

ПОЛИТИКА
информационной безопасности
в Государственном бюджетном учреждении культуры Республики Крым «Крымская
республиканская библиотека для молодежи»

Введение

Данная Политика информационной безопасности в Государственном бюджетном учреждении культуры Республики Крым «Крымская республиканская библиотека для молодежи» (далее – Политика, ГБУК КРБДМ соответственно) представляет собой фундаментальный документ, определяющий всесторонний подход к обеспечению информационной безопасности во всех сферах деятельности ГБУК КРБДМ.

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 (далее – СУИБ) и описывая принципы ее построения. Успешная реализация уставных задач ГБУК КРБДМ напрямую зависит от эффективного обеспечения информационной безопасности, что является одним из ключевых факторов ее жизнеспособности и развития.

Под обеспечением информационной безопасности в рамках данной Политики понимается комплекс мероприятий, направленных на защиту информационных ресурсов ГБУК КРБДМ, 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 ГБУК КРБДМ. Политика распространяется на все уровни доступа к информации – от сотрудников до внешних контрагентов, взаимодействующих с информационными системами ГБУК КРБДМ.

Важно подчеркнуть, что Политика исходит из принципиального понимания невозможности достижения абсолютной защищенности информации при использовании изолированных средств защиты. Безопасность учреждения ГБУК КРБДМ достигается лишь путем 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, защищенной информационной среды. При этом необходимо стремиться к оптимальному балансу между уровнем защищенности, финансовыми затратами и операционной эффективностью.

Политика предусматривает не только технические, но 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 сотрудников вопросам информационной безопасности, повышение их осведомленности о возможных угрозах и правилах безопасного поведения.

Регулярные аудиты и проверки системы безопасности позволяют оценить ее эффективность и своевременно выявлять уязвимости.

Важным аспектом является взаимодействие с внешними организациями и

партнерами. 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 ГБУК КРБДМ – это не просто набор правил, а стратегический документ, определяющий всеобъемлющий подход к защите информационных ресурсов. Ее успешная реализация требует постоянного внимания, инвестиций в технологии и обучение персонала, а также постоянно адаптации к эволюционирующим угрозам в сфере информационной безопасности. Только системный, комплексный подход, учитывающий все аспекты – технические, организационные и человеческий фактор – позволит ГБУК КРБДМ 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. **Виртуальная частная сеть (VPN)** – Технология, обеспечивающая безопасный удаленный доступ к сети через интернет.
4. **Доступность** – Обеспечение доступа к информации и связанным с ней активам авторизованным пользователям в нужное время.
5. **Информационная безопасность (ИБ)** – Состояние информации, при котором обеспечивается её конфиденциальность, целостность и доступность.
6. **Инцидент информационной безопасности** – Событие, которое может привести к нарушению конфиденциальности, целостности или доступности информации.
7. **Конфиденциальность** – Обеспечение доступа к информации только авторизованным пользователям.
8. **Межсетевой экран (брандмауэр)** – Система, предназначенная для защиты сети от несанкционированного доступа.
9. **Многофакторная аутентификация (MFA)** – Использование нескольких методов аутентификации для повышения безопасности.
10. **Мониторинг безопасности** – Процесс наблюдения за системой или сетью для обнаружения и предотвращения угроз.
11. **Обучение и осведомленность** – Программы и мероприятия, направленные на повышение знаний сотрудников в области информационной безопасности.
12. **Пароль** – Секретная комбинация символов, используемая для аутентификации пользователя.
13. **План реагирования на инциденты** – Набор процедур, которые описывают, как организация должна реагировать на инциденты информационной безопасности.
14. **Резервное копирование** – Процесс создания копий данных для восстановления в случае их потери или повреждения.
15. **Риск** – Вероятность того, что угроза воспользуется уязвимостью и приведет к ущербу.
16. **Система обнаружения вторжений (IDS)** – система, предназначенная для обнаружения попыток несанкционированного доступа или атак.
17. **Система управления информационной безопасностью (СУИБ)** – Комплекс структурированных политик, процессов и технических средств, направленных на обеспечение информационной безопасности в организации.

18. **Система контроля и управления доступом (СКУД)** – Комплекс оборудования, главная функция которого – ограничение доступа на охраняемый объект.

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

20. **Угроза безопасности** – Потенциальная возможность нарушения безопасности информации, которая может привести к ущербу.

