Приложение 1

к приказу № 57р

от 11.07.2024

ПОЛИТИКА

информационной безопасности комитета по земельным ресурсам и землеустройству города Барнаула

1. Перечень используемых определений, обозначений и сокращений

АИБ – Администратор информационной безопасности.

АРМ – Автоматизированное рабочее место.

АС – Автоматизированная система.

ИБ – Информационная безопасность.

ИР – Информационные ресурсы.

ИС – Информационная система.

МЭ – Межсетевой экран.

НСД – Несанкционированный доступ.

ОС – Операционная система.

ПБ – Политики безопасности.

ПДн – Персональные данные.

ПО – Программное обеспечение.

СЗИ – Средство защиты информации.

ЭВМ – Электронная – вычислительная машина, персональный компьютер.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Администратор информационной безопасности – специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в ЛВС, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Доступ к информации – возможность получения информации и ее использования.

Идентификация – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация – это актив, который, подобно другим активам, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Информационная безопасность – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов.

Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач подразделений комитета по земельным ресурсам и землеустройству города Барнаула.

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

Информационные ресурсы – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.

Источник угрозы – намерение или метод, нацеленный на умышленное использование уязвимости, либо ситуация или метод, которые могут случайно проявить уязвимость.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность – доступ к информации только авторизованных пользователей.

Критичная информация – информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование подразделений комитета по земельным ресурсам и землеустройству города Барнаула или иного вида ущерба.

Локальная вычислительная сеть – группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

Межсетевой экран – программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав сети, а также между сетью комитета по земельным ресурсам и землеустройству города Барнаула и внешними сетями (сетью Интернет).

Несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Политика информационной безопасности – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в комитете по земельным ресурсам и землеустройству города Барнаула для обеспечения его информационной безопасности.

Пользователь локальной вычислительной сети – сотрудник организации (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в сети в установленном порядке и получивший права на доступ к ресурсам сети в соответствии со своими функциональными обязанностями.

Программное обеспечение – совокупность прикладных программ, установленных на сервере или ЭВМ.

Рабочая станция – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

Регистрационная (учетная) запись пользователя – включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название подразделения, телефоны, E-mail и т.п.

Роль – совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.

Ответственный за техническое обеспечение – сотрудник организации, занимающийся сопровождением автоматизированных систем, отвечающий за функционирование локальной сети комитета по земельным ресурсам и землеустройству города Барнаула и ПК.

Угрозы информации – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т.е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

Уязвимость – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности при реализации угроз в информационной сфере.

Целостность информации – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

2. Вводные положения

2.1. Введение

Политика ИБ комитета по земельным ресурсам и землеустройству города Барнаула (далее – комитет по земельным ресурсам и землеустройству города Барнаула) определяет цели и задачи системы обеспечения ИБ и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется комитет по земельным ресурсам и землеустройству города Барнаула в своей деятельности.

2.2. Цели

Основными целями политики ИБ являются защита информации комитета по земельным ресурсам и землеустройству города Барнаула от возможного нанесения материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в Положении о деятельности комитета по земельным ресурсам и землеустройству города Барнаула.

Общее руководство обеспечением ИБ осуществляется председателя комитета по земельным ресурсам и землеустройству города Барнаула. Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет АИБ. Ответственность за функционирование информационных систем комитета по земельным ресурсам и землеустройству города Барнаула несет администратор информационной системы.

Должностные обязанности АИБа и системного администратора закрепляются в соответствующих инструкциях.

Руководители структурных подразделений комитета по земельным ресурсам и землеустройству города Барнаула ответственны за обеспечение выполнения требований ИБ в своих подразделениях.

Сотрудники комитета по земельным ресурсам и землеустройству города Барнаула обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других документов внутренних документов комитета по земельным ресурсам и землеустройству города Барнаула по вопросам обеспечения ИБ.

2.3. Задачи

Политика ИБ направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Наибольшими возможностями для нанесения ущерба комитету по земельным ресурсам и землеустройству города Барнаула обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне комитета по земельным ресурсам и землеустройству города Барнаула), либо иметь непреднамеренный ошибочный характер. Категории нарушителей и их возможности определяются в «Модели нарушителя».

На основе вероятностной оценки определяется перечень актуальных угроз безопасности, который отражается в «Модели угроз».

