ДЕПАРТАМЕНТ КУЛЬТУРЫ
ХАНТЫ-МАНСИЙСКОГО АВТОНОМНОГО ОКРУГА – ЮГРЫ

Бюджетное учреждение Ханты-Мансийского автономного округа – Югры
«Музей Природы и Человека»
(БУ «Музей Природы и Человека»)

ПРИКАЗ

23.01.2026
14/01-02

Ханты-Мансийск

Об информационной безопасности в БУ «Музей Природы и Человека»

В целях обеспечения информационной безопасности в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Музей Природы и Человека» (далее – Учреждение), на основании Доктрины информационной безопасности Российской Федерации, утверждённой Указом Президента Российской Федерации от 5 декабря 2016 года № 646, Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», **п р и к а з ы в а ю:**

1. Утвердить:

1.1. Политику информационной безопасности Учреждения (далее – Политика) согласно приложению 1 к настоящему приказу.

1.2. Должностной регламент ответственного за информационную безопасность в Учреждении согласно приложению 2 к настоящему приказу.

1.3. Положение о структурном подразделении, обеспечивающим информационную безопасность Учреждения приложению 3 к настоящему приказу.

2. Назначить заместителя директора по общим вопросам ответственным за информационную безопасность в Учреждении.

3. Закрепить за информационно-аналитической службой функционал по обеспечению информационной безопасности в Учреждении.

4. Кириченко Е.А., специалисту по информационным ресурсам информационно-аналитической службы, разместить электронный экземпляр Политики на официальном сайте Учреждения в сети «Интернет».

5. Пермитиной Д.В., помощнику руководителя 1 категории, довести настоящий приказ до сведения исполнителей.

6. Контроль за исполнением настоящего приказа оставляю за собой.

Директор

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 6F21192A720066E3065CAA8408F17214
Владелец Яшков Иван Александрович
Действителен с 06.06.2025 по 30.08.2026

И.А. Яшков

Приложение 1
к приказу БУ «Музей Природы и Человека»
от 23.01.2026 14/01-02

Политика информационной безопасности бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Музей Природы и Человека» (далее – Политика)

1. Назначение и правовая основа политики информационной безопасности

1.1. Настоящая Политика информационной безопасности бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Музей Природы и Человека» (далее – Учреждение) определяет основные принципы, направления и требования по защите информации, является основой для обеспечения режима информационной безопасности, служит руководством при разработке соответствующих положений, правил, инструкций.

1.2. Настоящая Политика является документом, доступным любому работнику Учреждения и пользователю его ресурсов, и представляет собой официально принятую руководством Учреждения систему взглядов на проблему обеспечения информационной безопасности.

1.3. Руководство Учреждения осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства, а также ожиданий работников Учреждения, посетителей, сдатчиков музейных предметов и других заинтересованных сторон. Обеспечение информационной безопасности – необходимое условие для успешного осуществления деятельности Учреждения. Нарушения в данной области могут привести к серьезным последствиям, включая потерю доверия со стороны работников Учреждения, посетителей, сдатчиков музейных предметов и других заинтересованных сторон.

1.4. Настоящая Политика разработана в соответствии с законодательством Российской Федерации и нормами права в части обеспечения безопасности защищаемой информации, требованиями нормативных актов федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим средствам разведки и технической защиты информации, и основывается, в том числе, на:

- Доктрине информационной безопасности Российской Федерации (Утверждена Указом Президента Российской Федерации от 5 декабря 2016 года № 646);
- Федеральном законе от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральном законе от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

- Федеральном законе от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

- Федеральном законе от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

1.5. Необходимые требования обеспечения информационной безопасности Учреждения должны неукоснительно соблюдаться работниками Учреждения и другими сторонами, как это определяется положениями внутренних нормативных документов Учреждения, а также требованиями договоров и соглашений, стороной которых является Учреждение.

1.6. Настоящая Политика распространяется на процессы Учреждения и обязательна для применения всеми работниками и руководством Учреждения, а также пользователями его информационных ресурсов.

2. Термины и определения

В настоящей Политике использованы термины с соответствующими определениями законодательства Российской Федерации и норм права в части обеспечения информационной безопасности, требованиями нормативных актов федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.

2.1. Информация – сведения (сообщения, данные) независимо от формы их представления.

2.2. Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

2.3. Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

2.4. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.5. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.6. Обработка персональных данных - любое действие (операция)

или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.7. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2.8. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.9. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.10. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.11. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

2.12. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.13. Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

2.14. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.15. Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2.16. Режим обработки персональных данных – организационно-технические мероприятия по защите персональных данных, позволяющие Оператору персональных данных при существующих или возможных обстоятельствах обеспечить целостность, доступность и конфиденциальность персональных данных, избежать неоправданных расходов, и реализующие меры по охране персональных данных, включающие в себя:

- определение перечня персональных данных в соответствии с целями и задачами обработки, требованиями Федерального закона от 27 июля 2006 года № 152 «О персональных данных»;

- ограничение доступа к персональным данным путем установления порядка обращения с ними и контроля за соблюдением такого порядка;

- определение класса информационной системы, в которой осуществляется обработка персональных данных;

- учет лиц, получивших доступ к персональным данным, и (или) лиц, которым такая информация была предоставлена или передана;

- регулирование отношений по использованию персональных данных работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров и соглашений.

