты сети от несанкционированного доступа.

8. **Многофакторная аутентификация (MFA)** – использование нескольких методов аутентификации для повышения безопасности.

9. **Мониторинг безопасности** – процесс наблюдения за системой или сетью для обнаружения и предотвращения угроз.

10. **Обучение и осведомлённость** – программы и мероприятия, направленные на повышение знаний сотрудников в области информационной безопасности.

11. **Пароль** – секретная комбинация символов, используемая для аутентификации пользователя.

12. **План реагирования на инциденты** – набор процедур, которые описывают, как организация должна реагировать на инциденты информационной безопасности.

13. **Резервное копирование** – процесс создания копий данных для восстановления в случае их потери или повреждения.

14. **Риск** – вероятность того, что угроза воспользуется уязвимостью и приведёт к ущербу.

15. **Система обнаружения вторжений (IDS)** – система, предназначенная для обнаружения попыток несанкционированного доступа или атак.

16. **Система управления информационной безопасностью (СУИБ)** – комплекс структурированных политик, процессов и технических средств, направленных на обеспечение информационной безопасности в организации.

17. **Система контроля и управления доступом (СКУД)** – комплекс оборудования, главная функция которого – ограничение доступа на

охраняемый объект.

18. **Средство криптографической защиты информации (СКЗИ)** — программа или устройство, которое шифрует документы и генерирует электронную подпись.

19. **Угроза безопасности** – потенциальная возможность нарушения безопасности информации, которая может привести к ущербу.

20. **Уровень риска** – мера риска, выраженная в виде сочетания последствий и их вероятности.

21. **Учётная запись** – набор данных, который идентифицирует пользователя в системе и предоставляет доступ к ресурсам.

22. **Уязвимость** – слабое место в системе, которое может быть использовано угрозой для нарушения безопасности.

23. **Целостность** – обеспечение точности и полноты информации и методов её обработки.

24. **Шифрование** – процесс преобразования информации в форму, которая не может быть прочитана без соответствующего ключа.

1. Нормативные документы

Политика разработана в соответствии с требованиями законодательства Российской Федерации и регуляторов в области информационной безопасности:

1. Конституции Российской Федерации;

2. Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;

3. Федерального закона «О персональных данных»» от 27.07.2006 № 152-ФЗ;

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

5. Указа Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 06.03.1997 № 188;

6. Указа Президента РФ «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» от 01.05.2022 № 250;

7. Указа Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

8. Приказа ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02. 2013 № 21;

9. Приказа ФСО России от 07.09.2016 № 443 «Об утверждении положения о Российском государственном сегменте информационно-телекоммуникационной сети «Интернет»»;

10. Приказа ФСТЭК России от 11.04. 2025 № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений».

11. Методики оценки угроз безопасности информации, утверждённого ФСТЭК России 05.02.2021.

2. Цели, задачи и направления

Основная цель настоящей Политики заключается в защите информационных ресурсов от потенциального материального, физического, морального или иного ущерба, который может быть нанесен в результате случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также в минимизации рисков информационной безопасности.

Для достижения основной цели необходимо обеспечивать эффективное выполнение следующих задач:

2.1. Своевременное выявление, оценка и прогнозирование источников угроз ИБ;

2.2. Создание механизма оперативного реагирования на угрозы ИБ;

2.3. Предотвращение и/или снижение ущерба от реализации угроз ИБ;

2.4. Защита от вмешательства в процесс функционирования ИС посторонних лиц;

2.5. Соответствие требованиям Федерального законодательства, методических документов ФСБ России, ФСТЭК России, Роскомнадзора и договорным обязательствам в части ИБ;

2.6. Достижение адекватности мер по защите от угроз ИБ;

2.7. Изучение партнёров, клиентов, конкурентов и кандидатов на работу;

2.8. Недопущение проникновения структур организованной преступности и отдельных лиц с противоправными намерениями;

2.9. Выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности работников;

2.10. Повышение деловой репутации и корпоративной культуры.

3. Область действия

Настоящая Политика распространяется на деятельность УМЦ и обязательна для исполнения всеми его работниками. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

4. Принципы политики информационной безопасности

Эти принципы учитывают комплексный подход, законодательные требования и современные вызовы в области ИБ:

4.1. **Комплексность и системность** – обеспечение информационной безопасности достигается через согласованное взаимодействие технических, организационных и административных мер. Все элементы СУИБ должны быть взаимосвязаны и интегрированы в единую архитектуру, учитывающую все аспекты защиты информации.

