КОМИТЕТ ПО УПРАВЛЕНИЮ МУНИЦИПАЛЬНЫМ ИМУЩЕСТВОМ КАЧКАНАРСКОГО ГОРОДСКОГО ОКРУГА

РАСПОРЯЖЕНИЕ

от 28 февраля 2024 года № 19
г. Качканар Свердловской области

Об утверждении Положения об информационной безопасности (защите информации) в Комитете по управлению муниципальным имуществом Качканарского городского округа

Во исполнение федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и защите информации» и федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» Комитет по управлению муниципальным имуществом Качканарского городского округа делает следующее распоряжение:

1. Утвердить Положение об информационной безопасности (защите информации) в Комитете по управлению муниципальным имуществом Качканарского городского округа (приложение).
2. Главному специалисту Горшениной С.Г. ознакомить всех специалистов Комитета с настоящим распоряжением под роспись.
3. Опубликовать настоящее распоряжение на официальном сайте Комитета по управлению муниципальным имуществом Качканарского городского округа.
4. Контроль за исполнением настоящего распоряжения оставляю за собой.

Председатель Комитета О.В.Адамчук

УТВЕРЖДЕНО
распоряжением Комитета
по имуществу КГО
от 28.02.2024 № 19

ПОЛОЖЕНИЕ
Об информационной безопасности Комитета по управлению муниципальным имуществом Качканарского городского округа

1. Общие положения

1. Положение об информационной безопасности Комитета по управлению муниципальным имуществом Качканарского городского округа (далее – Положение, Комитет) регламентирует порядок организации и правила обеспечения информационной безопасности в Комитете, распределение функций и ответственности за обеспечение информационной безопасности между сотрудниками Комитета, требования по информационной безопасности к информационным средствам, применяемым в Комитете.

2. Положение является локальным нормативным актом Комитета. Требования настоящего Положения обязательны для всех сотрудников Комитета и распространяются на автоматизированные системы, средства телекоммуникаций и помещения Комитета.

Положение подлежит применению по месту нахождения Комитета: Свердловская область, г.Качканар, ул.Сверлова, д. 8

3. Настоящее Положение разработано в соответствии с:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- «ГОСТ Р 51583-2014. Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» (утвержден и введен в действие Приказом Росстандарта от 28.01.2014 № 3-ст);
- «ГОСТ Р 56545-2015. Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей» (утвержден и введен в действие Приказом Росстандарта от 19.08.2015 № 1180-ст);
- «ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» (принят и введен в действие Постановлением Госстандарта Российской Федерации от 09.02.1995 № 49);
- «ГОСТ Р 56938-2016. Национальный стандарт Российской Федерации. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения» (утвержден и введен в действие Приказом

Росстандарта от 01.06.2016 N 457-ст);

- «ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» (утв. Приказом Ростехрегулирования от 27.12.2007 № 513-ст);

- «ГОСТ Р ИСО/МЭК 27033-1-2011. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции» (утвержден и введен в действие Приказом Росстандарта от 01.12.2011 № 683-ст);

- и иными нормами действующего законодательства Российской Федерации.

4. Основные понятия, используемые в настоящем Положении:

сервер - аппаратно-программный комплекс, исполняющий функции хранения и обработки запросов пользователей и не предназначенный для локального доступа пользователей (выделенный сервер, маршрутизатор и другие специализированные устройства) ввиду высоких требований по обеспечению надежности, степени готовности и мер безопасности информационной системы Комитета.

рабочая станция - персональный компьютер (терминал), предназначенный для доступа пользователей к ресурсам Автоматизированной системы Комитета, приема передачи и обработки информации.

автоматизированная система (АС) - совокупность программных и аппаратных средств, предназначенных для хранения, передачи и обработки данных и информации и производства вычислений.

системный администратор – сотрудник Комитета, либо лицо, по гражданско-правовому договору выполняющие функции системного администратора, и в обязанности которого входит обслуживание всего аппаратно-программного комплекса Комитета, управление доступом к сетевым ресурсам, а также поддержание требуемого уровня отказоустойчивости и безопасности данных, их резервное копирование и восстановление;

пользователь - сотрудник Комитета, использующий ресурсы информационной системы Комитета для выполнения должностных обязанностей;

учетная запись - информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в автоматизированной системе. Учетная запись может содержать дополнительную информацию (адрес электронной почты, телефон и т.п.);

пароль - секретная строка символов (букв, цифр, специальных символов), предъявляемая пользователем компьютерной системе для получения доступа к данным и программам. Пароль является средством защиты данных от несанкционированного доступа;

изменение полномочий - процесс создания удаления, внесения изменений в учетные записи пользователей АС, создание, удаление изменение наименований почтовых ящиков и адресов электронной почты, создание, удаление изменение групп безопасности и групп почтовой рассылки, а также другие изменения, приводящие к расширению (сокращению) объема информации либо ресурсов доступных пользователю АС.

