УДК 004

Ижболдина Т. К.
Уфимский университет науки и технологий, Уфа

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

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ УДАЛЕННОЙ РАБОТЫ

Аннотация. В условиях массового перехода на удаленный формат работы, вопросы информационной безопасности (ИБ) приобрели особую

важность и актуальность. В данной статье рассматриваются основные угрозы, возникающие при дистанционной работе, и предлагаются комплексные меры защиты информации. Дистанционный формат, при всей его гибкости и удобстве, создает множество уязвимостей: от использования ненадежных сетей и личных устройств до рисков фишинга и утечек данных. Особое внимание уделяется использованию VPN, многофакторной аутентификации, шифрованию данных и обучению сотрудников.

Ключевые слова: удаленная работа, фишинг, VPN, многофакторная аутентификация, DLP-система, кибербезопасность.

С переходом на удаленный формат работы многие компании и организации столкнулись с новыми инцидентами ИБ. По данным Xakep.ru, в 2023 г. доля целевых атак на организациях увеличилась на 78 % от общего числа [1]. Одной из причин такого роста стала неспособность традиционных средств защиты информации противодействовать атакам. Злоумышленники активно используют уязвимости в домашних сетях, фишинговые атаки и слабые пароли для доступа к корпоративным системам. В связи с этим организациям необходимо адаптировать свои стратегии защиты данных с учетом новых реалий.

К основным угрозам информационной безопасности при дистанционном формате работы относятся:

1. Небезопасные сети и устройства.

В офисной среде IT-отдел обеспечивает централизованный контроль над всей инфраструктурой: корпоративными компьютерами, серверами, маршрутизаторами и межсетевыми экранами. Однако при удаленной работе сотрудники часто подключаются к корпоративным ресурсам через личные устройства (ноутбуки, планшеты, смартфоны) и непроверенные сети, такие как: домашний Wi-Fi становится уязвимым, если роутер не обновлен или использует слабые настройки безопасности (например, устаревший протокол WPA2 или стандартный пароль администратора), что позволяет злоумышленникам перехватывать трафик; общедоступные точки доступа (кафе, аэропорты, коворкинги) представляют угрозу из-за отсутствия шифрования, что облегчает проведение атак типа Man-in-the-Middle (MITM) с перехватом логинов, паролей и конфиденциальных данных; кроме того, личные устройства сотрудников без защиты (отсутствие антивируса, файрвола или актуальных обновлений) превращаются в легкую мишень для вредоносного ПО.

2. Методы социальной инженерии и фишинг.

Социальная инженерия остается крайне опасным методом атак на удаленных сотрудников, особенно уязвимых из-за цифрового формата работы и отсутствия личного взаимодействия. Злоумышленники активно используют психологические манипуляции, поскольку удаленные работники не могут оперативно проверить подозрительные запросы у

коллег, а стресс и высокая нагрузка снижают их бдительность [2]. Наиболее распространены фишинговые письма, маскирующиеся под сообщения от руководства или ИТ-службы с просьбой «обновить данные», фейковые звонки от «техподдержки» с требованием передать пароли или установить вредоносное ПО, а также поддельные профили коллег в мессенджерах, рассылающие зараженные вложения. Эти методы особенно эффективны благодаря изолированности удаленных команд и повышенной доверчивости сотрудников в условиях стресса [6].

3. Организация контроля доступа.

При офисной работе ИТ-специалисты могут оперативно заблокировать уволенного сотрудника или отследить подозрительную активность, однако в удаленном формате контроль значительно усложняется: сотрудники часто используют слабые пароли (типа «123456» или «Password1»), которые легко подбираются брутфорс-атаками; отсутствие сегментации прав приводит к ситуации, когда все удаленные работники имеют одинаковый доступ к системам, что увеличивает риски при компрометации даже одной учетной записи; кроме того, многие сотрудники пренебрегают обновлением операционных систем и корпоративных приложений, оставляя уязвимости (например, в RDP-подключениях), которыми могут воспользоваться злоумышленники [3].

Для эффективной борьбы с названными угрозами безопасности предлагаются следующие методы защиты информации для сотрудников, работающих в удаленном формате:

1. Использование виртуальных частных сетей (VPN). Хороший VPN-сервис шифрует весь интернет-трафик, делая его недоступным для перехвата даже при подключении через ненадежные сети [4]. VPN-сервисы сами могут собирать и анализировать данные пользователей.

2. Внедрение DLP-систем для предотвращения утечек и обязательное шифрование корпоративной переписки.