Для противодействия угрозам ИБ в комитете по земельным ресурсам и землеустройству города Барнаула на основе имеющегося опыта составляется прогностическая модель предполагаемых угроз и модель нарушителя. Чем точнее сделан прогноз (составлены модель угроз и модель нарушителя), тем ниже риски нарушения ИБ при минимальных ресурсных затратах.

Разработанная на основе прогноза политика ИБ и в соответствии с ней построенная СУИБ является наиболее правильным и эффективным способом добиться минимизации рисков нарушения ИБ для комитета по земельным ресурсам и землеустройству Барнаула. Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

Стратегия обеспечения ИБ заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала.

Задачами настоящей политики являются:

 описание организации СУИБ;

 определение Политик ИБ, а именно: политика реализации антивирусной защиты; политика учетных записей; политика предоставления доступа к ИР; политика использования паролей; политика защиты АРМ; политика конфиденциального делопроизводства;

 определение порядка сопровождения ИС комитета по земельным ресурсам и землеустройству города Барнаула.

2.4. Область действия

Настоящая Политика распространяется на все структурные подразделения комитета по земельным ресурсам и землеустройству города Барнаула и обязательна для исполнения всеми его сотрудниками и должностными лицами. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

2.5. Период действия и порядок внесения изменений

Настоящая Политика вводится в действие Приказом председателя комитета по земельным ресурсам и землеустройству города Барнаула.

Политика признается утратившей силу на основании Приказа председателя комитета по земельным ресурсам и землеустройству города Барнаула.

Изменения в политику вносятся Приказом председателя комитета по земельным ресурсам и землеустройству города Барнаула.

Инициаторами внесения изменений в политику информационной безопасности являются:

 председатель комитета по земельным ресурсам и землеустройству города Барнаула;

 руководители отделов комитета по земельным ресурсам и землеустройству города Барнаула;

 администратор информационной безопасности.

Плановая актуализация настоящей политики производится ежегодно и имеет целью приведение в соответствие определенных политикой защитных мер реальным условиям и текущим требованиям к защите информации.

Внеплановая актуализация политики ИБ и производится в обязательном порядке в следующих случаях:

 при изменении политики Российской Федерации в области ИБ, указов и законов Российской Федерации в области защиты информации;

 при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся ИБ комитета по земельным ресурсам и землеустройству города Барнаула;

 при происшествии и выявлении инцидента (инцидентов) по нарушению ИБ, влекущего ущерб комитету по земельным ресурсам и землеустройству города Барнаула.

Ответственными за актуализацию политики ИБ (плановую и внеплановую) несет АИБ.

Контроль за исполнением требований настоящей политики и поддержанием ее в актуальном состоянии возлагается на АИБа.

3. Политики информационной безопасности комитета по земельным ресурсам и землеустройству города Барнаула

3.1. Назначение политик информационной безопасности

Политики ИБ комитета по земельным ресурсам и землеустройству города Барнаула – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в комитете по земельным ресурсам и землеустройству города Барнаула.

Политики ИБ относятся к административным мерам обеспечения ИБ и определяют стратегию комитета по земельным ресурсам и землеустройству города Барнаула в области ИБ.

Политики ИБ регламентируют эффективную работу СЗИ. Они охватывают все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях. Политики ИБ реализуются посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Все документально оформленные решения, формирующие Политики, должны быть утверждены комитета по земельным ресурсам и землеустройству города Барнаула.

3.2. Основные принципы обеспечения информационной безопасности

Основными принципами обеспечения ИБ являются следующие:

 постоянный и всесторонний анализ информационного пространства комитета по земельным ресурсам и землеустройству города Барнаула с целью выявления уязвимостей информационных активов;

 своевременное обнаружение проблем, потенциально способных повлиять на ИБ комитета по земельным ресурсам и землеустройству города Барнаула, корректировка моделей угроз и нарушителя;

 разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей комитета по земельным ресурсам и землеустройству города Барнаула, а также повышать трудоемкость технологических процессов обработки информации;

 контроль эффективности принимаемых защитных мер;

 персонификация и адекватное разделение ролей и ответственности между сотрудниками комитета по земельным ресурсам и землеустройству города Барнаула, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

3.3. Соответствие Политики безопасности действующему законодательству

Правовую основу политик составляют законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, сотрудников и государства в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.