2. Цели и задачи обеспечения безопасности информации

5. Информационная безопасность является одним из составных элементов комплексной безопасности Комитета.

Под информационной безопасностью Комитета понимается состояние защищенности информационных ресурсов, технологий их формирования и использования, а также деятельность, направленная на обеспечение защищенного состояния объекта информации, в том числе объектов автоматизированных и телекоммуникационных систем, противодействия техническим разведкам, включающая комплексные, криптографические, компьютерные, организационные, технические средства защиты.

6. Обеспечение информационной безопасности осуществляется по следующим направлениям:

- правовая защита – процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная защита – это регламентация деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;
- инженерно-техническая защита – это использование различных технических средств, препятствующих нанесению ущерба.

7. Информационная безопасность включает:

- защиту интеллектуальной собственности Комитета;
- защиту компьютеров, локальных сетей и сети подключения к системе Интернета;
- организацию защиты конфиденциальной информации, в т.ч. персональных данных сотрудников и иных физических лиц;
- учет всех носителей конфиденциальной информации.

8. Информационная безопасность Комитета должна обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);
- целостность (точность и полноту информации и компьютерных программ);
- доступность (возможность получения пользователями информации в пределах их компетенции).

9. К объектам информационной безопасности Комитета относятся:

- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;

- информацию, защита которой предусмотрена законодательными актами РФ, в т. ч. Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

- средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

10. Главная цель обеспечения безопасности информации, циркулирующей в Комитете, является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации в целях предотвращения ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационно-телекоммуникационной системы Комитета.

11. Основными задачами обеспечения безопасности информации являются:

- соответствие положениям законодательных актов и нормативным требованиям по защите информации;

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам Комитета, нарушению нормального функционирования и развития Комитета;

- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;

- эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;

- координация деятельности специалистов Комитета по обеспечению защиты информации;

- создание механизмов управления системой информационной безопасности;

- развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;

- создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности.

12. В целях реализации стоящих перед системой обеспечения информационной безопасности задач в Комитете устанавливается:

- недопущение несанкционированного доступа к персональным данным сотрудников и иных физических лиц при их обработке с использованием средств автоматизации или без использования таких средств;

- контроль использования электронных средств информационного обеспечения деятельности Комитета по прямому назначению в виде плановых и внеплановых проверок. Содержание проверок - сложившаяся практика использования персональных компьютеров, мультимедийных систем, копировально-множительной аппаратуры и сканирующих устройств, телефонных аппаратов, а также программного обеспечения к указанным средствам и устранение выявленных в ходе проверок недостатков;

- противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности Комитета нелицензированных программных продуктов и электронных носителей информации способных произвести заражение программного обеспечения вирусами;

- внутрисетевой контроль перемещения информации;

- принятие мер к воспрещению доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими, постоянное ознакомление со сведениями об информационных материалах признанных в соответствии с действующим законодательством экстремистскими, доведение этих сведений до сотрудников Комитета и принятие мер к воспрещению доступа к этим материалам;

- проверка целесообразности использования сотрудниками Комитета интернет-ресурсов, анализ допускаемых нарушений и принятие мер к недопущению их нецелевого использования средствами технического противодействия. Установление и доведение в форме инструкций до сотрудников Комитета требований об ограничениях при использовании интернет-ресурсов, постоянный контроль за выполнением указанных ограничений, разработка, внедрение, и применение технических (программных) средств противодействия возникающим нарушениям, либо злоупотреблениям;

- обучение персонала Комитета по вопросам обеспечения информационной безопасности, проведение занятий с персоналом в целях формирования у них соответствующих знаний, умений и навыков позволяющих соблюдать требования по обеспечению информационной безопасности Комитета;

- выявление фактов нецелевого использования средств телефонной связи и принятие мер технического и организационного характера по их недопущению;

- проведение служебных расследований по фактам нарушения требований защиты информации;

- документирование доказательств неправомерного доступа к компьютерной информации, создания, использования и распространения вредоносных компьютерных программ, нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации,

нарушения правил защиты информации, незаконной деятельности в области защиты информации, разглашения информации с ограниченным доступом, воспрепятствования уверенной работе сайтов в сети Интернет, нарушения требований законодательства о хранении документов и информации, содержащейся в информационных системах;

- взаимодействие с Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации по вопросам защиты информации в Комитете.