2.17. Рисковое событие информационной безопасности – это событие, обусловленное операционным риском, повлекшее или способное повлечь за собой потери Учреждения и произошедшее по причине ошибочности или сбоя процессов Учреждения, действий людей и систем, а также по причине внешних событий.

2.18. Угроза информационной безопасности – операционный риск, влияющий на нарушение одного (или нескольких) свойств информации – целостности, конфиденциальности, доступности.

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

3. Цели и задачи, принципы обеспечения информационной безопасности

3.1. Целями деятельности по обеспечению информационной безопасности Учреждения являются:

- снижение угроз информационной безопасности до приемлемого для Учреждения уровня;

- защита персональных данных, обрабатываемых в информационной системе Учреждения; защита информационной системы от возможного нанесения материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи;

- минимизация уровня рисков.

3.2. Основные задачи деятельности по обеспечению информационной безопасности Учреждения:

- отнесение информации к категории несекретной, ограниченного распространения, коммерческой и другим видам тайн, иной конфиденциальной информации, информации персонального характера подлежащей защите от неправомерного использования;

- прогнозирование и своевременное выявление угроз безопасности информационным ресурсам Учреждения, причин и условий, способствующих нанесению финансового, материального и морального

ущерба, нарушению его нормального функционирования и развития;

- создание условий функционирования Учреждения с наименьшей вероятностью реализации угроз безопасности информационных ресурсов и нанесения ущерба;

- создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявление негативных тенденций в функционировании Учреждения, на основе нормативных, правовых, организационных и технических мер и средств обеспечения безопасности;

- создание условий для максимально возможного предотвращения и локализации ущерба, наносимого неправомерными действиями физических и (или) юридических лиц.

3.3. Построение системы обеспечения безопасности информации Учреждения и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законности – соблюдение законодательства по защите информации, защите персональных данных и законных интересов всех участников информационного обмена;

- системности – подход к вопросам организации информационной безопасности должен быть логическим и последовательным: в первую очередь категорирование обрабатываемой информации, информационной системы, оценка риска информационной безопасности исходя из реальных угроз и уязвимости информационных ресурсов, затем создание комплекса организационных и технических мер и средств защиты, учитывающих специфику Учреждения;

- эффективности – реализуемые в разумно достаточном объеме меры и мероприятия по обеспечению информационной безопасности должны сводить риски к приемлемому уровню, при этом адекватность и эффективность защитных мер должна быть оцениваема на регулярной основе;

- целесообразности – соблюдение соразмерности затрат на обеспечение защиты информации и потенциальных потерь при реализации угроз;

- непрерывности – принцип функционирования системы информационной безопасности, учитывающий, что злоумышленники в любой момент времени ищут возможность обхода защитных мер, прибегая для этого к легальным и нелегальным методам;

- взаимодействии и координации – осуществление мер обеспечения информационной безопасности на основе четкой взаимосвязи структурных подразделений Учреждения, информационных технологий и подразделений- пользователей информационных ресурсов, сторонних специализированных организаций в области защиты информации и обслуживания информационных систем, координации их усилий для достижения поставленных целей, а также взаимодействия с уполномоченными государственными органами. Эксплуатация

технических средств и реализация мер информационной безопасности должны осуществляться подготовленными работниками Учреждения;

- совершенствовании – совершенствование мер и средств защиты информации на основе собственного опыта, появления новых технических средств с учетом изменений в методах и средствах атак информационных ресурсов, нормативно-технических требований, достигнутого отечественного и зарубежного опыта;

- приоритетности – категорирование (ранжирование) информации и всех информационных ресурсов Учреждения по степени важности и оценка реальных, а также потенциальных угроз информационной безопасности;

- информированности и персональной ответственности – пользователи информационных ресурсов должны знать о наличии системы контроля и защиты информации, информационных сервисов индивидуально идентифицирующих и аутентифицирующих пользователей и инициируемые ими процессы;

- обязательность контроля – контроль за деятельностью пользователей, а также мониторинг работы информационной системы должен осуществляться на основе применения средств оперативного контроля и регистрации, охватывать как несанкционированные, так и санкционированные действия.

