Директор краевого
государственного автономного
учреждения
«Краевой дворец молодежи»

_____ А.Е. Коробков
«____» _____2026 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Разработал:
Техник-программист А.А. Михайлов

г. Барнаул
2026

Предисловие

1. Политика разработана Краевым государственным автономным учреждения «Краевой дворец молодёжи» (далее - КГАУ «Краевой дворец молодёжи»).

2. Внесено техником-программистом КГАУ «Краевой дворец молодёжи» Михайловым А.А.

3. Утверждено и введено в действие приказом по организации от _____ № ___. Дата введения _____.

4. Настоящая Политика разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и иными нормативными правовыми документами.

Содержание

1. Общие положения 4
2. Термины и определения 5
3. Область применения 7
4. Цели, задачи и направления 8
5. Принципы защиты информации 9
6. Объекты защиты 13
7. Роли и обязанности лиц, участвующих в защите информирование 15
8. Техническое обеспечение информационной безопасности 17
9. Организационное обеспечение информационной безопасности 21
10. Управление доступом 23
11. Ответственность за нарушения в области информационной безопасности 27

1. Общие положения

Информационные ресурсы являются одним из ключевых активов КГАУ «Краевой дворец молодёжи» (далее – КГАУ "КДМ"). Данные информационные активы подлежат защите в соответствии с их ценностью, и способом, направленным на исключение и минимизацию рисков несанкционированного доступа и противоправных действий в отношении их. КГАУ «КДМ» осуществляет постоянное совершенствование системы информационной безопасности, обеспечивая соответствие законодательству и регуляторным нормам Российской Федерации.

Политика информационной безопасности КГАУ «КДМ» (далее – Политика) является корпоративным документом, который формулирует и отображает позицию КГАУ «КДМ» в области информационной безопасности, описывает основные принципы, определяющие высокоуровневые цели и задачи обеспечения информационной безопасности КГАУ «КДМ».

Настоящая Политика разработана в соответствии с законодательством Российской Федерации и требованиями Регуляторов в области информационной безопасности, с учетом лучших международных практик, в том числе отраженных в семействе стандартов серии ISO 27000, представленного в Российской Федерации как национальный стандарт "ГОСТ Р ИСО/МЭК 27000-2021" утвержденный Федеральным агентством по техническому регулированию и метрологии.

2. Термины и определения

2.1. В настоящей Политике используются термины и определения, установленные законодательством Российской Федерации об информации, информационных технологиях и о защите информации, а также термины и определения, установленные национальными стандартами в области защиты информации.

2.2. В настоящей Политике используются следующие понятия:

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Безопасность информации – защищенность информации от ее нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного ее тиражирования.

Доступность – возможность для авторизованного пользователя информационной системы за приемлемое время получить информационную услугу, предусмотренную функциональностью.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная безопасность (ИБ) – комплекс административно-правовых, организационно-распорядительных и технических мер, направленных на обеспечение конфиденциальности, целостности и санкционированной доступности информации в процессе ее сбора, обработки, передачи и хранения.

Информационная система (ИС) обработки информации – организационно-техническая структура, представляющая собой совокупность следующих взаимосвязанных компонентов:

- технических средств обработки и передачи данных;
- методов и алгоритмов обработки в виде соответствующего программного обеспечения;

– баз данных на различных носителях;

– персонала и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных.

Конфиденциальность – защита от несанкционированного ознакомления.

Несанкционированное действие – действие субъекта в нарушение установленных в системе правил обработки информации.

Пользователь – субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации.

Сеть (локальная сеть, ЛВС, LAN) – группа точек, узлов или других устройств, соединенных коммуникационным набором оборудования, обеспечивающее соединение станций и передачу между ними информации.

Угроза – реально или потенциально возможные действия по реализации опасных воздействующих факторов с целью преднамеренного или случайного нарушения режима функционирования объекта.