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

22. **Учетная запись** – Набор данных, который идентифицирует пользователя в системе и предоставляет доступ к ресурсам.

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

24. **Целостность** – Обеспечение точности и полноты информации и методов её обработки.

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

1. Нормативные документы

Политика разработана в соответствии с законодательством Российской Федерации и требованиями Регуляторов в области информационной безопасности:

- Конституция Российской Федерации;
- Уголовный Кодекс Российской Федерации. Статья 272. Неправомерный доступ к компьютерной информации;
- Уголовный Кодекс Российской Федерации. Статья 273. Создание, использование и распространение вредоносных компьютерных программ;
- Уголовный Кодекс Российской Федерации. Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;
- Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 06.03.1997 г. № 188;
- Указ Президента РФ «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» от 01.05.2022 г. № 250;
- Указ Президента РФ «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05.12.2016 г. № 646;
- Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 г. № 687;
- Постановление Правительства РФ ««Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 г. № 1119;
- Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ;
- Федеральный закон «О персональных данных» от 27.07.2006 г. № 152-ФЗ;
- Федеральный закон «О коммерческой тайне» от 29.07.2004 г. № 98-ФЗ;
- Федеральный закон «Об электронной подписи» от 06.04.2011 г. № 63-ФЗ;
- Приказ 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 г. № 21;
- Приказ ФСО России «Об утверждении положения о Российском государственном сегменте информационно- телекоммуникационной сети «Интернет»» от 07.09.2016 г. № 443;

- Приказ ФСБ России «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» от 10.07.2014 г. № 378;

- Приказ ФСБ России «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств» от 18.03.2025 г. № 117;

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

- иные нормативные правовые акты Российской Федерации и нормативные документы уполномоченных органов государственной власти.

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 (далее – ИБ).

Для достижения основной цели необходимо обеспечивать эффективное выполнение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз ИБ;
- создание механизма оперативного реагирования на угрозы ИБ;
- предотвращение и/или снижение ущерба от реализации угроз ИБ;
- защита от вмешательства в процесс функционирования ИС посторонних лиц;
- соответствие требованиям Федерального законодательства, методических документов ФСБ России, ФСТЭК России, Роскомнадзор и договорным обязательствам в части ИБ;
- обеспечение непрерывности критических бизнес-процессов;
- достижение адекватности мер по защите от угроз ИБ;
- изучение партнёров, клиентов, конкурентов и кандидатов на работу;
- недопущение проникновения структур организованной преступности и отдельных лиц с противоправными намерениями;
- выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников; повышение деловой репутации и корпоративной культуры.

3. Область действия

Настоящая Политика распространяется на все структурные подразделения ГБУК КРБДМ и обязательна для исполнения всеми его сотрудниками и должностными лицами. 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

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

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

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

4.3 Риск-ориентированный подход

Защита 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 должна соответствовать законодательству Российской Федерации.

4.7 Ответственность и обучение персонала

Все сотрудники обязаны соблюдать правила ИБ и проходить регулярное обучение по вопросам безопасного поведения, распознавания угроз и работы с информационными системами. Осведомленность 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 путем раннего выявления угроз, анализа тенденций в области кибербезопасности и внедрения передовых технологий защиты.

4.11 Учет человеческого фактора

Политика учитывает, что сотрудники 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

Система управления информационной безопасностью обеспечивает координацию всех процессов ИБ в ГБУК КРБДМ. СУИБ включает политики, регламенты, технические и организационные меры, направленные на защиту информации.

Роли и ответственность:

- **Руководство ГБУК КРБДМ:**

- Утверждает политику ИБ и выделяет бюджет для её реализации.

- Назначает ответственных за информационную безопасность.
 - Контролирует выполнение Политики.
 - **Ответственные лица:**
 - Разрабатывают и внедряют регламенты, процедуры и меры защиты.
 - Проводят обучение сотрудников, мониторинг угроз и аудит системы ИБ.
 - Координируют реагирование на инциденты.
 - **Сотрудники:**
 - Соблюдают правила ИБ, изложенные в Политике и регламентах.
 - Проходят обучение и сообщают о подозрительной активности.
 - Несут ответственность за нарушение Политики (вплоть до дисциплинарных мер).
- 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 ГБУК КРБДМ проводит регулярный анализ рисков информационной безопасности для выявления и минимизации угроз.