4. Объекты информационной безопасности

4.1. Основными объектами защиты системы информационной безопасности в Учреждении являются:

- персональные данные, информационные ресурсы обрабатывающие персональные данные, сведения ограниченного распространения, независимо от формы и вида их представления;

- информационные ресурсы, содержащие персональные данные физических лиц;

- работники Учреждения, являющиеся пользователями информационных ресурсов (систем) Учреждения;

- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы;

- программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) информационной системы Учреждения, с помощью которых производится обработка защищаемой информации;

- помещения, предназначенные для обработки персональных данных, сведений конфиденциального (персонального) характера;

- помещения, в которых расположены средства обработки защищаемой информации;

- технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация.

4.2. Подлежащая защите информация может находиться:

- на бумажных носителях;

- в электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники);

- передаваться по телефону, факсу и т.п. в виде электрических сигналов;

- в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров;

- записываться и воспроизводиться с помощью программныхи технических средств (диктофоны, видеомагнитофоны и др.).

4.3. Среда информационного обмена обеспечивается, в том числе, общедоступными информационными ресурсами.

5. Угрозы информационной безопасности

5.1. Под угрозами информационной безопасности понимаются потенциально возможные негативные воздействия на защищаемую информацию, к числу которых относятся:

- несанкционированное распространение (передача) персональных данных;

- утрата сведений, составляющих конфиденциальную информацию, персональные данные Учреждения и иную защищаемую информацию, а также искажение такой информации;

- утечка – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д);

- недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, маршрутизаторов, систем управления баз данных, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств;

- отсутствие планирования и контроля;

- низкая степень надежности программного обеспечения;

- недостаточная осведомленность персонала, низкая квалификация персонала и пользователей в области информационных технологий.

5.2. В результате воздействия указанных угроз могут возникнуть следующие негативные последствия, влияющие на состояние информационной безопасности Учреждения и его нормальное функционирование:

- финансовые потери, связанные с утечкой или разглашением защищаемой информации;

- финансовые потери, связанные с уничтожением и последующим

восстановлением утраченной информации;

- ущерб от дезорганизации деятельности Учреждения и потери, связанные с невозможностью выполнения им своих обязательств;

- моральные потери (ущерб репутации Учреждения).

6. Меры обеспечения информационной безопасности

6.1. Требования об обеспечении информационной безопасности Учреждения и обработке персональных данных обязательны к соблюдению всеми работниками Учреждения и пользователями информационных систем.

6.2. Руководство Учреждения приветствует и поощряет в установленном порядке деятельность работников Учреждения и пользователей информационных систем по обеспечению информационной безопасности.

6.3. Неисполнение или некачественное исполнение работниками Учреждения и пользователей информационных систем обязанностей по обеспечению информационной безопасности и обработке персональных данных может повлечь применение к виновным административных мер воздействия, степень которых определяется установленным в Учреждении порядком либо требованиями действующего законодательства.

6.4. Система обеспечения безопасности информационных ресурсов должна соответствовать экономической целесообразности.

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

6.6. Управление рисками информационной безопасности в Учреждении включает в себя:

- анализ влияния на информационную безопасность Учреждения применяемых в деятельности Учреждения технологий, а также внешних по отношению к Учреждению событий;

- выявление проблем обеспечения информационной безопасности, анализ причин их возникновения и прогнозирование их развития;

- определение моделей угроз, выявление, анализ и оценка значимых для Учреждения угроз информационной безопасности;

- выявление возможных негативных последствий для Учреждения, наступающих в результате проявления рисков информационной безопасности, в том числе связанных с нарушением свойств безопасности информационных активов Учреждения;

- идентификацию и анализ рисковых событий информационной безопасности;

- оценку величины рисков информационной безопасности и выявление рисков, неприемлемых для Учреждения;

- оценку влияния защитных мер на цели основной деятельности Учреждения;

- оценку затрат на реализацию защитных мер.

6.7. Организационные меры обеспечения информационной безопасности включают в себя:

- организацию контроля доступа в здания и помещения Учреждения, предназначенные для обработки сведений конфиденциального и персонального характера;

- разработку и осуществление разрешительной системы допуска работников к работам с документами и персональными данными;

- заключение трудовых договоров и получение у работников добровольного согласия на соблюдение требований, регламентирующих режим информационной безопасности, обработки персональных данных и сохранность конфиденциальной информации (персональных данных);

- установление единого порядка хранения и обращения персональных данных, конфиденциальной информации (носителей информации);

- координацию работ по защите информации, обрабатываемой и передаваемой средствами и системами вычислительной техники и связи;

- проведение периодического обучения и повышения квалификации работников Учреждения в области информационной безопасности;

- минимизацию данных конфиденциального (персонального) характера, доступных работникам;

- обеспечение физической сохранности автоматизированной системы и дополнительного оборудования;

- практическую проверку функционирования мер защиты обработки персональных данных и конфиденциальной информации.