4.2. **Конфиденциальность, целостность, доступность**

4.2.1. Конфиденциальность: доступ к информации предоставляется только авторизованным лицам или системам.

4.2.2. Целостность: гарантируется точность, полнота и неизменность информации и методов ее обработки.

4.2.3. Доступность: информация и связанные с ней ресурсы доступны авторизованным пользователям в нужное время.

4.3. **Риск-ориентированный подход - з**ащита информации основывается на регулярном анализе угроз и уязвимостей, оценке рисков и выборе мер, минимизирующих вероятность и последствия инцидентов. Меры защиты должны быть пропорциональны уровню риска.

4.4. **Минимизация и оптимальность:** меры безопасности должны обеспечивать необходимый уровень защиты при оптимальных финансовых и операционных затратах. Стремление к абсолютной безопасности не должно приводить к чрезмерным ограничениям или неоправданным расходам.

4.5. **Непрерывность и адаптивность**: система ИБ должна быть динамичной, с регулярным мониторингом, анализом и обновлением мер защиты для реагирования на новые угрозы, изменения в инфраструктуре или законодательстве.

4.6. **Соответствие нормативным требованиям**: политика ИБ должна соответствовать законодательству Российской Федерации.

4.7. **Ответственность и обучение персонала**: все работники обязаны соблюдать правила ИБ и проходить регулярное обучение по вопросам безопасного поведения, распознавания угроз и работы с информационными системами. Осведомлённость персонала — ключевой фактор снижения человеческого фактора как источника уязвимостей.

4.8. **Резервное копирование и восстановление** — регулярное создание резервных копий критически важных данных и тестирование процедур восстановления для обеспечения непрерывности бизнес-процессов в случае сбоев или атак.

4.9. **Прозрачность и документирование:** все процессы, связанные с ИБ, документируются (политики, регламенты, журналы аудита). Прозрачность процессов позволяет проводить проверки, выявлять уязвимости и подтверждать соответствие требованиям.

4.10. **Проактивность**: упор делается на предотвращение инцидентов путём раннего выявления угроз, анализа тенденций в области кибербезопасности и внедрения передовых технологий защиты.

4.11. **Учёт человеческого фактора**: Политика учитывает, что работники могут быть как слабым звеном, так и важным элементом защиты. Меры включают не только обучение, но и создание корпоративной культуры, поощряющей ответственное отношение к ИБ.

5. Организация управления информационной безопасностью

СУИБ обеспечивает координацию всех процессов ИБ в организации. СУИБ включает политику, регламенты, технические и организационные меры, направленные на защиту информации.

Роли и ответственность:

5.1. Руководство организации:

5.1.1. Утверждает политику ИБ и выделяет бюджет для её реализации;

5.1.2. Назначает ответственного за защиту ИБ и администратора информационной безопасности;

5.2. **Ответственный за защиту ИБ:**

5.2.1. Контролирует выполнение политики и координирует все аспекты СУИБ;

5.3. Администратор информационной безопасности:

5.3.1. Разрабатывает и внедряет регламенты, процедуры и меры защиты;

5.3.2. Проводит обучение сотрудников, мониторинг угроз и аудит системы ИБ;

5.3.3. Реагирует на инциденты.

5.4. Работники:

5.4.1. Соблюдают правила ИБ, изложенные в политике и регламентах;

5.4.2. Проходят обучение и сообщают о подозрительной активности;

5.4.3. Несут ответственность за нарушение Политики.

Регулярные совещания по ИБ проводятся не реже одного раза в квартал для обсуждения угроз, инцидентов и планов улучшения.

6. Управление рисками информационной безопасности

В соответствии с принципом риск-ориентированного подхода организация проводит регулярный анализ рисков информационной безопасности для выявления и минимизации угроз.

6.1. **Анализ угроз и уязвимостей**: проводится не реже одного раза в год с использованием методик ФСТЭК России. Угрозы включают кибератаки, утечки данных, сбои оборудования. Уязвимости выявляются через сканирование систем и аудит.

6.2. **Оценка рисков**: риски оцениваются по вероятности и потенциальному ущербу (низкий, средний, высокий). Например, утечка персональных данных классифицируется как высокий риск.

6.3. **План управления рисками**: для каждого риска разрабатываются меры:

6.3.1. технические: внедрение межсетевых экранов, шифрования, антивирусов;

6.3.2. организационные: обучение сотрудников, регламенты доступа.

6.4. **Мониторинг и пересмотр**: план рисков обновляется при внедрении новых систем, изменении законодательства или появлении новых угроз.