6.1 Процесс управления рисками:

- **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.
 - **Оценка рисков:** Риски оцениваются по вероятности и потенциальному ущербу (низкий, средний, высокий). Например, утечка персональных данных классифицируется как высокий риск.
 - **План управления рисками:** Для каждого риска разрабатываются меры:
 - Технические: внедрение межсетевых экранов, шифрования, антивирусов.
 - Организационные: обучение сотрудников, регламенты доступа.
 - **Мониторинг и пересмотр:** План рисков обновляется при внедрении новых систем, изменении законодательства или появлении новых угроз.
- Ответственным за управление рисками является отдел ИБ.
- Все сотрудники обязаны сообщать о выявленных уязвимостях или подозрительной активности.

7. Технические меры защиты

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

Ключевые меры:

- **Межсетевые экраны (брандмауэры):** Фильтруют сетевой трафик, предотвращая несанкционированный доступ. Настраиваются для блокировки подозрительных IP-адресов.
- **Шифрование:** Все конфиденциальные данные защищаются сертифицированными СКЗИ при хранении и передаче. Используются протоколы TLS для сетевых соединений.
- **Многофакторная аутентификация (MFA):** Применяется для доступа к ключевым устройствам.
- **Резервное копирование:** Критические данные резервируются ежемесячно, копии хранятся в защищённом месте.
- **Антивирусное ПО:** Ключевые устройства оснащены антивирусами с автоматическим обновлением. Проводятся автоматические проверки на вредоносное ПО.

- **Обновление ПО:** Системы и приложения обновляются для устранения уязвимостей автоматически или при необходимости.

8. Организационные меры защиты

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

Ключевые меры:

- **Контроль доступа:**
 - Пароли должны быть сложными (не менее 8 символов, включая буквы, цифры, символы) и обновляться каждые полгода.
 - **Политика чистого стола и чистого экрана:**
 - Конфиденциальные документы хранятся в запираемых шкафах.
 - Рабочие станции блокируются автоматически через 5 минут бездействия.
 - **Правила использования ресурсов:**
 - Электронная почта используется только для рабочих задач, с фильтрацией входящих сообщений.
 - Доступ в интернет осуществляется с фильтрацией контента.
 - Личные устройства допускаются к корпоративной сети только после проверки системным администратором.
 - **Обработка конфиденциальной информации:**
 - Конфиденциальные данные обрабатываются в защищённых системах с использованием шифрования.
 - **Утилизация носителей:** Носители информации (бумажные, электронные) уничтожаются сертифицированными методами (например, shredding, перезапись данных).
- 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.

Ключевые меры:

- **Соглашения о конфиденциальности:**
 - Все сотрудники подписывают соглашение о неразглашении персональных данных.
 - Соглашение включает ответственность за нарушение правил ИБ.
- **Обучение ИБ:**
 - При трудоустройстве проводится вводный инструктаж по ИБ (правила паролей, распознавание фишинга, работа с данными).
 - Обучение документируется, а участие является обязательным.
- **Процедуры при увольнении или переводе:**
 - Доступ к системам блокируется в течение 24 часов после увольнения.
 - Проводится аудит активности сотрудника за последний месяц.
 - Сотрудник возвращает все носители информации и оборудование.

Руководство обеспечивает финансирование программ обучения, а ответственные лица координируют их проведение. Нарушение правил ИБ сотрудниками влечёт дисциплинарные меры.

10. Требования по информационной защите

10.1 В отношении всех информационных активов ГБУК КРБДМ, активов, находящихся под контролем ГБУК КРБДМ, а также активов, используемых для доступа к инфраструктуре ГБУК КРБДМ, должна быть определена ответственность соответствующего сотрудника.

10.2 Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами ГБУК КРБДМ должна доводиться до сведения руководителя.

10.3 Внос в здание и помещения ГБУК КРБДМ личных портативных компьютеров и внешних носителей информации (диски, флеш-карты и т.п.), а также вынос их за пределы ГБУК КРБДМ производится только при согласовании с системным администратором.

10.4 Все данные, составляющие тайну ГБУК КРБДМ и хранящиеся на внешних жестких дисках, портативных компьютерах, должны быть зашифрованы.

10.5 Все работы в пределах ГБУК КРБДМ должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию администрацией.

10.6 В целях обеспечения санкционированного доступа к информационным ресурсам ГБУК КРБДМ, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

10.7 Пользователи обязаны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять доступ к служебному компьютеру третьим лицам.

10.8 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.