Уязвимость – любая характеристика автоматизированной системы, использование которой может привести к реализации угроз.

Целостность информации – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому ее состоянию).

Шифрование – это преобразование данных в нечитабельную форму, используя ключи шифрования-расшифровки.

3. Область применения

3.1. Требования Политики распространяются на процессы КГАУ «КДМ», на всю информационно-техническую инфраструктуру организации, включая системы виртуализации и средства мониторинга, механизмы контроля действий всех пользователей, включая внешних специалистов, системы защиты от несанкционированного доступа и компьютерных атак, средства мониторинга безопасности и системы обнаружения вторжений, процессы управления уязвимостями, механизмы реагирования на инциденты, системы резервного копирования и восстановления.

3.2. Требования являются обязательными для выполнения всеми работниками КГАУ «КДМ», а также распространяются на взаимоотношения с поставщиками, провайдерами и иными партнерами, услуги которых связаны с использованием, обработкой или доступом к информации или информационным активам КГАУ «КДМ». Область применения настоящей Политики покрывает весь жизненный цикл (создание, эксплуатация и вывод из эксплуатации) защищаемых объектов КГАУ «КДМ».

3.3. Положения настоящей Политики распространяются на все информационные системы и на всех сотрудников КГАУ «КДМ».

3.4. Положения настоящей Политики обязательны к исполнению для всех пользователей информационных систем КГАУ «КДМ» (далее - Пользователи), а также для администраторов безопасности и системных администраторов (далее - Администраторы).

3.5. В соответствии с указом Президента Российской Федерации № 188 «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 года к сведениям конфиденциального характера (защищаемой информации) в КГАУ «КДМ» относятся:

– сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные

данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

– сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

– служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

– сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

4. Цели, задачи и направления

4.1. Целями настоящей Политики являются обеспечение конфиденциальности, целостности, доступности защищаемой информации КГАУ «КДМ». Защита корпоративной информационной системы КГАУ «КДМ» (далее – ИС) от возможного нанесения им материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а также минимизация уровня рисков информационной безопасности.

4.2. Цели, задачи и направления Политики:

– поддержка процессов КГАУ «КДМ» посредством обеспечения Конфиденциальности, Целостности и Доступности информации и информационных систем;

– снижение риска нарушения Конфиденциальности, Целостности и Доступности информации путем определения правил использования информации и информационных систем;

– распространение информации об общих правилах ИБ среди работников КГАУ «КДМ» и третьих лиц, которая определяет обязанности, ответственность и роль каждого работника;

– обеспечение соответствия нормам законодательства РФ, требованиям Регуляторов, миссии КГАУ «КДМ»;

– обеспечение защиты деловой репутации и имиджа КГАУ «КДМ»;

– обеспечение масштабирования процессов КГАУ «КДМ» и укрепление доверия клиентов к продуктам и услугам КГАУ «КДМ», создавая таким путем конкурентные преимущества;

– управление ИБ, в частности определение ролей и обязанностей в области ИБ всех сотрудников КГАУ «КДМ»;

– классификация информационных активов;

– проведение оценки рисков ИБ;

– обеспечение безопасности информационных активов в соответствии с категорией их классификации и оценкой рисков;

– мониторинг событий ИБ и управление Инцидентами ИБ;

– обеспечение непрерывности деятельности КГАУ «КДМ»;

– организация и контроль обеспечения безопасного управления жизненным циклом информационных систем КГАУ «КДМ».

5. Принципы защиты информации

5.1. Деятельность КГАУ «КДМ» в области информационной безопасности осуществляется с соблюдением следующих основных принципов.

5.2. **Ориентация на стратегию КГАУ «КДМ»** – стратегические инициативы по информационной безопасности разрабатываются и осуществляются в соответствии с общей стратегией и целями развития КГАУ «КДМ», с учетом корпоративных стратегий в области информационных

технологий и в области производственной автоматизации, метрологии и контроля качества.