Ответственным за управление рисками является программист УМЦ, который готовит и представляет отчёты руководству в установленном порядке. Все сотрудники обязаны сообщать о выявленных уязвимостях или подозрительной активности.

7. Технические меры защиты

УМЦ использует современные технологии для защиты информации в соответствии с принципом многоуровневой защиты.

Ключевые меры:

7.1. **Межсетевые экраны (брандмауэры):** фильтруют сетевой трафик, предотвращая несанкционированный доступ, настраиваются для блокировки подозрительных IP-адресов.

7.2. **Шифрование**: все конфиденциальные данные защищаются сертифицированными СКЗИ при хранении и передаче. Используются протоколы TLS для сетевых соединений.

7.3. **Резервное копирование**: критические данные резервируются еженедельно, копии хранятся в сетевом хранилище. Процедуры восстановления тестируются ежегодно.

7.4. **Антивирусное ПО**: все устройства оснащены антивирусами с автоматическим обновлением. Проводятся ежемесячные проверки на

вредоносное ПО.

7.5. **Обновление ПО**: системы и приложения обновляются для устранения уязвимостей не реже одного раза в квартал.

8. Организационные меры защиты

Организационные меры обеспечивают соблюдение правил ИБ всеми сотрудниками в соответствии с принципами контроля доступа и прозрачности.

8.1. **Контроль доступа:**

8.1.1. Доступ предоставляется по принципу минимальных привилегий (Least Privilege);

8.1.2. Пароли должны быть сложными (не менее 12 символов, включая буквы, цифры, символы) и обновляться каждые 90 дней.

8.2. **Политика чистого стола и чистого экрана:**

8.2.1. Конфиденциальные документы хранятся в запираемых шкафах.

8.2.2. Рабочие станции блокируются автоматически через 5 минут бездействия.

8.3. **Правила использования ресурсов:**

8.3.1. Электронная почта используется только для рабочих задач, с фильтрацией входящих сообщений;

8.3.2. Доступ в интернет осуществляется через защищённые шлюзы с фильтрацией контента;

8.3.3. Применение личных устройств к корпоративной сети не допускается.

8.4. **Обработка конфиденциальной информации:**

8.4.1. Конфиденциальные данные обрабатываются в защищённых системах с использованием шифрования;

8.4.2. Передача данных возможна только через безопасные каналы.

8.5. **Утилизация носителей**

8.5.1. Носители информации (бумажные, электронные) уничтожаются сертифицированными методами (например, шредирование).

Все сотрудники обязаны ознакомиться с организационными мерами и подписать соответствующее соглашение. Нарушение правил влечёт дисциплинарную ответственность.

9. Безопасность персонала

Персонал является ключевым элементом системы ИБ, и его действия регулируются для снижения рисков, связанных с человеческим фактором, в соответствии с принципом ответственности и обучения.

9.1. **Соглашения о конфиденциальности:**

9.1.1. При приеме на работу сотрудники подписывают согласие на обработку персональных данных и согласие о неразглашении персональных данных.

9.1.2. При увольнении работники подписывают соглашение о неразглашении персональных данных, ставших им известными в ходе работы.

9.2. **Обучение ИБ:**

9.2.1. Инструктаж по ИБ (правила паролей, распознавание фишинга, работа с данными) проводится при приеме на работу в рамках вводного инструктажа по информационной безопасности

9.2.2. Обучение документируется, а участие является обязательным.

9.3. **Процедуры при увольнении или переводе:**

9.3.1. Сотрудник возвращает оборудование и все носители информации.

Нарушение правил ИБ сотрудниками влечёт дисциплинарные меры, включая увольнение.

10. Требования по информационной защите

10.1. В помещениях ГКУ ДПО РК «УМЦ по ГОЧС» использование личных портативных компьютеров и внешних носителей информации (диски, флеш-карты и т.п.) работниками запрещено, вынос служебных СВТ за пределы УМЦ производится только при согласовании с директором или заместителем директора.

10.2. Все работы в пределах УМЦ должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешённых к использованию.

10.3. Пользователи обязаны руководствоваться рекомендациями по защите своего пароля и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учётную запись третьим лицам, включая членов семьи.

10.4. В процессе работы сотрудники обязаны использовать режим «Экранной заставки» с парольной защитой. Рекомендуется устанавливать максимальное время «простоя» компьютера до появления экранной заставки не более 15 минут.

10.5. Каждый работник обязан немедленно уведомить администратора информационной безопасности, ответственного за ЗИ или руководство УМЦ обо всех случаях предоставления доступа третьим лицам к ресурсам сети учреждения.