3.4. Ответственность за реализацию политик информационной безопасности

Ответственность за разработку мер и контроль обеспечения защиты информации несёт АИБ.

Ответственность за реализацию политик возлагается:

 в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты – на АИБа;

 в части, касающейся доведения правил политик до сотрудников комитета по земельным ресурсам и землеустройству города Барнаула, а также иных лиц (см. область действия настоящей политики) – на АИБа;

 в части, касающейся исполнения правил политики, – на каждого сотрудника комитета по земельным ресурсам и землеустройству города Барнаула, согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей политики.

3.5. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе

Организация обучения сотрудников комитета по земельным ресурсам и землеустройству города Барнаула в области ИБ возлагается на АИБа. Обучение проводится согласно Плану, утвержденному председателя комитета по земельным ресурсам и землеустройству города Барнаула.

Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по информационной безопасности».

Допуск персонала к работе с защищаемыми ИР комитета по земельным ресурсам и землеустройству города Барнаула осуществляется только после его ознакомления с настоящими политиками, а также после ознакомления пользователей с «Порядком работы пользователей» комитета по земельным ресурсам и землеустройству города Барнаула, а так же иными инструкциями пользователей отдельных ИС. Согласие на соблюдение правил и требований настоящих политик подтверждается подписями сотрудников в «Журнале проведения инструктажа по информационной безопасности».

Допуск персонала к работе с КИ комитета по земельным ресурсам и землеустройству города Барнаула осуществляется после ознакомления с «Порядок организации работы с материальными носителями защищаемых информационных ресурсов», «Порядок организации работы с электронными носителями конфиденциальной информации». Правила допуска к работе с ИР лиц, не являющихся сотрудниками комитета по земельным ресурсам и землеустройству города Барнаула, определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

3.6. Защищаемые информационные ресурсы комитета по земельным ресурсам и землеустройству города Барнаула

Защищаемые информационные ресурсы определяются в соответствии с «Перечнем защищаемых ресурсов», утверждаемым соответствующим Приказом комитета по земельным ресурсам и землеустройству города Барнаула.

4. Политики информационной безопасности

4.1. Политика предоставления доступа к информационному ресурсу

4.1.1. Назначение

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к защищаемым ИР комитета по земельным ресурсам и землеустройству города Барнаула.

4.1.2. Положение политики

Положения данной политики определены в «Положении о разрешительной системе допуска», утверждаемом соответствующим Приказом комитета по земельным ресурсам и землеустройству города Барнаула.

4.2. Политика учетных записей

4.2.1. Назначение

Настоящая политика определяет основные правила присвоения учетных записей пользователям информационных активов комитета по земельным ресурсам и землеустройству города Барнаула.

4.2.2. Положение политики

Регистрационные учетные записи подразделяются на:

 пользовательские – предназначенные для идентификации/аутентификации пользователей информационных активов комитета по земельным ресурсам и землеустройству города Барнаула;

 системные – используемые для нужд операционной системы;

 служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений.

Каждому пользователю информационных активов комитета по земельным ресурсам и землеустройству города Барнаула назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

В общем случае запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или организации труда (например, посменное дежурство), использование общей учетной записи должно сопровождаться отметкой в журнале учета машинного времени, которая должна однозначно идентифицировать текущего владельца учетной записи в каждый момент времени. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.

Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.

Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.

Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.

Настоящая Политика определяет основные правила парольной защиты в комитете по земельным ресурсам и землеустройству города Барнаула.

Положения политики закрепляются в «Порядке по организации парольной защиты».

4.3. Политика реализации антивирусной защиты

4.3.1. Назначение

Настоящая Политика определяет основные правила для реализации антивирусной защиты в комитете по земельным ресурсам и землеустройству города Барнаула.

Положения политики закрепляются в «Порядке по проведению антивирусного контроля».

4.4. Политика защиты автоматизированного рабочего места

4.4.1. Назначение

Настоящая Политика определяет основные правила и требования по защите автоматизированных рабочих мест комитета по земельным ресурсам и землеустройству города Барнаула.

4.5. Политика использования паролей

4.5.1. Назначение

Настоящая Политика определяет основные правила и требования по защите информации комитета по земельным ресурсам и землеустройству города Барнаула от неавторизованного доступа, утраты или модификации.