5.3. **Централизация функций управления** – принцип заключается в возможности принятия управленческих решений в области информационной безопасности на уровне КГАУ «КДМ» за счет оперативного мониторинга (ИТ-пространства КГАУ «КДМ» и внешней обстановки в информационной сфере) и оценки состояния информационной безопасности; осуществления централизованного управления стратегическими инициативами по информационной безопасности; контроля реализации мероприятий по развитию информационной безопасности; создания и развития централизованных решений в области информационной безопасности.

5.4. **Проактивный подход и управление рисками** – базируется на мониторинге, анализе и оценке появляющихся, актуальных и будущих ИБ-рисков и угроз информационной безопасности (включая изучение технологий, используемых злоумышленниками) с целью своевременного и осознанного принятия превентивных мер для предупреждения компьютерных атак и недопущения ущерба КГАУ «КДМ».

5.5. **Стандартизация и унификация** – подразумевает разработку стандартизованных требований и подходов, типовых технических решений и элементов архитектуры обеспечения информационной безопасности для унификации средств и методов решения однотипных задач; интерфейсов управления системами информационной безопасности.

5.6. **Импортозамещение** – заключается в снижении рисков неблагоприятной внешней конъюнктуры за счёт ориентирования на отечественные решения, средства и сервисы при обеспечении информационной безопасности на территории Российской Федерации.

5.7. **Ресурсное обеспечение** – означает необходимость выделения целевого финансирования на обеспечение и развитие информационной

безопасности КГАУ «КДМ», поддержание требуемой организационной структуры.

5.8. **Законность и соответствие** – деятельность по обеспечению информационной безопасности КГАУ «КДМ» основывается на выполнении требований нормативных правовых актов Российской Федерации.

5.9. **Повышение культуры информационной безопасности** – декларирует необходимость не только информировать всех работников КГАУ «КДМ», её Деловых партнёров и третьих лиц, использующих ИТ-активы КГАУ «КДМ», о требованиях информационной безопасности, также развивать навыки приемлемого обращения с информацией и безопасной работы с ИТ-активами КГАУ «КДМ».

5.10. **Развитие компетенций и профессионализма** – принцип означает необходимость постоянного развития компетенций и практических навыков специалистов по информационной безопасности в условиях непрекращающегося изменения ИБ-рисков, ландшафта используемых информационных технологий и техник потенциальных нарушителей. Обеспечение информационной безопасности при автоматизации технологических и производственных процессов требует компетенций и знаний в области информационной безопасности.

5.11. **Накопление знаний и обмен опытом** – следует накапливать знания и обмениваться опытом в ходе осуществления практической деятельности по обеспечению информационной безопасности (при мониторинге и реагировании на компьютерные атаки, при внедрении и эксплуатации технических решений, при аудитах информационной безопасности и т.д.).

5.12. **Информационная безопасность как свойство информации** – принцип заключается в следующем:

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

– предпочтительными являются ИТ-активы с наибольшим покрытием требований информационной безопасности встроенными функциями (при прочих равных характеристиках);

– встроенные функции по информационной безопасности должны быть настроены и использоваться при эксплуатации ИТ-активов, включая программно-аппаратные средства, автоматизированные системы управления и т.д.;

– соответствие приобретаемого/внедряемого ИТ-актива требуемому уровню информационной безопасности подтверждается согласно существующими процедурами, с учетом требований применимого законодательства.

5.13. **Информационная безопасность как неотъемлемое свойство ИТ-услуги** – означает, что предлагаемые и оказываемые в интересах КГАУ «КДМ» ИТ-услуги и ИТ-сервисы должны разрабатываться и оказываться с учетом требований информационной безопасности.

5.14. **Совместимость** – подразумевает подбор компонентов для обеспечения информационной безопасности способом, гарантирующим их взаимную системную совместимость с используемыми ИТ-решениями, информационными технологиями и с решениями по автоматизации технологических и производственных процессов КГАУ «КДМ».