6.8. Технические меры обеспечения информационной безопасности включают в себя:

- обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам информационных систем Учреждения и информации, обрабатываемой в них;

- применение программных, программно-аппаратных средств криптографической защиты информации;

- обеспечение бесперебойной работы информационной системы обработки персональных данных и сети связи;

- обеспечение возобновления работы информационных ресурсов и сети связи после прерываний и нештатных ситуаций;

- применение средств защиты от вредоносных программ;

- применение средств обнаружения вторжений;

- обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты;

- предотвращения несанкционированного изменений программ и

оборудования, контроль всех процедур, производимых с файлами на носителях и т.д.;

- проверку машинных и ручных протоколов выполнения работ со стороны пользователей;

- применение мер и технических средств, снижающих вероятность несанкционированного получения информации в устной форме (пассивная защита).

6.9. Управление инцидентами информационной безопасности в Учреждении включает в себя:

- сбор информации о событиях информационной безопасности;

- выявление и анализ инцидентов информационной безопасности;

- расследование инцидентов информационной безопасности;

- оперативное реагирование на инцидент информационной безопасности;

- минимизация негативных последствий инцидентов информационной безопасности;

- оперативное доведение до руководства Учреждения информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;

- выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки;

- пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности.

7. Структура управления политикой информационной безопасности

7.1. В целях выполнения задач по обеспечению информационной безопасности Учреждения, в Учреждении определены следующие роли:

- Руководитель Учреждения.

- Ответственный за информационную безопасность.

- Ответственный за обеспечение информационной безопасности.

- Администратор информационных систем персональных данных.

- Работники Учреждения.

7.2. При необходимости могут быть определены и другие роли по информационной безопасности.

7.3. Общее руководство обеспечением информационной безопасности Учреждения осуществляет руководитель Учреждения.

7.4. Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы менеджмента информационной безопасности Учреждения лежит на ответственном за информационную безопасность.

7.5. Ответственность работников Учреждения за невыполнение

настоящей Политики определяется законодательством Российской Федерации, а также локальными актами Учреждения.

7.6. Оперативная деятельность и планирование деятельности по обеспечению информационной безопасности Учреждения осуществляются и координируются ответственным за информационную безопасность.

7.7. Задачи ответственного за организацию информационной Учреждения определяются законодательством Российской Федерации и локальными актами Учреждения.

7.8. Руководитель Учреждения может создавать оперативные группы для проведения расследований инцидентов информационной безопасности, возглавляемые ответственным за информационную безопасность, и может, при необходимости привлекать для работы в них ответственных работников Учреждения на основе совмещения работы в группе со своими основными должностными обязанностями.

7.9. Финансирование работ по реализации положений настоящей Политики осуществляется в рамках бюджета Учреждения.

8. Контроль за соблюдением положений Политики

8.1. Общий контроль состояния информационной безопасности Учреждения осуществляется руководителем Учреждения.

8.2. Контроль соблюдения настоящей Политики осуществляет ответственный за организацию обработки персональных данных на основе проведения внутреннего аудита информационной безопасности.

8.3. Контроль осуществляется путем проведения мониторинга и управлением инцидентов информационной безопасности Учреждения, по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий.

9. Заключительные положения

9.1. Требования настоящей Политики могут развиваться другим внутренними нормативными документами Учреждения, которые дополняют и уточняют ее.

9.2. В случае изменения действующего законодательства и иных нормативных актов, а также Устава Учреждения настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Учреждения. В этом случае ответственный за обработку персональных данных обязан незамедлительно инициировать внесение соответствующих изменений.

Приложение 2

к приказу БУ «Музей Природы и Человека»
от 23.01.2026 14/01-02

Должностной регламент ответственного за информационную безопасность в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Музей Природы и Человека»

I. Общие положения

1. Настоящее положение определяет полномочия, права и обязанности заместителя директора бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Музей Природы и Человека» (далее – учреждение), ответственного за обеспечение информационной безопасности в учреждении, в том числе за обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты (далее – ответственное лицо).

2. Ответственное лицо определяется руководителем учреждения.

3. Ответственное лицо осуществляет свою деятельность на основании настоящего Положения.

4. Ответственное лицо входит в состав коллегиальных органов учреждения.

5. Указания и поручения ответственного лица в части обеспечения информационной безопасности являются обязательными для исполнения всеми работниками.

II. Квалификационные требования к ответственному лицу

6. Ответственное лицо должно иметь высшее образование (не ниже уровня специалитета, магистратуры) по направлению обеспечения информационной безопасности. Если ответственное лицо имеет высшее образование по другому направлению подготовки (специальности), он должен пройти обучение по программе профессиональной переподготовки по направлению «Информационная безопасность».