3. Порядок обеспечения информационной безопасности

13. При размещении средств вычислительной техники должны быть приняты меры по исключению несанкционированного доступа в помещения посторонним лицам, не имеющим допуск к работе в этих помещениях.

В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями.

Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

14. Общее руководство системой информационной безопасности Комитета осуществляет председатель Комитета.

15. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику Комитета должна быть присвоена учетная запись пользователя и пароль, а также представлены полномочия (права доступа пользователя АС). Использование чужой учетной записи запрещено.

16. Регистрация учетных записей производится в Журнале регистрации пользователей Комитета по управлению муниципальным имуществом Качканарского городского округа (далее по тексту - Журнал регистрации пользователей) (приложение № 1).

17. При поступлении нового сотрудника на муниципальную службу системный администратор, на основании распоряжения председателя Комитета либо лица, его заменяющего, создает новую учетную запись пользователя, предоставляет полномочия, присваивает первичный пароль вновь созданной учетной записи, при необходимости создает почтовый ящик пользователя (далее – объекты безопасности).

18. По окончании процедур создания нового объекта безопасности системный администратор вносит соответствующую запись в Журнал регистрации пользователей.

19. Основанием для изменения полномочий (предоставления, изменения либо прекращения действий прав доступа пользователя АС) является задание, полученное системным администратором от председателя Комитета либо лица, его заменяющего. Проведение изменений системным администратором

без наличия задания от председателя Комитета либо лица, его замещающего, запрещено.

Изменение предоставленных полномочий сотрудниками, не уполномоченными на проведение подобных действий, запрещено и идентифицируется как факт несанкционированного доступа.

20. Все изменения в списках доступа должны быть выполнены системным администратором не позднее одного дня с момента получения задания на внесение изменений.

21. После получения информации о намерениях специалиста уволиться, по распоряжению председателя Комитета либо лица, его заменяющего, организовываются мероприятия по обеспечению мониторинга действий увольняющегося специалиста в информационной системе, обратив особое внимание на факты копирования (переноса) информации, содержащейся в информационной системе, на съемные носители информации, передачи электронных документов по электронной почте, установки и запуска стороннего программного обеспечения.

22. После увольнения муниципального служащего его учетная запись и иные объекты безопасности подлежат удалению. Основанием для удаления объектов безопасности является задание, полученное системным администратором от председателя Комитета либо лица, его заменяющего. Удаление объектов безопасности системным администратором без наличия задания от председателя Комитета либо лица, его замещающего, запрещено.

Одновременно с удалением объектов безопасности проводится инвентаризация программного обеспечения и данных, содержащихся на автоматизированном рабочем месте уволившего специалиста, на предмет наличия стороннего программного обеспечения и каналов удаленного доступа и удаляется неиспользуемое в работе программное обеспечение.

23. Задание на удаление должно быть исполнено системным администратором не позднее одного дня с момента получения.

24. По окончании процедуры удаления учетной записи системный администратор вносит соответствующую запись в Журнал регистрации пользователей.

25. Локальные учетные записи компьютеров (Administrator, Guest) предназначены для служебного использования системным администратором при настройке системы и не предназначены для повседневной работы.

Создание и использование локальных учетных записей на рабочих станциях запрещено.

26. Встроенная учетная запись Guest (Гость) должна быть заблокирована на всех рабочих станциях при первоначальном конфигурировании операционной системы.

27. Категорически запрещается использование встроенной учетной записей Administrator (SA для SQL сервера и т.п.) для повседневной работы, для запуска служб и сервисов либо для доступа к сетевым ресурсам. Использование встроенных учетных записей допускается только в случаях, требующих реквизитов именно этой учетной записи (восстановление AD, восстановление поврежденных данных системы, в некоторых случаях проведение обновлений системы и т.п.).

28. Создание специальных учетных записей (реквизиты доступа к активному сетевому оборудованию, учетные записи для доступа к базам данным, а также все учетные записи, реквизиты которых не хранятся в едином каталоге AD) производится системным администратором при возникновении необходимости.

4. Требования к паролям

29. Первичный пароль в виде комбинации символов (букв, цифр, знаков препинания, специальных символов) устанавливается системным администратором при создании новой учетной записи.

Допускается в качестве первичного пароля использовать несложную комбинацию символов, либо повторяющиеся символы.

Ответственность за сохранность первичного пароля лежит на системном администраторе.