4.5.2. Положения политики

Положения данной политики определяются в соответствии с используемым техническим решением.

5. Профилактика нарушений политик информационной безопасности

Под профилактикой нарушений политик ИБ понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений ИБ в комитете по земельным ресурсам и землеустройству города Барнаула и проведение разъяснительной работы по ИБ среди пользователей.

Положения определены документами, утвержденными Приказом «Об обучении сотрудников правилам защиты информации», и «Порядком технического обслуживания средств вычислительной техники».

5.1. Ликвидация последствий нарушения политик информационной безопасности

АИБ, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС, должен своевременно обнаруживать нарушения ИБ, факты осуществления НСД к защищаемым ИР и предпринимать меры по их локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения ИБ или осуществления НСД к защищаемым ИР ИС рекомендуется уведомить АИБа, и далее следовать их указаниям.

Действия АИБа и администратора информационной системы при признаках нарушения политик информационной безопасности регламентируются следующими внутренними документами:

 регламентом пользователя;

 политикой информационной безопасности;

 регламентом администратора информационной безопасности;

 регламентом системного администратора.

После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС, а также зарегистрировать факт нарушения в карточку данных об инциденте информационной безопасности.

5.2. Ответственность за нарушение Политик безопасности

Ответственность за выполнение правил ПБ несет каждый сотрудник комитета по земельным ресурсам и землеустройству города Барнаула в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса Российской Федерации сотрудники, нарушающие требования ПБ комитета по земельным ресурсам и землеустройству города Барнаула, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный комитету по земельным ресурсам и землеустройству города Барнаула в результате нарушения ими правил политики ИБ (Ст. 238 Трудового кодекса Российской Федерации).

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

|  |
| --- |
| Приложение 5 |
| к приказу №57р |
| от 11.07.2024 |

РЕГЛАМЕНТ  
резервного копирования информации в Комитета

1. ‍Перечень используемых определений, обозначений и сокращений

* АИБ – администратор информационной безопасности.
* ИБ – информационная безопасность.
* НСД – несанкционированный доступ.
* ОС – операционная система.
* ПО – программное обеспечение.
* СУБД – система управления базами данных.
* Администратор информационной безопасности – специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в ИС, в том числе ИСПДн, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