7. Для ответственного лица требуются наличие следующих знаний, умений и профессиональных компетенций:

а) основные (в том числе производственные, бизнес и управленческие) процессы учреждения и специфика обеспечения информационной безопасности учреждения;

б) влияние информационных технологий на деятельность учреждения, в том числе:

роль и место информационных технологий (в том числе степень интеграции информационных технологий) в процессах функционирования учреждения;

зависимость основных процессов функционирования учреждения от

информационных технологий;

в) информационно-телекоммуникационные технологии, в том числе:

современные информационно-телекоммуникационные технологии, используемые в учреждении;

способы построения информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления формирования информационных ресурсов (далее – системы и сети), в том числе ограниченного доступа;

типовые архитектуры систем и сетей, требования к их оснащенности программными (программно-техническими) средствами;

принципы построения и функционирования современных операционных систем, систем управления базами данных, систем и сетей, основных протоколов систем и сетей;

г) обеспечение информационной безопасности, в том числе:

цели, задачи, основы организации, ключевые элементы, основные способы и средства обеспечения информационной безопасности;

цели обеспечения информационной безопасности применительно к основным процессам функционирования учреждения, реализации и контроля их достижения;

принципы и направления стратегического развития информационной безопасности в учреждении;

правила разработки, утверждения и отмены организационно-распорядительных документов по вопросам обеспечения информационной безопасности в учреждении, состав и содержание таких документов;

порядок организации работ по обеспечению информационной безопасности в учреждении;

основные негативные последствия, наступление которых возможно в результате реализации угроз безопасности информации, способы и методы обеспечения и поддержания необходимого уровня (состояния) информационной безопасности учреждения для исключения (невозможности реализации) негативных последствий, а также порядок проведения практических проверок и контроля результативности применяемых способов и методов обеспечения информационной безопасности учреждения;

основные угрозы безопасности информации, предпосылки их возникновения и возможные пути их реализации, а также порядок оценки таких угроз;

возможности и назначения типовых программных, программно-аппаратных (технических) средств обеспечения информационной безопасности;

способы и средства проведения компьютерных атак, актуальные тактики и техники нарушителей;

порядок организации взаимодействия структурных подразделений учреждения при решении вопросов обеспечения информационной

безопасности;

управление проектами по информационной безопасности;

антикризисное управление и принятие управленческих решений при реагировании на кризисы и компьютерные инциденты;

планирование деятельности по обеспечению информационной безопасности в учреждении, филиале;

формулирование измеримых и практических результатов деятельности по обеспечению информационной безопасности учреждения, филиала;

организация разработки политики (правил, процедур), регламентирующей вопросы информационной безопасности в учреждении, филиале;

внедрение политики;

организация контроля и анализа применения политики;

организация мероприятий по разработке единых инструментов и механизмов контроля деятельности по обеспечению информационной безопасности в учреждении, филиале;

поддержка и совершенствование деятельности по обеспечению информационной безопасности в учреждении, филиале;

организация мероприятий по определению угроз безопасности информации систем и сетей, а также по формированию требований к обеспечению информационной безопасности в учреждении;

организация внедрения способов и средств для обеспечения информационной безопасности в учреждении, филиале;

организация мероприятий по анализу и контролю состояния информационной безопасности учреждения и модернизации (трансформации) процессов функционирования учреждения в целях обеспечения информационной безопасности в учреждении;

обеспечение информационной безопасности в ходе эксплуатации систем и сетей, а также при выводе их из эксплуатации;

организация мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы учреждения и реагированию на компьютерные инциденты;

организация мероприятий по отслеживанию и контролю достижения целей информационной безопасности (фактически достигнутый эффект и результат) в учреждении, филиале.

8. От ответственного лица требуется знание:

а) защиты государственной тайны;

б) защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональных данных;

в) обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

г) обнаружения, предупреждения и ликвидации последствий

компьютерных атак и реагирования на компьютерные инциденты;

д) создания и обеспечения безопасного функционирования государственных информационных систем и информационных систем в защищенном исполнении;

е) создания, обеспечения технических условий установки и эксплуатации средств защиты информации;

ж) иных нормативных правовых актов и стандартов в области информационной безопасности.

III. Трудовые (должностные) обязанности ответственного лица

9. Ответственное лицо принимает участие в формировании политики учреждения, отвечает за согласование стратегии развития учреждения в части вопросов обеспечения информационной безопасности.