30. При задании первичного пароля администратор обязан установить опцию, требующую смену пароля при первом входе в систему (отметка «Потребовать смену пароля при первом входе в систему»), а также уведомить владельца учетной записи о необходимости произвести смену пароля.

31. При сбросе забытого пароля на учетную запись также используется первичный пароль.

32. Установку основного пароля в виде комбинации символов (букв, цифр, знаков препинания, специальных символов), известная только пользователю и используемая для подтверждения подлинности владельца учетной записи, производит пользователь при первом входе в систему с новой учетной записью.

33. При выборе пароля необходимо руководствоваться следующими правилами:

- длина пароля должна составлять не менее 8 символов;
- при выборе пароля, рекомендуется использовать комбинацию из строчных и прописных букв, цифр, знаков препинания и специальных символов;
- запрещается использовать в качестве пароля название учетной записи, фамилию или имя пользователя, а также легко угадываемые сочетания символов;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.), а также сокращения (USER, ADMIN, root, и т.д.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

34. Пользователь несет персональную ответственность за сохранение в тайне основного пароля.

Запрещается сообщать пароль другим лицам (в том числе при убытии в командировку, отпуск и в случае болезни), записывать его, а также пересылать открытым текстом в электронных сообщениях.

35. Пользователь обязан не реже одного раза в три месяца производить смену основного пароля, соблюдая требования настоящего Положения.

36. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом председателю Комитета и системному администратору, а также изменить основной пароль.

37. Восстановление забытого основного пароля пользователя осуществляется системным администратором путем изменения (сброса) основного пароля пользователя на первичный пароль на основании письменной заявки пользователя.

38. Для предотвращения угадывания паролей системный администратор обязан настроить механизм блокировки учетной записи при трехкратном неправильном вводе пароля.

39. Разблокирование учетной записи пользователя осуществляется системным администратором на основании заявки владельца учетной записи.

40. При настройке служебных учетных записей, учетных записей служб и сервисов, а также специальных учетных записей используется административный пароль (комбинация букв, цифр, знаков препинания, специальных символов).

5. Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации, содержащими ключи квалифицированной электронной подписи

41. При использовании средств квалифицированной электронной подписи средства вычислительной техники должны быть сконфигурированы с учетом следующих требований:

- не использовать нестандартные, измененные или отладочные версии операционных систем;

- исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;

- исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;

- на средствах вычислительной техники с установленными средствами квалифицированной электронной подписи должна быть установлена только одна операционная система;

- все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);

- режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень;

- всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права;

- необходимо предусмотреть меры, максимально ограничивающие доступ к системному реестру, файлам и каталогам, временным файлам, журналам системы, файлам подкачки, кэшируемой информации (пароли и т.п.), отладочной информации;

- необходимо организовать удаление (по окончании сеанса работы средств квалифицированной электронной подписи) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их работы. Если это невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;

- исключить попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий;

- регулярно устанавливать пакеты обновлений безопасности операционной системы (Service Packs, Hot fix и т.п.), обновлять антивирусные базы.

42. В случае подключения технических средств с установленными средствами квалифицированной электронной подписи к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

43. Ключи квалифицированной электронной подписи при их создании должны записываться на предварительно проинициализированные (отформатированные) ключевые носители, типы которых поддерживаются используемым средством квалифицированной электронной подписи согласно технической и эксплуатационной документации к ним.

44. Ключи квалифицированной электронной подписи на ключевом носителе могут быть защищены паролем (ПИН-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство квалифицированной электронной подписи.

Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца ключа квалифицированной электронной подписи.

45. Запрещается:

- осуществлять несанкционированное копирование ключевых носителей;

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер и иные средства отображения информации;

- использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;

- вносить какие-либо изменения в программное обеспечение средств квалифицированной электронной подписи;

- записывать на ключевые носители постороннюю информацию;

- оставлять средства вычислительной техники с установленными средствами квалифицированной электронной подписи без контроля после ввода ключевой информации;

- использовать ключ электронной подписи и соответствующий сертификат ключа проверки электронной подписи, Заявление на изменение статуса которого подано в территориальный орган Федерального казначейства, в течение времени, исчисляемого с момента подачи Заявления на изменение статуса сертификата по момент официального информирования об изменении статуса сертификата, либо об отказе в изменении статуса;

- использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено;

- удалять ключевую информацию с ключевого носителя до истечения срока действия, аннулирования или прекращения действия сертификата ключа проверки электронной подписи.

