УДК 004.056

Казанцев В.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ УДАЛЕННОЙ РАБОТЕ

Аннотация. В статье раскрываются особенности организации защиты информации, связанные с удаленной работой сотрудников, которые применяют мобильные устройства в своей деятельности. В содержании статьи акцентируется внимание на проблемах, возникающих в связи с этим, проводится анализ существующих мер безопасности при удаленной работе при помощи мобильных устройств и определяются направления совершенствования существующей практики их применения.

Ключевые слова: информация, информационная безопасность, мобильное устройство, смартфон, удаленный доступ, удаленное рабочее место.

Сегодня удаленная работа набирает все большую популярность, и формат работы продолжает укрепляться на рынке труда [1]. Но, не все организации готовы к полноценному переходу на такой формат, и даже те, кто перешли на удаленную работу, зачастую испытывают трудности с обеспечением надежной защиты конфиденциальной информации. Главная проблема, с которой сталкиваются при внедрении удаленной работы сотрудников, – это риски в сфере информационной безопасности (ИБ), способные нанести ущерб репутации и финансовому положению компании. Кроме того, встает также вопрос, связанный с адаптацией сотрудников при переходе на удаленный формат из офиса и поддержанием необходимой продуктивности в связи с отсутствием физического контроля.

Стоит отметить, что растущая тенденция использования личных устройств, в том числе и мобильных, для удаленной работы требует особого внимания к вопросам защиты информации. Современные смартфоны не так давно стали мощным инструментом для удаленной работы, решающим те задачи, которые ранее требовали применение персональных компьютеров (ПК). Для компаний основным преимуществом стало сокращение затрат на покупку оборудования для персонала и его техническое обслуживание, а повышение гибкости и мобильности сотрудников [2].

В формате, когда сотрудник уходит на удаленную работу, особенно с использованием личных мобильных устройств, возникает целый ряд проблем и рисков информационной безопасности. Утечка конфиден-

циальных данных может иметь серьезные последствия для организации. Поэтому крайне важно вовремя и эффективно выявлять уязвимости и угрозы информационной безопасности, а также разрабатывать и внедрять современные средства и методы защиты данных при организации удаленной работы с использованием мобильных устройств.

Удаленная работа вне офиса создает серьезные риски для защиты конфиденциальной информации [3]. Так, в случае потери или кражи устройства с данными, корпоративные сведения могут быть раскрыты неавторизованным лицом. Нельзя не взять во внимание и кибератаки, нацеленные на уязвимые и оставленные без надзора мобильные устройства. Для обеспечения надежной защиты информации требуется применять шифрование данных, использовать сложные пароли и внедрять другие охранные меры, а также регулярно проводить проверки на предмет угроз, особенно при удаленном формате работы.

Риск заражения мобильных устройств сотрудников вредоносным ПО или использования нелицензионных программ сотрудниками крайне значителен. Нельзя исключить вероятность перехода работника по подозрительной ссылке, что приведет к заражению устройства и, как следствие, к потере личной и конфиденциальной информации.

Зачастую домашние сети имеют слабую защиту. Пользователи пренебрегают сменой стандартных паролей Wi-Fi или делают сеть открытой, вовсе отключая парольную защиту. Настройка и выбор VPN могут представлять сложность для некоторых пользователей. Бесплатные VPN-сервисы также небезопасны, так как подвергают риску данные и конфиденциальность.

При переходе на удаленный режим работы взаимодействие между сотрудниками осуществляется через мессенджеры, электронную почту, видеоконференции и другие платформы. Вероятность взлома учетных записей значительно возрастает при недостаточном уровне защиты паролями.

Также руководство сталкивается с трудностями при внедрении правил информационной безопасности среди персонала в связи с тем, что личные гаджеты не являются собственностью компании. Довольно сложно обязать работников применять специальные программы для хранения паролей, вовремя устанавливать обновления антивирусного ПО и повсеместно активировать двойную аутентификацию при входе в сервисы. Особенно трудно это отследить, учитывая тот факт, что сотрудник находится на удаленном формате работы. Все вышеперечисленные факторы значительно повышают угрозу утечки и несанкционированного доступа к защищаемой информации, поэтому важно применять эффективные меры по защите, например обязательное внедрение организационных и технических мер от утечки и несанкционированного доступа.

К организационным мерам можно отнести [4]:

– разграничение прав доступа сотрудников при организации удаленной работы с мобильных устройств;

– соблюдение регламентов работы с конфиденциальной информацией;

– регулярное обучение и повышение квалификации сотрудников по защите информации.

Как отмечалось ранее, одной лишь организационной защиты информации недостаточно, необходимо внедрение и технических средств: антивирусных программ; использование VPN-сервисов на платной основе для обеспечения безопасного доступа к корпоративной сети; настройка двухфакторной аутентификации для доступа к важным сервисам; осуществление контроля за корпоративной электронной почтой и корпоративной телефонией; использование шифрования при передаче данных; применение лицензионного ПО; регулярное изменение паролей и усиление требований к их надежности; своевременное обновление операционных систем и ПО.

Стоит отметить, что использование DLP-систем является комплексным решением, которое имеет возможность анализа данных и в случае обнаружения угрозы незамедлительное оповещение. Примерами популярных российских DLP-систем, работающих на мобильных платформах iOS и Android, являются: Naumen Service Desk, SearchInform КИБ, InfoWatch Traffic Monitor и др.

DLP-системы имеют возможность контролировать потоки информации по различным каналам обмена информации, проводить аудит подключаемых накопителей, контроль распечатанных документов, реагирование на удаление и установку программ и другие важные функции. Популярность DLP-систем при переходе на удаленный формат работы растет с каждым годом, поскольку обеспечивает высокий уровень безопасности информации.

Список использованных источников:

1. Бирюков А.А. Информационная безопасность: защита и нападение: руководство / А.А. Бирюков. 3-е изд. М.: ДМК Пресс, 2023. 440 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/455351 (дата обращения: 15.04.2025).

2. Кибербезопасность: технические и правовые аспекты защиты информации: сборник научных трудов I Национальной научно-практической конференции (г. Москва, 24–26 мая 2023 г.) / под ред. А.А. Акаева [и др.]. М.: РТУ МИРЭА, 2023. 319 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/398231 (дата обращения: 15.04.2025).

3. Шевченко О.А. Удаленка. Дистанционная (удаленная) работа. Комментарий законодательства и схемы: учебное пособие / О.А. Шевченко, К. С. Балицкий, Е. А. Кашехлебова. М.: Проспект, 2021. 31 с. Электрон. Версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/281033 (дата обращения: 13.03.2025).

4. Яппаров Р.М. К вопросу о безопасности объектов критической информационной инфраструктуры / Р.М. Яппаров // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: Сборник материалов VII Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 24–25 мая 2024 г. Уфа: Уфимский университет науки и технологий, 2024. С. 55–58.

Kazantsev V.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

ENSURING INFORMATION SECURITY DURING REMOTE WORK

Abstract. The article reveals the specifics of the organization of information protection related to the remote work of employees who use mobile devices in their activities. The content of the article focuses on the problems that arise in this regard, analyzes the existing security measures for remote work using mobile devices and identifies areas for improving the existing practice of their application.

Keywords: information, rights, information protection, information security, mobile device, smartphone, remote access, remote workplace.