1. ‍Общие положения
   1. ‍Настоящий Регламент проведения резервного копирования (восстановления) программ и данных, хранящихся на серверах и рабочих станциях, обрабатывающих КИ, в том числе ПДн, Комитете по земельным ресурсам и землеустройству города Барнаула (далее – Комитет по земельным ресурсам и землеустройству города Барнаула) разработан с целью:
      1. ‍определения порядка резервирования данных для последующего восстановления работоспособности ИСПДн при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения (ПО), ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т. д.);
      2. ‍определения порядка восстановления информации в случае возникновения такой необходимости;
      3. ‍упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации.
   2. ‍В настоящем документе регламентируются действия при выполнении следующих мероприятий:
      1. ‍резервное копирование;
      2. ‍контроль резервного копирования;
      3. ‍хранение резервных копий;
      4. ‍полное или частичное восстановление данных и приложений.
   3. ‍Резервному копированию подлежит информация следующих основных категорий:
      1. ‍персональная информация пользователей (личные каталоги на файловых серверах);
      2. ‍групповая информация пользователей (общие каталоги отделов);
      3. ‍информация, необходимая для восстановления серверов и систем управления базами данных (СУБД);
      4. ‍персональные профили пользователей сети;
      5. ‍информация, обрабатываемая в ИСПДн;
      6. ‍справочно-информационная информация систем общего использования («Гарант», «Консультант+» и т. п.);
      7. ‍рабочие копии установочных компонентов ПО рабочих станций.
2. ‍Порядок резервного копирования
   1. ‍Резервное копирование производится на основании следующих данных:
      1. ‍состав и объем копируемых данных, периодичность проведения резервного копирования (из Перечня резервируемых данных);
      2. ‍максимальный срок хранения резервных копий – 3 месяца;
      3. ‍хранение 3-х следующих архивов:
      4. ‍архив на 5-е и 20-е число текущего месяца;
      5. ‍архив среда-четверг текущей недели;
      6. ‍архив, сделанный в текущую ночь.
   2. ‍Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, указанной в Перечне резервируемой информации, в установленные сроки и с заданной периодичностью.
   3. ‍О выявленных попытках НСД к резервируемой информации, а также иных нарушениях ИБ, произошедших в процессе резервного копирования, ответственный сотрудник сообщает АИБу.
3. ‍Методика резервного копирования
   1. ‍Для организации системы резервного копирования используются штатные средства ОС и используемого ПО. С целью оптимизации расходов на развёртывание системы резервного копирования, запись резервной копии осуществляется на специальный внешний носитель.
   2. ‍С помощью указанного ПО выполняются такие действия, как задание режимов и составление расписания резервного копирования клиентов, проводится контроль за состоянием выполнения заданий, запускаются процедуры восстановления информации.
   3. ‍Для снижения совокупной нагрузки на информационную систему все операции по резервированию информации проводятся в ночное время. Существуют три набора резервных копий:
      1. ‍Месячный набор. Записывается информация (Образ-файл, содержащий в себе полную копию содержания и структуры) на первые числа текущего месяца. Срок хранения – 3 месяца. Хранится на внешнем жёстком диске.
      2. ‍Двухнедельная копия. Записывается данные за две недели. Срок хранения – 1 месяц. Хранится на внешнем жёстком диске.
      3. ‍Ежедневная копия. Записывается ежесуточно. Срок хранения – 1 месяц. Записывается на внешнем жёстком диске.
   4. ‍Различаются три принципиально разных источника информации, подлежащей резервированию:
      1. ‍формация, хранимая непосредственно на файловом сервере;
      2. ‍базы данных Прикладной информационной системы;
      3. ‍системные файлы серверов (Образ).
   5. ‍Для резервирования информации, хранимой непосредственно в файловых системах и информации, хранимой в базах данных Прикладных информационных систем, используется штатные средства ПО, посредством которой формируются задания на проведение резервного копирования информации, находящейся в каталогах файлового сервера. При этом указывается срок хранения информации и периодичность выполнения резервного копирования.
   6. ‍При создании задания на создание образа системных дисков серверов указывается срок хранения информации и периодичность выполнения резервного копирования.
4. ‍Контроль результатов резервного копирования
   1. ‍Контроль результатов всех процедур резервного копирования осуществляется ответственными должностными лицами, в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур. В случае обнаружения ошибки ответственной лицо сообщает АИБу до 17 часов текущего рабочего дня. На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для её хранения.
5. ‍Ротация носителей резервной копии
   1. ‍Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации в случае отказа любого из устройств резервного копирования.
   2. ‍В случае необходимости замены испорченных носителей информации новыми ответственный сотрудник заблаговременно за 10 рабочих дней согласовывает с АИБом спецификации новых носителей информации. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования, а также перемещение их, осуществляются ответственным сотрудником в присутствии АИБа.
   3. ‍В качестве новых носителей информации допускается повторное использование тех, у которых срок хранения содержащейся информации истек.
   4. ‍Персональные данные с носителей, которые перестают использоваться в системе резервного копирования, должна стираться с составлением Акта.
6. ‍Восстановление информации из резервных копий
   1. ‍В случае необходимости восстановление данных из резервных копий производится на основании Заявки владельца информации на имя ответственного сотрудника.
   2. ‍После поступления заявки восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