5.15. **Надежность** – использование компонентов и средств для обеспечения информационной безопасности, соответствующих требованиям по надежности, готовности и обслуживаемости.

5.16. **Адекватность и обоснованность решений** – принимаемые в КГАУ «КДМ» меры и применяемые средства информационной безопасности эффективны, результативны и соразмерны с величиной ИБ-рисков и угроз информационной безопасности, влияющих на цели КГАУ «КДМ».

5.17. **Комплексность** – применение любых доступных законных методов, средств и мероприятий (включая законодательные и нормативно-правовые, организационно-административные, программно-технические, инженерно-

технические, физические), направленных на снижение ИБ-рисков, пресечение угроз информационной безопасности и недопущение ущерба КГАУ «КДМ», её Деловым партнёрам и работникам.

5.18. **Разделение и минимизация полномочий** – означает, что выполнение критичных (итоговых) операций проводится только посредством разделения действий. Исключение единоличного совершения критичной операции может быть организовано на уровне организационных мер и/или программно-технических средств за счет выделения полномочий или роли пользователя. Программно-технический способ разделений полномочий является предпочтительным относительно организационного. Полномочия должны быть минимально достаточными для выполнения лицом своих должностных обязанностей, либо выполнения контрактных обязательств. При необходимости должен осуществляться контроль конфликта полномочий – организационный, а также программно-аппаратный.

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

6. Объекты защиты

В рамках обеспечения информационной безопасности объектами защиты в КГАУ «КДМ» являются информация, обрабатываемая в КГАУ «КДМ», вне зависимости от формы представления; активы КГАУ «КДМ», включающие:

– автоматизированные рабочие места, средства обработки информации и мобильные технические средства;

– ИС, системы хранения данных, программное обеспечение и отдельные технические решения;

– ИТ-инфраструктура, информационно-телекоммуникационные сети и системы связи;

– решения по цифровизации бизнес- и технологических (производственных) процессов.

– Технологическая информация. (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);

– Технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);

– Информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащих защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;

– Информацию о средствах защиты персональных данных, их составе и структуре, принципах и технических решениях защиты;

– Информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;

– Служебные данные (метаданные), появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки Обрабатываемой информации.

– Программно-технические средства обработки (Общесистемное и специальное программное обеспечение, операционные системы, клиент-серверные приложения и другие);

– Резервные копии общесистемного программного обеспечения; инструментальные средства и утилиты систем управления ресурсами Аппаратные средства обработки ПДн (АРМ и сервера);

– Сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.).

7. Роли и обязанности лиц, участвующих в защите информирование

7.1. Защиту информации организует отдел информационных технологий.

7.2. Требуемый уровень информационной безопасности обеспечивается проведением мероприятий всеми лицами, взаимодействующими с информационными активами. Защиту информации для каждого информационного актива обеспечивают:

– специалисты по защите информации;

– сотрудники, использующие информационные активы;

– сотрудники, обеспечивающие эксплуатацию информационных активов.

7.3. Подразделения (работники), использующие информационные активы, должны участвовать в проведении мероприятий и принятии мер по защите информации в объеме, установленном в локальных нормативных актах КГАУ «КДМ».

7.4. Подразделения, обеспечивающие эксплуатацию и развитие информационных активов, должны проводить мероприятия и принимать меры по защите информации в ходе сопровождения, обслуживания, развития информационных активов, поставки комплектующих, отладки информационных активов и иных видов эксплуатационных работ объеме, установленном в локальных нормативных актах КГАУ «КДМ».

7.5. Специалистами по защите информации должны применяться программные, программно-аппаратные средства, обеспечивающие выполнение возложенных на них обязанностей (функций) по защите информации, в том числе

по выявлению угроз безопасности информации, обнаружению и предотвращению вторжений, проведению контроля уровня защищенности информации, содержащейся в информационных системах, мониторингу информационной безопасности информационных систем, выявлению уязвимостей, контролю настроек и конфигураций информационных систем, а также средства и системы, предназначенные для автоматизации и аналитической поддержки деятельности по защите информации.