10.6. Доступ к сети Интернет обеспечивается только в образовательных

и служебных целях и не может использоваться для незаконной деятельности. Запрещается посещение сайтов, содержащих оскорбительный, противозаконный или неэтичный контент.

10.7. Работники обязаны обеспечивать физическую безопасность оборудования, на котором хранится информация, включая компьютеры, ноутбуки и периферийные устройства.

10.8. Работникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения.

10.9. На всех компьютерах, используемых в УМЦ, должны быть установлены программы для защиты информации: межсетевой экран и антивирусное программное обеспечение.

10.10. Работникам запрещается блокировать, изменять настройки или устанавливать иное антивирусное ПО.

11. Физическая безопасность

Физическая безопасность предотвращает несанкционированный доступ, кражу или повреждение информационных активов в соответствии с принципом многоуровневой защиты.

11.1. **СКУД:** доступ предоставляется только уполномоченным лицам.

11.2. **Видеонаблюдение и сигнализация:**

11.2.1. Установлена пожарная и охранная сигнализация.

11.3. **Сторонние службы:**

11.3.1. Уборка, техническое обслуживание и другие службы работают под надзором.

11.4. **Защита от физических угроз:**

11.4.1. Оборудование защищено от пожара, затопления и перебоев питания с помощью систем климат-контроля и резервного питания.

11.4.2. Серверы размещаются в сейсмоустойчивых стойках.

12. Управление инцидентами информационной безопасности

В соответствии с принципом реагирования на инциденты организация разработала процедуры для обнаружения, локализации и устранения инцидентов ИБ, таких как утечки данных, кибератаки или сбои.

12.1. **Определение инцидента** – событие, нарушающее конфиденциальность, целостность или доступность информации (например, фишинговая атака, сбой сервера).

12.2. **Обнаружение**: сотрудники обязаны сообщать о подозрительной активности в течение 1 часа.

12.3. **Локализация:**

12.3.1. Блокировка заражённых учётных записей или устройств;

12.3.2. Отключение поражённых систем от сети.

12.4. **Устранение:**

12.4.1. Восстановление данных из резервных копий.

12.4.2. Устранение уязвимостей (например, обновление ПО).

12.5. **Анализ**:

12.5.1. Выявление причин инцидента и оценка ущерба.

12.5.2. Разработка мер для предотвращения повторения.

12.6. **Уведомление**: при утечке персональных данных регуляторы уведомляются в соответствии с требованиями Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ.

13. Взаимодействие с внешними сторонами

В соответствии с принципом защиты при взаимодействии с внешними сторонами организация обеспечивает безопасность обмена данными с партнёрами, подрядчиками и другими субъектами.

13.1. **Защищённые каналы связи:**

13.1.1. Обмен данными осуществляется через протоколы с шифрованием (TLS).

13.1.2. Используются сертифицированные СКЗИ для защиты конфиденциальных данных.

13.2. **Договорные обязательства:**

13.2.1. Договоры с внешними сторонами включают пункты о соблюдении стандартов ИБ.

13.2.2. Указывается ответственность за утечки данных или нарушения.

14. Реализация политики информационной безопасности

Реализация Политики информационной безопасности ГКУ ДПО РК «УМЦ по ГОЧС» осуществляется на основе нормативных документов, определяющих порядок выполнения процедур и процессов, связанных с профессиональной деятельностью.

15. Порядок внесения изменений и дополнений в политику информационной безопасности

Изменения и дополнения в политику информационной безопасности вносятся не реже одного раза в три года для обеспечения соответствия установленных мер защиты актуальным условиям и требованиям законодательства в области информационной безопасности.

16. Контроль за соблюдением политики информационной безопасности

16.1. Текущий контроль за соблюдением требований политики

информационной безопасности в УМЦ возлагается на заместителя директора.

16.2. Заместитель директора совместно с администратором информационной безопасности анализирует выполнение и соблюдение положений Политики и осуществляет контроль за исполнением её требований.

17. Ответственность за нарушение политики информационной безопасности

17.1. Ответственность за выполнение правил политики информационной безопасности несет каждый работник УМЦ в рамках своих служебных обязанностей и полномочий.

17.2. На основании ст. 192 Трудового кодекса Российской Федерации работники, нарушающие требования политику информационной безопасности УМЦ, могут быть привлечены к дисциплинарной ответственности.

17.3. Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный УМЦ в результате нарушения ими правил Политики (ст. 238 Трудового кодекса Российской Федерации).

17.4. За неправомерный доступ к служебной информации, не связанной с исполнением своих должностных обязанностей, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, работники УМЦ несут ответственность в соответствии с законами Российской Федерации.