46. Недопустимо пересылать файлы с ключевой информацией для работы в информационных системах по электронной почте сети Интернет или по внутренней электронной почте (кроме открытых ключей).

47. Носители ключевой информации должны использоваться только их владельцем и храниться в месте, не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.).

48. Носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средствами квалифицированной электронной подписи операций формирования и проверки квалифицированной электронной подписи, шифрования и дешифрования. На носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

49. В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства квалифицированной электронной подписи, необходимо гарантированно удалить всю информацию (при условии исправности технических средств), в том числе средства квалифицированной электронной подписи, журналы работы систем обмена электронными документами и так далее.

6. Доступ к интернет-ресурсам и электронной почте

50. Для исполнения задач, связанных с производственной деятельностью сотрудникам Комитета предоставляется доступ к интернет-ресурсам. Доступ к интернет-ресурсам в других целях запрещен.

51. Системный администратор обязан не реже одного раза в месяц представлять председателю Комитета отчет об использовании интернет-ресурсов сотрудниками Комитета.

52. Доступ к интернет-ресурсам может быть блокирован системным администратором без предварительного уведомления при возникновении нештатных ситуаций либо в иных случаях, предусмотренных организационными документами.

53. Для исполнения задач, связанных с производственной деятельностью сотрудникам Комитета может быть предоставлен доступ к системе электронной почты. Электронная почта является собственностью Комитета и может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещено.

54. Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию председателя Комитета либо лица его заменяющего.

55. Запрещается использование чужой электронной почты.

56. В случае обнаружения значительных отклонений в параметрах работы средств обеспечения работы системы электронной почты, системный администратор обязан немедленно сообщить об этом председателю Комитета для принятия решений.

57. Доступ к серверу электронной почты может быть блокирован системным администратором без предварительного уведомления при возникновении нештатных ситуаций.

58. При работе с электронной почтой сотрудники Комитета обязаны руководствоваться Инструкцией по обеспечению информационной безопасности в Комитете по имуществу КГО, утверждаемой распоряжением Комитета.

7. Средства защиты информации

59. К использованию в Комитете допускаются только лицензионные средства защиты информации, отвечающие требованиям, установленным законодательством Российской Федерации.

60. Установка средств защиты информации на компьютерах (серверах) Комитета осуществляется системным администратором.

Настройка параметров средств защиты информации осуществляется системным администратором в соответствии с руководствами по применению

конкретных средств защиты информации. Изменение настроек другими сотрудниками запрещено.

61. Ежедневно в начале работы при загрузке компьютера (для серверов при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов PC.

62. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (флеш-накопителях, магнитных дисках, CD-ROM и т.п.).

63. Антивирусная проверка должна проводиться на компьютерах сотрудников - не реже одного раза в неделю, на серверах - не реже двух раз в неделю.

64. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник Комитета самостоятельно или вместе с системным администратором должен провести внеочередной антивирусный контроль своей рабочей станции.

8. Хранение данных и установка программного обеспечения

65. Специалисты Комитета обязаны использовать предоставленные им аппаратно-программные средства только для хранения информационных ресурсов, необходимых для осуществления своих должностных обязанностей.

Хранение личной информации на компьютерах сотрудников запрещено.

66. Ответственность за обеспечение целостности данных, хранимых на компьютерах сотрудников Комитета, возлагается на самих сотрудников.

67. Ответственность за обеспечение целостности данных, хранимых на серверах Комитета, возлагается на системного администратора.

68. Установка нового программного обеспечения возможна только системным администратором. Установка нового программного обеспечения сотрудниками Комитета запрещена.

69. Сотрудникам Комитета запрещается производить какие-либо изменения в электрических схемах, монтаже, размещении и комплектации технических средств на автоматизированных рабочих местах.

При самовольном ремонте и (или) установке нового программного обеспечения ответственность за сбои в работе оборудования и программного обеспечения лежит на сотрудниках Комитета.

70. При обнаружении несанкционированных изменений в аппаратных или программных средствах сотрудники Комитета должны немедленно поставить в известность системного администратора и председателя Комитета.

Приложение № 1
к Положению об информационной
безопасности Комитета по
управлению муниципальным
имуществом Качканарского
городского округа, утвержденное
распоряжением Комитета по
имуществу КГО
от 28.02.2024 № 19

Журнал регистрации пользователей Комитета по управлению муниципальным имуществом Качканарского городского округа

№ п.п.	**Дата подключения отключения**	**Должность пользователя**	**Фамилия Имя Отчество**	**Учетная запись**	**Дата/Подпись**