Приложение 6.

УТВЕРЖДЕНО
Распоряжением Администрации
Качканарского городского округа
Свердловской области
от 29.09.2023 № 83
«Об информационной безопасности
(защите информации) в Администрации
Качканарского городского округа
Свердловской области»

Инструкция пользователя Администрации Качканарского городского округа Свердловской области

Общие обязанности сотрудников по обеспечению информационной безопасности

Сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации, несет персональную ответственность за свои действия и обязан:

1) использовать предоставленные ему аппаратно-программные средства только для выполнения своих должностных обязанностей;
2) использовать предоставленное ему дисковое пространство сервера только для хранения информационных ресурсов, необходимых для осуществления своих должностных обязанностей;
3) использовать пароли, отвечающие установленным требованиям информационной безопасности;
4) использовать антивирусное программное обеспечение при работе с внешними носителями информации и файлами полученными из интернета;
5) соблюдать требования федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи», федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и защите информации», Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных»;
6) при утере пароля пользователь немедленно поставить в известность ответственного по информационной безопасности. Ответственность за несвоевременность уведомления о факте компрометации пароля несет непосредственно пользователь;
7) при утере или компрометации электронной цифровой подписи немедленно поставить в известность непосредственного руководителя и ответственного по информационной безопасности. Ответственность за несвоевременность уведомления о факте утери или компрометации электронной цифровой подписи несет непосредственно пользователь;
8) при обнаружении несанкционированных изменений в аппаратных или программных средствах немедленно поставить в известность ответственного по информационной безопасности;
9) при обнаружении некорректного функционирования программного обеспечения по защите информации немедленно поставить в известность ответственного по информационной безопасности.

Сотруднику запрещается:

1) передавать любые пароли, предназначенные для работы с информационными системами, в том числе при убытии в командировку, отпуск и в случае болезни;

2) использовать в работе принадлежащие другим сотрудникам пароли, предназначенные для работы с информационными системами, в том числе при убытии сотрудника в командировку, отпуск и в случае болезни;
3) осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;
4) осуществлять несанкционированный доступ к информационным ресурсам;
5) самостоятельно производить установку, настройку и модификацию программного обеспечения;
6) использовать сменные машинные носители информации без предварительной проверки на наличие программных вирусов;
7) самостоятельно вскрывать и производить разборку компьютеров, периферийного оборудования;
8) производить какие-либо изменения в электрических схемах, монтаже, размещения и комплектации технических средств на автоматизированных рабочих местах.

Обязанности сотрудников по работе с корпоративной электронной почтой

Электронная почта является собственностью учреждения и может быть использована ТОЛЬКО в служебных целях. Использование электронной почты в других целях категорически запрещено.

Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления сотрудника по требованию непосредственного либо вышестоящего руководителя.

Сотруднику запрещается:

1) распространять информацию содержание и направленность которой запрещены международным и Российским законодательством;
2) осуществлять массовую рассылку почтовых сообщений;
3) предоставлять, кому бы-то ни было пароль доступа к своему почтовому ящику;
4) отправлять во вложениях файлы мультимедиа и исполняемые файлы, письма с такими вложениями не обрабатываются почтовым сервером и не могут быть доставлены;

При работе с почтовой обратить на следующие моменты :

1) Внимательно проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом;
2) Проверять письма, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;
3) Не переходить по ссылкам, которые содержатся в электронных письмах, особенно если они длинные или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyuri.com и т.д.);
4) Не нажимать на ссылки из письма, если они заменены на слова, не наводить на них мышкой и просматривать полный адрес сайтов;
5) Проверять ссылки, даже если письмо получено от другого пользователя информационной системы;

6) Не открывать вложения, особенно если в них содержаться документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD;
7) Пересылать все подозрительные электронные письма на почтовый ящик электронной почты sd@kgo66.ru с темой «Подозрительное письмо»

Внимание!

Возможность получить доступ к ресурсу не является гарантией того, что запрошенный ресурс является разрешенным политиками учреждения.

Вся информация о ресурсах, посещаемых сотрудниками компании, протоколируется и, при необходимости, может быть предоставлена руководителям подразделений, а так же руководству учреждения для детального изучения.

Сотрудники могут нести дисциплинарную ответственность за нарушение данной инструкции.