|  |
| --- |
| Приложение 16 |
| к приказу № 57р |
| от 11.07.2024 |

**ПОЛОЖЕНИЕ**

**о конфиденциальной информации Комитета**

1. ‍Перечень используемых определений, обозначений и сокращений

* КИ – конфиденциальная информация.
* НСД – несанкционированный доступ.
* Допуск к конфиденциальной информации – процедура оформления права работника Комитета для ознакомления со сведениями, относящимися к конфиденциальным.
* Доступ к конфиденциальной информации – ознакомление определенных лиц с КИ с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.
* Защита конфиденциальной информации – деятельность, направленная на предотвращение НСД к КИ и (или) её утечки.
* Информация – сведения (сообщения, данные) независимо от формы их представления.
* Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.
* Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
* Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.
* Контрагент – сторона гражданско-правового договора, которой обладатель КИ передал эту информацию.
* Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.
* Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.
* Обладатель конфиденциальной информации – лицо (физическое или юридическое), которое владеет сведениями, отнесенным к конфиденциальным, на законном основании, ограничило доступ к ним и установило в отношении ее режим конфиденциальности.
* Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных. Общедоступная информация – общеизвестные сведения и иная информация, доступ к которой не ограничен.
* Передача конфиденциальной информации – передача сведений, отнесенных к конфиденциальным, и зафиксированных на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.
* Предоставление конфиденциальной информации – передача сведений, отнесенных к конфиденциальным, и зафиксированных на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.
* Разглашение конфиденциальной информации – действие или бездействие, в результате которых сведения, отнесенные к конфиденциальным, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.
* Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.
* Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

2.‍Общие положения

2.1.‍Настоящее Положение о конфиденциальной информации (далее по тексту – Положение) устанавливает общие нормы о сведениях, относящихся к категории конфиденциальных, порядок их защиты, определяет единый для всех работников Комитета по земельным ресурсам и землеустройству города Барнаула(далее – Комитет по земельным ресурсам и землеустройству города Барнаула) порядок работы со сведениями, конфиденциального характера, порядок допуска к этим сведениям, а также меры ответственности, применяемые за нарушение требований, установленных настоящим Положением.

2.2.‍Настоящее Положение разработано на основе действующего законодательства Российской Федерации, в том числе Гражданского, Трудового и Уголовного кодексов Российской Федерации и Федерального закона Российской Федерации № 149 от 27.07.2006 «Об информации, информационных технологиях и о защите информации», а также Указа Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» и других законодательных и нормативно-правовых актов, регулирующих вопросы охраны конфиденциальной информации.

2.3.‍Положение распространяется на сведения конфиденциального характера Комитета независимо от вида носителя, на котором они зафиксированы.

2.4.‍Действие настоящего Положения распространяется на работников Комитета, работающих по служебному контракту (трудовому договору), заключенному с Комитетом, которые дали обязательство о неразглашении конфиденциальной информации, а также на лиц, работающих по гражданско-правовым договорам, заключенным с Комитетом, взявших на себя обязательство о неразглашении конфиденциальной информации), в порядке и на условиях, предусмотренных настоящим Положением.

3.‍Сведения, относимые к конфиденциальным

3.1.‍Сведения, относящиеся к конфиденциальной информации, определяются в «Перечне сведений конфиденциального характера», который утверждается Председателем комитета Комитета, принципы отнесения сведений к конфиденциальным определяются в «Инструкции о порядке организации и проведения работ по защите информации в информационных системах Комитета.

4.‍Порядок отнесения сведений к категории конфиденциальных

4.1.‍Порядок отнесения сведений к категории конфиденциальных определен в «Инструкции о порядке организации и проведения работ по защите информации в информационных системах Комитета.

5.‍Порядок оформления допуска к сведениям конфиденциального характера

5.1.‍Порядок оформления допуска к сведениям конфиденциального характера определен в «Положении о порядке организации и проведения работ по защите информации в информационных системах Комитета.

6.‍Меры по защите конфиденциальной информации

6.1.‍Меры по защите сведений конфиденциального характера определены в «Инструкции о порядке организации и проведения работ по защите информации в информационных системах Комитета.

6.2.‍Требования к обеспечению рабочих мест пользователей и порядок работы пользователей определены в приложениях к «Инструкции по организации и проведения работ по защите информации в информационных системах Комитета.

7.‍Ответственность за нарушение конфиденциальности информации

7.1.‍В случае разглашения сведений конфиденциального характера, ставших известными работнику в связи с исполнением им трудовых обязанностей, трудовой договор с работником может быть расторгнут по инициативе работодателя в соответствие с трудовым законодательством.

7.2.‍Собирание сведений, составляющих конфиденциальную информацию, путем похищения документов, подкупа или угроз, а равно иным незаконным способом влечет уголовную ответственность в соответствие с законом.

7.3.‍Разглашение конфиденциальной информации (за исключением случаев, когда разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, влечет дисциплинарную и (или) материальную ответственность.

7.4.‍Возмещение ущерба, причиненного Комитета в связи с нарушением прав Комитета на его конфиденциальную информацию, производится в установленном законом порядке, организациями и лицами (в том числе работниками Комитета), нарушившими действующее законодательство и указанные права.