10. Ответственное лицо:

а) организует разработку политики, направленной в том числе на обеспечение и поддержание стабильной деятельности учреждения и его (ее) процессов функционирования в случае проведения компьютерных атак, отвечает за согласование и утверждение политики в учреждении, реализацию мероприятий, предусмотренных политикой, отслеживает и контролирует результаты реализации политики;

б) организует работу по обеспечению информационной безопасности учреждения, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, формулированию перечня негативных последствий, проведению мероприятий по их недопущению, отслеживанию и контролю эффективности (результативности) таких мероприятий, а также по необходимому информационному обмену;

в) организует реализацию и контроль проведения в учреждении организационных и технических мер, решения о необходимости осуществления которых принимаются Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю с учетом меняющихся угроз в информационной сфере, а также самостоятельно ответственным лицом в результате своей деятельности;

г) организует беспрепятственный доступ (в том числе удаленный) должностным лицам Федеральной службы безопасности Российской Федерации и ее территориальных органов к информационным ресурсам, принадлежащим учреждению либо используемым учреждением, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет», в целях осуществления мониторинга их защищенности, а также работникам структурного подразделения, осуществляющего функции по обеспечению информационной безопасности;

д) организует взаимодействие с должностными лицами Федеральной службы безопасности Российской Федерации и ее территориальных органов, в том числе контроль исполнения указаний, данных Федеральной службой безопасности Российской Федерации и ее территориальными органами по результатам мониторинга защищенности информационных ресурсов, принадлежащих учреждению либо используемых учреждением, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет»;

е) организует контроль за выполнением требований нормативных правовых актов, нормативно-технической документации, за соблюдением установленного порядка выполнения работ при решении вопросов, касающихся защиты информации;

ж) организует развитие информационной безопасности, формирование и развитие навыков работников учреждения в сфере информационной безопасности;

з) организует разработку и реализацию мероприятий по обеспечению информационной безопасности в учреждении в соответствии с требованиями к обеспечению информационной безопасности, установленными федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации;

и) организует контроль пользователей информационных ресурсов учреждения в части соблюдения ими режима конфиденциальности информации, правил работы со съемными машинными носителями информации, выполнения организационных и технических мер по защите информации;

к) организует планирование мероприятий по обеспечению информационной безопасности в учреждении, филиале;

л) организует подготовку правовых актов, иных организационно-распорядительных документов по вопросам обеспечения информационной безопасности в учреждении, осуществляет согласование иных документов учреждения в части обеспечения информационной безопасности;

м) организует проведение научно-исследовательских и опытно-конструкторских работ по вопросам обеспечения информационной безопасности в учреждении, филиале;

н) организует проведение контроля за состоянием обеспечения информационной безопасности в учреждении (филиале), включая оценку защищенности систем и сетей.

11. Ответственное лицо:

а) осуществляет регулярный контроль текущего уровня (состояния) информационной безопасности в учреждении, а также отвечает за реализацию мероприятий, направленных на поддержание и развитие уровня (состояния) информационной безопасности в учреждении, в том числе с учетом появления новых угроз безопасности информации и современных способов и методов проведения компьютерных атак;

б) осуществляет регулярное и своевременное информирование руководства учреждения о компьютерных инцидентах, текущем уровне (состоянии) информационной безопасности в учреждении и результатах практических учений по противодействию компьютерным атакам;

в) осуществляет контроль за ведением организационно-распорядительной документации, статистического учета и отчетности по курируемым разделам работы;

г) осуществляет согласование требований к системам и сетям, оператором которых является Учреждение (филиал), в части обеспечения информационной безопасности;

д) осуществляет руководство структурным подразделением учреждения, обеспечивающим информационную безопасность учреждения.

12. Ответственное лицо:

а) организует и контролирует проведение мероприятий по анализу и оценке состояния информационной безопасности учреждения и контролирует их результаты;

б) организует и контролирует функционирование системы обеспечения информационной безопасности в учреждении, координирует функционирование систем обеспечения информационной безопасности филиала.

в) координирует деятельность иных структурных подразделений учреждения по вопросам обеспечения информационной безопасности.

13. Ответственное лицо согласовывает политику, технические задания и иную основополагающую документацию в сфере информационных технологий, цифровизации и цифровой трансформации учреждения.

14. Ответственное лицо с использованием нормативных правовых документов и методических материалов Федеральной службы безопасности Российской Федерации организует обнаружение, предупреждение и ликвидацию последствий компьютерных атак, реагирование на компьютерные инциденты с информационными ресурсами учреждения.

15. Ответственное лицо обеспечивает планирование и реализацию мероприятий по переводу систем и сетей на отечественные средства защиты информации, а также контроль за соблюдением запрета на использование средств защиты информации, странами происхождения которых являются иностранные государства в соответствии с пунктом 6 Указа Президента Российской Федерации от 1 мая 2022 года № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

16. Ответственное лицо сопровождает мероприятия по разработке (модернизации) систем и сетей в части информационной безопасности, а также требований нормативных правовых актов, нормативно-технических и методических документов по защите информации и выполнения этих требований.

17. Ответственное лицо проводит работу по унификации способов и средств по обеспечению информационной безопасности, иных технических

решений в учреждении (филиале).

18. Ответственное лицо принимает меры по совершенствованию обеспечения информационной безопасности в учреждении (филиале).