3. Многофакторная аутентификация (MFA). Даже если злоумышленник получит логин и пароль сотрудника, без дополнительного кода из SMS или мобильного приложения он не сможет получить доступ к системе [5]. Этот простой метод уже предотвратил множество успешных атак по всему миру. Однако даже самые совершенные технические средства не помогут, если сотрудники не понимают основ кибербезопасности.

4. Регулярное обучение должно стать нормой. Необходимо повсеместно практиковать нескучные лекции и практические тренинги с примерами реальных атак. Полезно проводить тестовые фишинговые рассылки внутри компании, чтобы сотрудники на практике учились распознавать угрозы.

5. Для защиты конфиденциальных данных необходимо использовать шифрование как при передаче, так и при хранении информации. Современные решения позволяют шифровать электронную почту, файлы в облачных хранилищах и даже сообщения в корпоративных чатах [7].

Особенно это актуально для компаний, работающих с персональными данными клиентов или коммерческой тайной.

6. Мониторинг безопасности в условиях удаленной работы также требует особого подхода. Системы класса EDR (Endpoint Detection and Response) позволяют отслеживать угрозы на устройствах сотрудников в реальном времени и автоматически блокировать подозрительную активность. При этом важно найти баланс между безопасностью и приватностью, чтобы чрезмерный контроль не вызывал сопротивления у сотрудников.

7. Отдельного внимания заслуживает резервное копирование (back up) данных. Удаленные сотрудники могут случайно удалить или повредить важные файлы, а ransomware-атаки могут зашифровать данные на их устройствах. Регулярные back up в защищенное облачное хранилище или на корпоративные серверы помогут быстро восстановить информацию в случае инцидента.

Таким образом, переход на удаленную работу – это не просто смена рабочего места, а фундаментальное изменение подходов к информационной безопасности. Комплексные технические решения, обучение сотрудников и четкие регламенты должны работать в совокупности. Компании, которые смогут найти баланс между удобством удаленной работы и защитой данных, получат значительное конкурентное преимущество в современном цифровом мире [8].

Список использованных источников:

1. Хакер. Атаки и тренды Q2 2023: что нужно знать о киберугрозах последнего квартала // Xakep.ru. 2023. 30 августа. URL: https://xakep.ru/2023/08/30/q2-2023-attacks-and-trends/.

2. Козлов Д.В., Шестаков А.А. Современные угрозы информационной безопасности в условиях удаленной работы // Информационная безопасность. 2022. № 3(45). С. 56–62.

3. Мельников В.П. Кибербезопасность и защита данных. М.: Юрайт, 2021. 318 с.

4. NIST Special Publication 800-46r2 "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security". 2022. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf /.

5. ENISA Threat Landscape 2023 "Top Cyber Threats and Trends". European Union Agency for Cybersecurity, 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 /.

6. Скляров Д.В., Туманов В.Е. Защита информации в облачных сервисах. СПб.: БХВ-Петербург, 2020. 256 с. Электрон. версия. URL: https://books.4nmv.ru/books/iskusstvo_zashchity_i_vzloma_informatsii_3642868.pdf /.

7. ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection". 2022 / URL: https://www.iso.org/standard/27001 /.

8. Зыков А.И. Цифровизация как средство повышения эффективности предприятия / А.И. Зыков, Р.М. Яппаров // Взаимодействие вузов, научных организаций и учреждений культуры в сфере защиты информации и технологий безопасности: сборник статей по материалам V Международной научной конференции, посвященной памяти доктора технических наук, профессора А.А. Тарасова и доктора технических наук, старшего научного сотрудника О.В. Казарина, Москва, 24–26 апреля 2024 г. М.: Федеральное государственное автономное образовательное учреждение высшего образования «Российский государственный гуманитарный университет», 2024. С. 124-127.

Izhboldina T. K.
Ufa University of Science and Technology, Ufa

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

FEATURES OF ENSURING INFORMATION SECURITY IN THE CONTEXT OF REMOTE WORK

Abstract. In the context of the massive transition to a remote work format, information security issues have become particularly important and relevant. This article examines the main threats posed by remote work and suggests comprehensive information protection measures. The remote format, for all its flexibility and convenience, creates many vulnerabilities: from the use of unreliable networks and personal devices to the risks of phishing and data leaks. Special attention is paid to the use of VPNs, multi-factor authentication, data encryption and employee training.

Keywords: remote work, phishing, VPN, multi-factor authentication, encryption, DLP system, cybersecurity.