7.5.‍Ответственность в соответствии с действующим законодательством несут также работники и должностные лица Комитета, не выполнившие или не обеспечившие выполнение требований настоящего положения и тем самым способствовавшие нарушению, а также не принимавшие необходимых и достаточных мер по пресечению ставших им известными фактов нарушения прав Комитета.

8.‍Заключительные положения

8.1.‍Настоящее положение утверждается и изменяется Председателем комитета Комитета.

8.2.‍Настоящее положение уточняется и изменяется в соответствии с изменением действующего законодательства.

|  |
| --- |
| Приложение 17 |
| к приказу № 57р |
| от 11.07.2024 |

**ПОРЯДОК**

**по защите информации от утечки по техническим каналам**

1. Общие положения
   1. Настоящий Порядок определяет структуру системы технической защиты информации ограниченного доступа, основы организации технической защиты информации ограниченного доступа и финансирование мероприятий по технической защите информации ограниченного доступа в комитете по земельным ресурсам и землеустройству города Барнаула (далее – комитет по земельным ресурсам и землеустройству города Барнаула).
   2. Настоящий Порядок является документом, обязательным для исполнения в комитете по земельным ресурсам и землеустройству города Барнаула при проведении работ по технической защите информации ограниченного доступа от утечки по техническим каналам, несанкционированного доступа к информации ограниченного доступа, специальных воздействий на информацию ограниченного доступа в целях ее уничтожения, искажения и блокирования.
   3. Настоящий Порядок разработан в соответствии с Положением о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденным постановлением Совета Министров – Правительства Российской Федерации № 912-51 от 15.09.1993.
2. Структура системы технической защиты информации ограниченного доступа в комитет по земельным ресурсам и землеустройству города Барнаула
   1. Систему технической защиты информации ограниченного доступа в комитете по земельным ресурсам и землеустройству города Барнаула возглавляет Администратор информационной безопасности комитета по земельным ресурсам и землеустройству города Барнаула.
   2. Организационную структуру системы технической защиты информации ограниченного доступа в комитете по земельным ресурсам и землеустройству города Барнаула образуют:

* главный специалист по информатизации комитета по земельным ресурсам и землеустройству города Барнаула – в части реализаций мер технической защиты информации ограниченного доступа в комитете по земельным ресурсам и землеустройству города Барнаула.

1. Организация технической защиты информации ограниченного доступа
   1. Мероприятия по технической защите информации ограниченного доступа являются составной частью деятельности комитета по земельным ресурсам и землеустройству города Барнаула и осуществляются во взаимосвязи с другими мерами по обеспечению установленного режима секретности и конфиденциальности проводимых работ с информацией ограниченного доступа.
   2. Проведение любых мероприятий и работ с использованием информации ограниченного доступа без принятия необходимых мер по ее технической защите не допускается.
   3. Ответственность за организацию и своевременную реализацию эффективных мер по технической защите информации ограниченного доступа возлагается на руководителя комитета по земельным ресурсам и землеустройству города Барнаула.
   4. Техническая защита информации ограниченного доступа осуществляется путем выполнения комплекса мероприятий, направленных на предотвращение:

* утечки информации ограниченного доступа по техническим каналам за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами;
* несанкционированного доступа к обрабатываемой, хранящейся в технических средствах и передаваемой по каналам связи информации ограниченного доступа;
* преднамеренных программно-технических воздействий с целью хищения, разрушения (уничтожения), искажения информации ограниченного доступа в процессе обработки, передачи и хранения;
* перехвата техническими средствами речевой информации ограниченного доступа из помещений.
  1. Объектами, подлежащими технической защите, являются:
* информационные ресурсы, представленные в виде носителей на магнитной и оптической основах, информативных физических полей, информационных массивов и баз данных и содержащие информацию ограниченного доступа;
* технические средства обработки и передачи информации ограниченного доступа;
* помещения, предназначенные для обработки информации ограниченного доступа и проведения секретных (конфиденциальных) переговоров.
  1. Основными организационно-техническими мероприятиями по технической защите информации ограниченного доступа являются:
* категорирование объектов, указанных в пункте 3.5 настоящего раздела, в зависимости от их важности, степени секретности (конфиденциальности) информации ограниченного доступа и условий эксплуатации, а также классификация автоматизированных систем по требованиям защищенности от несанкционированного доступа к информации ограниченного доступа;
* разработка и внедрение решений по технической защите информации ограниченного доступа при создании и эксплуатации объектов, указанных в пункте 3.5 настоящего раздела;
* применение информационных и автоматизированных систем управления в защищенном исполнении;
* организация аттестации объектов, указанных в пункте 3.5 настоящего раздела
* раздела, по требованиям безопасности информации ограниченного доступа (в случае, если это необходимо по требованиям законодательства);
* обеспечение физической защиты объектов, указанных в пункте 3.5 настоящего раздела;
* обеспечение защиты информации ограниченного доступа от утечки по техническим каналам при ее обработке, хранении и передаче;
* обеспечение защиты информации ограниченного доступа от несанкционированного доступа к ней в автоматизированных информационных системах и локальных вычислительных сетях, а также от компьютерных вирусов;
* совершенствование методической базы обеспечения информационной безопасности;
* организация и проведение контроля состояния технической защиты информации ограниченного доступа.
  1. Конкретные методы, приемы и меры технической защиты информации ограниченного доступа разрабатываются в зависимости от степени возможного ущерба в случае ее утечки, разрушения (уничтожения) на основании федеральных законов, стандартов, нормативно-методических и руководящих документов по технической защите информации ограниченного доступа Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации.
  2. Подготовка и переподготовка (повышение квалификации) специалистов по технической защите информации ограниченного доступа комитета по земельным ресурсам и землеустройству города Барнаула в области технической защиты информации ограниченного доступа организуются на базе учебных заведений, осуществляющих подготовку, переподготовку и повышение квалификации специалистов в области защиты информации.

1. Контроль состояния технической защиты информации ограниченного доступа
   1. Контроль состояния технической защиты информации ограниченного доступа (далее – Контроль) осуществляется в целях оценки организации технической защиты информации ограниченного доступа, своевременного выявления и предотвращения утечки информации ограниченного доступа по техническим каналам, несанкционированного доступа к ней, оценки защиты ее от технических разведок.

Контроль заключается в проверке выполнения требований федеральных законов, нормативно-методических и руководящих документов по технической защите информации ограниченного доступа Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации, а также в оценке достаточности принимаемых мер по технической защите информации ограниченного доступа.

* 1. Основными задачами контроля являются:
* оценка деятельности комитета по земельным ресурсам и землеустройству города Барнаула по руководству и координации работ в области технической защиты информации ограниченного доступа в пределах их компетенции;
* выявление технических каналов утечки информации ограниченного доступа на объектах, указанных в пункте 3.5 раздела 3 настоящего Руководства, каналов несанкционированного доступа к информации ограниченного доступа и специальных воздействий на информацию ограниченного доступа, анализ и инструментальная оценка возможностей технических разведок по получению информации ограниченного доступа;
* оценка эффективности проводимых мер по технической защите информации ограниченного доступа;
* выявление и анализ нарушений, установленных федеральным законодательством норм и требований, нормативно-методических и руководящих документов по технической защите информации ограниченного доступа Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации и принятие оперативных мер по пресечению выявленных нарушений;
* разработка рекомендаций по устранению выявленных недостатков в организации и состоянии работ по технической защите информации ограниченного доступа;
* проверка устранения недостатков, выявленных в результате Контроля.
  1. Контроль в комитете по земельным ресурсам и землеустройству города Барнаула организуется в соответствии с федеральным законодательством.
  2. Контроль в комитете по земельным ресурсам и землеустройству города Барнаула (порядок функционирования средств технической защиты информации, соблюдение установленных режимов работы объектов, указанных в пункте 3.5 раздела 3 настоящего Руководства, выполнение установленных мер по технической защите информации ограниченного доступа, в том числе от несанкционированного доступа) осуществляется структурными подразделениями (штатными специалистами) по защите информации, а также утвержденными экспертными комиссиями по защите информации.

1. Финансирование мероприятий по технической защите информации ограниченного доступа
   1. Финансирование мероприятий по технической защите информации ограниченного доступа в комитете по земельным ресурсам и землеустройству города Барнаула предусматривается в бюджетных сметах комитета по земельным ресурсам и землеустройству города Барнаула.