7.6. По решению Директора КГАУ «КДМ» для проведения мероприятий и принятия мер по защите информации могут привлекаться организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации. Состав проводимых организациями лицензиатами мероприятий и принимаемых ими мер по защите информации, используемых при этом программных, программно-аппаратных средств, предназначенных для защиты информации, определяется в договорах или иных документах, на основании которых такие организации-лицензиаты привлекаются к защите информации.

Специалисты по защите информации должны осуществлять контроль проводимых организациями-лицензиатами мероприятий и принимаемых ими мер по защите информации.

7.7. Специалисты по защите информации должны разрабатывать и представлять Директору КГАУ «КДМ» обоснованные предложения по организационным, материально-техническим и иным обеспечивающим ресурсам, необходимым для проведения мероприятий и принятия мер по защите информации, с указанием сведений о целях защиты информации, на достижение которых требуются ресурсы, и перечня негативных последствий (событий), наступление которых прогнозируется в случае отсутствия ресурсов.

7.8. Директор КГАУ «КДМ» или ответственное лицо на основе представленных предложений и в пределах имеющихся средств предусматривает выделение организационных, материально-технических и иных обеспечивающих ресурсов для проведения мероприятий и принятия мер по защите информации,

привлечения при необходимости дополнительных сил и средств для защиты информации.

8. Техническое обеспечение информационной безопасности

8.1. Система обеспечения безопасности информационных ресурсов должна предусматривать комплекс организационных, технических, программных и криптографических средств и мер по защите информации в процессе документооборота, при работе работников с конфиденциальными документами и сведениями, при обработке информации в автоматизированных системах различного уровня и назначения, при передаче по каналам связи, при ведении конфиденциальных переговоров.

8.2. Предоставление прав доступа работникам КГАУ «КДМ» к соответствующей информации определяется в порядке, определяемом внутренними документами КГАУ «КДМ».

8.3. Одним из направлений обеспечения информационной безопасности является реализация технической политики, то есть защита информационных ресурсов от хищения, утраты, уничтожения, разглашения, утечки, искажения и подделки за счет несанкционированного доступа и иных воздействий.

8.4. В рамках обеспечения информационной безопасности, техническая политика предусматривает:

8.4.1. реализацию единой разрешительной системы допуска работников к работам, документам и информации конфиденциального характера;

8.4.2. ограничение доступа работников и посторонних лиц в здания, помещения, где обрабатывается (хранится) информация конфиденциального характера, в том числе на объекты информатики;

8.4.3. разграничение доступа пользователей к данным автоматизированных систем различного уровня и назначения;

8.4.4. учет документов, информационных массивов, регистрация действий пользователей ИС, контроль за несанкционированным доступом и действиями пользователей;

8.4.5. криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи;

8.4.6. предотвращение внедрения в автоматизированные ИС программ вирусного характера.

8.5. Защита информационных ресурсов от несанкционированного доступа предусматривает:

8.5.1. единую централизованную политику обеспечения безопасности автоматизированных систем, регистрации и проверки прав доступа работников КГАУ «КДМ»;

8.5.2. обоснованность доступа, предполагающую наличие соответствующей формы допуска работника для ознакомления с информацией (документацией) определенного уровня конфиденциальности при необходимости ознакомления с данной информацией или действий с ней для выполнения производственных функций;

8.5.3. персональную ответственность, предполагающую ответственность работника за использование и сохранность доверенной информации (документов, носителей информации, информационных массивов), за свои действия в автоматизированной системе;

8.5.4. надежность хранения, предполагающую хранение информации (документов, носителей информации, информационных массивов) в условиях, исключающих несанкционированное ознакомление, ее уничтожение, подделку или искажение;

8.5.5. централизованный контроль за действиями работников с конфиденциальными документами, а также конфиденциальной информацией в автоматизированных системах;

8.5.6. целостность технической и программной среды, обрабатываемой информации и средств защиты, предполагающую физическую сохранность средств информатизации, неизменность программной среды, определяемую предусмотренной технологией обработки информации, выполнение средствами защиты предусмотренных функций, изолированность средств защиты от пользователей.