19. Ответственное лицо повышает на постоянной основе профессиональную компетенцию, знания и навыки в области обеспечения информационной безопасности.

20. Ответственное лицо выполняет иные обязанности, исходя из возложенных полномочий и поставленных руководством учреждения задач в рамках обеспечения информационной безопасности учреждения (филиала).

21. Ответственное лицо:

а) соблюдает и обеспечивает выполнение законодательства Российской Федерации;

б) представляет по запросам Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю достоверные сведения о результатах реализации политики (фактически достигнутом эффекте и результате) и текущем уровне (состоянии) информационной безопасности в учреждении;

в) поддерживает уровень квалификации и постоянно развивает свои навыки в области информационной безопасности, необходимые для обеспечения информационной безопасности в учреждении;

г) организовывает при необходимости проведение и участвует в пределах своей компетенции в отраслевых, межотраслевых, межрегиональных и международных выставках, семинарах, конференциях, работе межведомственных рабочих групп, отраслевых экспертных сообществ, международных органов и организаций;

д) участвует в пределах компетенции в осуществлении закупок товаров, работ, услуг для обеспечения нужд в сфере информационной безопасности.

IV. Права ответственного лица

22. Ответственное лицо имеет право:

а) давать указания и поручения работникам учреждения в части обеспечения информационной безопасности;

б) запрашивать от работников учреждения информацию и материалы, необходимые для реализации возложенных на ответственное лицо прав и обязанностей;

в) участвовать в заседаниях (совещаниях) коллегиальных органов учреждения, принятии решений по вопросам деятельности учреждения, а также по внесению предложений по совершенствованию деятельности учреждения;

г) участвовать в разработке политики, выносить политику на обсуждение, утверждение коллегиальному органу учреждения;

д) представлять результаты реализации политики коллегиальному органу учреждения;

е) принимать решения по вопросам обеспечения информационной безопасности учреждения;

ж) взаимодействовать с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю и иными федеральными органами исполнительной власти по вопросам обеспечения информационной безопасности, в том числе по вопросам совершенствования законодательства Российской Федерации в области обеспечения информационной безопасности;

з) вносить предложения о привлечении организаций, имеющих соответствующие лицензии на деятельность в области защиты информации, в соответствии с законодательством Российской Федерации к проведению работ по обеспечению информационной безопасности;

и) организовывать на объектах учреждения мероприятия по информационной безопасности, разработку и представление руководителю учреждения предложений по внесению изменений в процессы функционирования, принятию других мер, направленных на недопущение реализации негативных последствий;

к) обеспечивать надлежащие организационно-технические условия, необходимые для исполнения обязанностей ответственного лица.

V. Ответственность ответственного лица

23. Ответственное лицо в соответствии с законодательством Российской Федерации несет ответственность:

а) за неисполнение или ненадлежащее исполнение своих обязанностей;

б) за действия (бездействие), ведущие к нарушению прав и законных интересов учреждения;

в) за разглашение государственной тайны и иных сведений, ставших ему известными в связи с исполнением своих обязанностей;

г) за достижение целей обеспечения информационной безопасности;

д) за поддержание и непрерывное развитие информационной безопасности учреждения для исключения (невозможности реализации) негативных последствий;

е) за организацию мероприятий по разработке (модернизации) систем и сетей в части информационной безопасности учреждения;

ж) за нарушения требований по обеспечению информационной безопасности;

з) за нарушения в обеспечении защиты систем и сетей, повлекшие негативные последствия.

Приложение 3

к приказу БУ «Музей Природы и Человека»
от 23.01.2026 14/01-02

Положение
о структурном подразделении учреждения, обеспечивающем информационную безопасность в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Музей Природы и Человека»

I. Общие положения

1. Настоящее типовое положение определяет цели, задачи и функции структурного подразделения бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Музей Природы и Человека» (далее – учреждение), обеспечивающего информационную безопасность учреждения (далее – подразделение).

2. Подразделение в своей деятельности руководствуется Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации, международными договорами Российской Федерации, нормативными правовыми актами федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности, другими нормативными правовыми документами в сфере обеспечения информационной безопасности, указаниями руководителя учреждения и настоящим типовым положением.

3. Подразделение подчинено заместителю руководителя учреждения, ответственному за обеспечение информационной безопасности в учреждении, либо иным лицам из состава руководства учреждения при условии осуществления курирования со стороны руководителя учреждения.

4. Контроль за деятельностью подразделения осуществляет руководитель учреждения.