10.9 Пароли для входа в операционную систему, BIOS, электронную почту, а также в информационные системы, используемые в учреждении, хранятся у ответственного за информационную безопасность.

10.10 При использовании для авторизации в информационных системах учетной записи портала «Госуслуги» или квалифицированной электронной подписи (КЭП) передача паролей не требуется и не допускается.

10.11 Пароли учитываются в Журнале учета паролей, используемых в работе на автоматизированных рабочих местах.

10.12 Каждый сотрудник обязан немедленно уведомить системного администратора обо всех случаях предоставления доступа третьим лицам к ресурсам сети ГБУК КРБДМ.

10.13 Доступ к сети Интернет обеспечивается только в служебных целях и не может использоваться для незаконной деятельности. Запрещается посещение сайтов, содержащих оскорбительный, противозаконный или неэтичный контент.

10.14 Сотрудники обязаны обеспечивать физическую безопасность оборудования, на котором хранится информация ГБУК КРБДМ, включая компьютеры, ноутбуки и периферийные устройства.

10.15 Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит системным администратором.

10.16 Все ключевые рабочие станции должны быть оснащены антивирусным программным обеспечением, утвержденным системным администратором. Сотрудникам запрещается блокировать, изменять настройки или устанавливать иное антивирусное

ПО.

10.17 Сотрудники обязаны регулярно создавать резервные копии всех основных служебных данных и программного обеспечения, используемых в рабочих процессах.

11. Физическая безопасность

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

Ключевые меры:

- **Видеонаблюдение и сигнализация:**
 - Критические зоны находятся под круглосуточным видеонаблюдением.
 - Установлены пожарные и охранные сигнализации с уведомлением службы безопасности.
- **Контроль доступа посетителей:**
 - Все посетители регистрируются на входе и сопровождаются сотрудниками.
- **Сторонние службы:**
 - Техническое обслуживание и другие службы работают под надзором.
- **Защита от физических угроз:**
 - Ключевые рабочие станции защищены от перебоев питания с помощью системы резервного питания.
 - Системный администратор обеспечивает техническое обслуживание оборудования.

12. Управление инцидентами информационной безопасности

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

Процесс управления инцидентами:

- **Определение инцидента:** Событие, нарушающее целостность, конфиденциальность, или доступность информации (например, фишинговая атака, сбой сервера).
- **Обнаружение:**
 - Сотрудники обязаны сообщать о подозрительной активности в течение 1 часа.
- **Локализация:**
 - Блокировка заражённых учётных записей или устройств.
 - Отключение поражённых систем от сети.
- **Устранение:**
 - Восстановление данных из резервных копий.
 - Устранение уязвимостей (например, обновление ПО).
- **Анализ:**
 - Выявление причин инцидента и оценка ущерба.
 - Разработка мер для предотвращения повторения.
- **Уведомление:** При утечке персональных данных регуляторы уведомляются в течение 72 часов в соответствии с ФЗ-152. Все инциденты регистрируются в журнале, который ведёт ответственное лицо. Ежегодно проводятся учения для подготовки к инцидентам. Отчёт об инцидентах предоставляется руководству в течение 5 дней после устранения.

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.

Ключевые меры:

- **Защищённые каналы связи:**

- Обмен данными осуществляется через защищённые системы ЭДО, использующие протоколы с шифрованием (TLS).

- Используются сертифицированные СКЗИ для защиты конфиденциальных данных.

- **Договорные обязательства:**

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

- Указывается ответственность за утечки данных или нарушения.

14. Реализация политики информационной безопасности

Реализация Политики информационной безопасности ГБУК КРБДМ осуществляется на основе нормативных документов, определяющих порядок выполнения процедур и процессов, связанных с профессиональной деятельностью в ГБУК КРБДМ.

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

Текущий контроль за соблюдением требований Политики информационной безопасности ГБУК КРБДМ возлагается на сотрудника, назначенного приказом руководителя ГБУК КРБДМ.

Руководитель ГБУК КРБДМ регулярно анализирует выполнение и соблюдение положений Политики информационной безопасности, а также осуществляет последующий контроль за исполнением ее требований.

17. Ответственность за нарушение Политики безопасности

Ответственность за выполнение правил ПБ несет каждый сотрудник ГБУК КРБДМ в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса Российской Федерации сотрудники, нарушающие требования Политики, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

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

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, сотрудники ГБУК КРБДМ несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.