8.6. Обеспечение безопасности ИС предполагает разработку необходимых мер защиты на этапе формирования будущей автоматизированной системы, что заключается в составлении спецификаций на приобретаемое оборудование и программное обеспечение с учетом предъявляемых требований по безопасности.

8.7. В процессе формирования заказа на построение ИС необходимо учитывать не только основной набор функциональных сервисов (бухгалтерские системы, системы автоматизации процедур, делопроизводства и тому подобные), но и ряд необходимых вспомогательных сервисов, обеспечивающих надежное функционирование системы и требуемый уровень безопасности. При этом необходимо учитывать, что в защите нуждаются все сервисы и коммуникационные пути между ними. В случае, если не все функционально законченные сервисы обладают полным набором механизмов безопасности, они требуют объединения в составные сервисы, в совокупности, обладающие таким набором и с внешней точки зрения представляющих собой единое целое.

8.8. Обеспечение единой политики процедур регистрации и предоставления доступа, а также требование обоснованности доступа реализуется в рамках разрешительной системы допуска к работам, документам и сведениям, которая предполагает определение для всех пользователей автоматизированных систем доступные им информационные и программные ресурсы, а также конкретные операции (чтение, запись, модификация, удаление, выполнение) с помощью заданных программно-технических средств доступа.

8.9. Условие надежности хранения информации реализуется с помощью:

8.9.1. Оборудования помещений, в которых ведется обработка конфиденциальной информации сейфами и металлическими шкафами для хранения документов, а также техническими средствами разграничения и контроля доступа;

8.9.2. Использования криптографического преобразования информации в автоматизированных системах.

8.10. Система контроля за действиями работников реализуется с помощью:

8.10.1. Организационных мер и технических средств контроля при работе с конфиденциальными документами и сведениями;

8.10.2. Регистрации (протоколирования средствами системного аудита) действий пользователей с информационными и программными ресурсами автоматизированных систем с указанием даты и времени, идентификаторов запрашивающего и запрашиваемых ресурсов, вида взаимодействия и его результата, включая запрещенные попытки доступа;

8.10.3. Сигнализации о несанкционированных действиях пользователей.

8.10.4. Целостность автоматизированных систем достигается комплексом программно-технических средств и организационных мероприятий, осуществляемых ответственными лицами КГАУ «КДМ».

8.10.5. При необходимости передачи по внешним линиям связи конфиденциальной информации, основным направлением защиты информации от перехвата, искажения и навязывания ложной информации является использование криптографического преобразования информации, а на небольших расстояниях, использование защищенных волоконно-оптических линий связи.

8.10.6. Для защиты информации должны использоваться средства криптографической защиты данных гарантированной стойкости для определенного уровня конфиденциальности передаваемой информации и соответствующая ключевая система, обеспечивающая надежный обмен информацией и аутентификацию (подтверждение подлинности) сообщений.

8.10.7. Необходимой составляющей системы безопасности должно быть обеспечение качества работ и используемых средств и мер защиты, нормативной базой которого является система стандартов и других нормативных правовых актов по безопасности, утвержденных органами государственного управления в соответствии с их компетенцией и определяющие нормы защищенности информации и требования в различных направлениях защиты информации.

8.10.8. В целях обеспечения заданного качества функционирования системы информационной безопасности, должно проводиться предпроектное обследование и проектирование ИС, выработка требований по средствам защиты информации и контроля, предполагаемых к использованию в этих системах, а также контроль защищенности информационных ресурсов.