II. Цели и задачи деятельности подразделения

5. Деятельность подразделения направлена:

а) на исключение или существенное снижение негативных последствий (ущерба) в отношении учреждения вследствие нарушения функционирования информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления в результате реализации угроз безопасности информации;

б) на обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации;

в) на повышение защищенности учреждения от возможного нанесения ему (ей) материального, репутационного или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем учреждения или несанкционированного доступа к циркулирующей в них информации и ее несанкционированного использования;

г) на обеспечение надежности и эффективности функционирования и безопасности информационных систем, производственных процессов и информационно-технологической инфраструктуры учреждения;

д) на обеспечение выполнения требований по информационной безопасности при создании и функционировании информационных систем и информационно-телекоммуникационной инфраструктуры учреждения.

6. Основными задачами деятельности подразделения являются:

а) планирование, организация и координация работ по обеспечению информационной безопасности и контроль за ее состоянием в учреждении;

б) выявление угроз безопасности информации и уязвимостей информационных систем, программного обеспечения и программно-аппаратных средств;

в) предотвращение утечки информации по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;

г) поддержание стабильной деятельности учреждения и его (ее) производственных процессов в случае проведения компьютерных атак;

д) обеспечение нормативно-правового обеспечения использования информационных ресурсов.

III. Функции подразделения

7. Подразделение выполняет следующие функции:

а) разработка, координация, управление и контроль за реализацией плана (программы) работ по обеспечению информационной безопасности в учреждении, филиале;

б) разработка предложений по совершенствованию организационно-распорядительных документов по обеспечению информационной безопасности в учреждении и представление их руководителю учреждения;

в) выявление и проведение анализа угроз безопасности информации в отношении учреждения, уязвимостей информационных систем, программного обеспечения программно-аппаратных средств и принятие мер по их устранению;

г) обеспечение в соответствии с требованиями по информационной безопасности, в том числе с целью исключения (невозможности реализации) негативных последствий, разработки и реализации организационных мер и применения средств обеспечения информационной безопасности;

д) обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты;

е) исполнение указаний, данных Федеральной службой безопасности Российской Федерации и ее территориальными органами, Федеральной службой по техническому и экспортному контролю по результатам мониторинга защищенности информационных ресурсов, принадлежащих учреждению либо используемых учреждением, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет»;

ж) проведение анализа и контроля за состоянием защищенности систем и сетей и разработка предложений по модернизации (трансформации) основных процессов учреждения в целях обеспечения информационной безопасности в учреждении;

з) подготовка отчетов о состоянии работ по обеспечению информационной безопасности в учреждении;

и) организация развития навыков безопасного поведения в учреждении, в том числе проведение занятий с руководящим составом и специалистами учреждения по вопросам обеспечения информационной безопасности;

к) выполнение иных функций, исходя из поставленных руководством учреждения целей и задач в рамках обеспечения информационной безопасности в учреждении, филиале.

IV. Права подразделения

8. С целью реализации функций подразделение имеет право:

а) запрашивать и получать в установленном порядке доступ к работам и документам структурных подразделений учреждения, необходимым для принятия решений по всем вопросам, отнесенным к компетенции подразделения;

б) готовить предложения о привлечении к проведению работ по обеспечению информационной безопасности организаций, имеющих лицензии на соответствующий вид деятельности;

в) контролировать деятельность любого структурного подразделения учреждения по выполнению требований к обеспечению информационной безопасности;

г) постоянно повышать профессиональные компетенции, знания и навыки работников в области обеспечения информационной безопасности;

д) участвовать в пределах своей компетенции в отраслевых, межотраслевых, межрегиональных и международных выставках, семинарах, конференциях, в работе межведомственных рабочих групп, отраслевых экспертных сообществ, международных органов и организаций;

е) участвовать в работе комиссий учреждения при рассмотрении вопросов обеспечения информационной безопасности;

ж) вносить предложения руководству учреждения о приостановлении работ в случае обнаружения факта нарушения информационной безопасности;

з) вносить представления руководству учреждения в отношении работников учреждения (далее – работники) при обнаружении фактов нарушения работниками установленных требований безопасности информации в учреждении, в том числе ходатайствовать о привлечении указанных работников к административной или уголовной ответственности;

и) вносить на рассмотрение руководству учреждения предложения по вопросам деятельности подразделения.

V. Взаимоотношения и связи подразделения

9. Подразделение осуществляет свои полномочия во взаимодействии со структурными подразделениями учреждения, а также в пределах своей компетенции с иными органами (организациями) и гражданами в установленном порядке.

10. По указанию руководства осуществляет взаимодействие с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю по вопросам информационной безопасности.

VI. Показатели эффективности и результативности подразделения

11. Эффективность и результативность деятельности подразделения определяются по итогам выполнения учреждением программы обеспечения информационной безопасности с учетом приоритетных целей, предусмотренных разделом II настоящего положения.

12. Работники подразделения несут ответственность за выполнение возложенных на них обязанностей в соответствии с должностными регламентами, утверждаемыми руководителем учреждения либо должностным лицом, наделенным руководителем учреждения соответствующими полномочиями.