8.10.9. Применение аутентификации в автоматизированных системах обусловлено необходимостью гарантированного сопоставления участников информационного обмена учетным записям в системе в целях предоставления им законно предоставленных прав на реализацию системных процедур. Аутентификация в вычислительных сетях призвана обеспечить заданную степень уверенности получателя в том, что полученная информация была передана отправителем и при этом не была заменена или искажена.

8.10.10. Целью аутентификации является защита участников информационного обмена от стороннего вмешательства путем взаимной идентификации. Важной мерой защиты передаваемых в электронном виде данных, является шифрование.

9. Организационное обеспечение информационной безопасности

9.1. Задачи обеспечения безопасности информационных ресурсов решаются следующими организационными методами:

9.1.1. разработкой и осуществлением разрешительной системы допуска работников к работам с документами и сведениями конфиденциального характера;

9.1.2. установлением единого порядка хранения и обращения конфиденциальной информации (документов, носителей информации);

9.1.3. координацией работ по защите информации, обрабатываемой и передаваемой средствами и системами вычислительной техники и связи.

9.2. В работе с работником КГАУ «КДМ» основными организационными мерами в плане достижения информационной безопасности являются:

9.2.1. заключение трудовых договоров и получение у работников добровольного согласия на соблюдение требований, регламентирующих режим информационной безопасности и сохранность конфиденциальной информации;

9.2.2. проведение первоначального инструктажа, периодического обучения и повышения квалификации работников КГАУ «КДМ» в области информационной безопасности.

9.3. Система распределения обязанностей между отдельными работниками может в значительной мере способствовать повышению общего уровня информационной безопасности. Этого можно достичь следующими методами:

9.3.1. минимизация данных, доступных работникам. Каждый работник должен знать только те детали процедур обработки данных, которые необходимы ему для выполнения своих обязанностей. Организация технологического процесса сбора и обработки информации и планирование помещений должны по мере возможности исключать или сводить к минимуму контакты персонала в процессе выполнения работ. Каждый работник должен знать все о своей работе и связанных с нею ограничениях, а также четко представлять последствия нарушения этих ограничений;

9.3.2. разделение полномочий и дублирование контроля. В системах с высокими требованиями по обеспечению сохранности данных ответственная

работа или процедура (например, изменение статуса электронного документа) выполняется после подтверждения ее необходимости двумя работниками. Временные или вновь принятые работники, а также работники, проходящие обучение, стажировку, практику не должны самостоятельно выполнять ответственные задания.

9.4. Административные меры защиты информации предполагают:

9.4.1. обеспечение физической сохранности автоматизированной системы и дополнительного оборудования;

9.4.2. организацию контроля доступа и режима выполнения работ персоналом подразделения информационных технологий;

9.4.3. инспектирование правильности и полноты выполнения персоналом подразделения информационных технологий мер по обеспечению сохранности необходимых дубликатов файлов, библиотеки программ, оборудования системы;

9.4.4. практическую проверку функционирования отдельных мер защиты: предотвращения недозволенных изменений программ и оборудования, контроль всех процедур, производимых с файлами на носителях и т.д.;

9.4.5. проверку машинных и ручных протоколов выполнения работ со стороны пользователей;

9.4.6. ознакомление работников отдела информационных технологий со всеми новыми разработками по обеспечению сохранности данных.

10. Управление доступом

Владельцы активов, по согласованию с ответственным за защиту информации, определяют соответствующие правила управления доступом, права доступа и ограничения для конкретных ролей работников КГАУ «КДМ» по отношению к своим активам с уровнем детализации и набором мер, отражающих риски, связанные с обеспечением ИБ.

10.1. Как логические, так и физические меры по управлению доступом рассматриваются совместно.

В КГАУ «КДМ» учитываются:

– требования безопасности бизнес-приложений;

– политики распространения информации и авторизации;

– соответствие между правами доступа и политиками категорирования информации для систем и сетей;

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

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

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

– требования к формальной авторизации результатов запросов доступа;

– требования к периодическому пересмотру прав доступа;

– аннулирование прав доступа;

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

В отношении использования сетей и сетевых сервисов учитываются:

– сети и сетевые сервисы, к которым разрешен доступ;

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

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

– требования к Аутентификации и авторизации пользователя для доступа к различным сетевым сервисам;

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

Процесс управления идентификаторами работников КГАУ «КДМ» включает:

– использование уникальных идентификаторов пользователей, позволяющих фиксировать несанкционированные действия пользователей;

– своевременное отключение или удаление идентификаторов уволенных работников;

– выявление и удаление/блокирование избыточных идентификаторов пользователей;

– исключение возможности передачи идентификаторов пользователей другим пользователям и третьим лицам;

– безопасное хранение учетных записей пользователей;

– требования к парольной защите.

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

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

– проверку предоставления уровня доступа соответствующего политикам доступа;

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

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

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

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

При пересмотре прав доступа учитываются:

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

– регулярные проверки назначенных привилегий. Работники осведомлены:

– о необходимости тайного хранения закрытой Аутентификационной информации, исключая ее компрометацию;

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

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

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

– о недопустимости использования идентичного набора символов пароля, используемого для доступа к информационным системам и сервисам КГАУ «КДМ», в частных целях;

– о недопустимости использования корпоративных ресурсов в личных целях.

10.2. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику КГАУ «КДМ», допущенному к работе с ресурсами ИС присваивается уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИС.

10.3. В качестве модели разграничения доступа к ресурсам ИС выбрана ролевая модель. Пользователям назначается роль в разграничительной системе

ИС в зависимости от выполняемых должностных обязанностей и задач и, соответственно, в зависимости от необходимости по доступу к тем или иным ресурсам ИС. Помимо учетных записей Пользователей доступ к системе получают различные системные службы и процессы.

10.4. Идентификация и аутентификация на сетевом оборудовании (коммутаторы, маршрутизаторы, точки доступа и т. д.) разрешена только администраторам безопасности, системным администраторам и сотрудникам сторонней организации, производящим работы в сети КГАУ «КДМ» на договорной основе под контролем Администратора.

10.5. Пользователям запрещены любые действия в ИС до прохождения процедуры идентификации и аутентификации в системе.

11. Ответственность за нарушения в области информационной безопасности

Работники КГАУ «КДМ» должны выполнять требования и правила информационной безопасности при работе с информацией и ИТ-активами КГАУ «КДМ» и его деловых партнёров.

Высокие корпоративные стандарты и правила обеспечения информационной безопасности обязательны для всех без исключения работников КГАУ «КДМ» и должны учитываться во взаимоотношениях с деловыми партнерами.

Руководство КГАУ «КДМ» возлагает ответственность на администратора безопасности и системного администратора за организацию повседневной деятельности и выделение необходимых ресурсов для обеспечения информационной безопасности как неотъемлемой составляющей бизнес- и производственных процессов; за своевременную идентификацию значимых ИТ-активов, назначение ответственных за ИТ-активы и управление доступа к ним; за предъявление установленных требований информационной безопасности

к работникам КГАУ «КДМ» и деловым партнерам, и контроль за их выполнением.

При использовании сети Интернет, при общении в социальных сетях и мессенджерах, использовании электронной почты, других средств телекоммуникаций и мобильных технических средств работникам КГАУ «КДМ» рекомендуется проявлять осмотрительность и сдержанность, чтобы не допускать рисков личной безопасности, а также избегать непреднамеренной утечки рабочей информации.

Каждый работник КГАУ «КДМ» за несоблюдение требований информационной безопасности несет дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

ЛИСТ ОЗНАКОМЛЕНИЯ СОТРУДНИКОВ

С политикой ознакомлен (ы):

№ п/п	Фамилия сотрудника	Дата ознакомления	Роспись в ознакомлении