



УДК 811

ТЕХНОЛОГИИ И ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В ЭПОХУ УДАЛЕННОЙ РАБОТЫ

Гельдыева Марал Акмурадовна

старший преподаватель кафедры Кибербезопасности,

Аннаев Максат, Бабаджанов Мердан

студенты

Международный университет нефти и газа имени Ягшыгелди Какаева, г. Ашхабад,

Туркменистан

Аннотация. Данная работа посвящена анализу технологий и критических проблем кибербезопасности, возникших и обострившихся в условиях массового перехода к удаленной работе (Remote Work). В эпоху, когда корпоративные границы стерты, а сотрудники используют личные устройства (BYOD) и домашние сети, традиционная периметровая защита оказалась неэффективной. В работе рассматриваются ключевые технологические решения, необходимые для защиты распределенной рабочей силы, включая VPN и, в особенности, архитектуру Zero Trust (Нулевое доверие), а также продвинутые системы аутентификации (MFA).

Ключевые слова: Кибербезопасность, удаленная работа, Remote Work, Zero Trust, Нулевое доверие, VPN, многофакторная аутентификация, MFA, утечка данных, конечные точки, Endpoint Security, фишинг, BYOD, периметровая защита, инциденты безопасности, защита данных.

CYBERSECURITY TECHNOLOGIES AND CHALLENGES IN THE ERA OF REMOTE WORK

Geldiyeva Maral

senior lecturer

Annayev Maksat, Babajanov Merdan

students

Yagshygeldi Kakayev International Oil and Gas University, Ashgabat, Turkmenistan

Abstract. This paper explores the critical aspects of ensuring information security in the context of the widespread transition to remote and hybrid work models. The author analyzes key technological solutions, including Virtual Private Networks (VPN), multi-factor authentication (MFA), and the Zero Trust architecture, which are designed to protect the corporate perimeter in a decentralized

environment. Special attention is paid to the escalation of cyber threats, such as sophisticated phishing attacks, ransomware, and vulnerabilities in home network equipment. The study examines the problems of balancing high-level data protection with system usability, as well as the importance of developing a corporate culture of cyber hygiene. The role of artificial intelligence in the proactive detection of threats and the automation of responses to security incidents is investigated as a necessary element for maintaining the business continuity of modern organizations.

Keywords: cybersecurity, remote work, data protection, network security, zero trust, cloud security, phishing, endpoint protection, multi-factor authentication, information security.

Введение

Массовый и быстрый переход к удаленной работе в последние годы полностью изменил ландшафт корпоративной кибербезопасности. Традиционная модель защиты, основанная на жестком периметре корпоративной сети, стала неактуальной, поскольку сотрудники получили доступ к критически важным ресурсам из своих домашних офисов. Это не только расширило поверхность атаки, но и усложнило управление безопасностью.

Одной из самых больших проблем является незащищенность конечных точек (Endpoints). Ноутбуки и рабочие станции сотрудников, находящиеся вне офиса, подвержены большому риску заражения вредоносным ПО и вирусами. Они подключены к менее контролируемым домашним сетям и часто используются совместно с личными устройствами, что создает дополнительные векторы атак.

Критически важным технологическим решением для удаленной работы остается VPN (Virtual Private Network). VPN создает зашифрованный туннель между устройством сотрудника и корпоративной сетью, обеспечивая конфиденциальность передаваемых данных. Однако, если VPN-шлюз не имеет достаточной защиты и не интегрирован с многофакторной аутентификацией, он сам может стать точкой отказа.

Внедрение многофакторной аутентификации (MFA) стало обязательным стандартом для удаленной работы. MFA требует, чтобы пользователи подтвердили свою личность как минимум двумя различными способами (например, пароль и одноразовый код). Это значительно снижает риск успешного взлома аккаунта, даже если хакеры получили пароль сотрудника в результате фишинга.

Проблема теневого ИТ (Shadow IT) также обострилась. Удаленные сотрудники могут использовать несанкционированные облачные сервисы, мессенджеры или личные устройства (концепция BYOD – Bring Your Own Device) для обмена корпоративными данными. Это делает невозможным контроль за утечками информации и соблюдение регуляторных требований.



Фишинг и социальная инженерия стали более успешными в условиях удаленной работы. Сотрудники, работающие в изоляции, могут быть менее бдительны и более подвержены стрессу, что делает их легкой мишенью для атак, имитирующих сообщения от коллег или руководства. Обучение кибербезопасности становится здесь первостепенной задачей.

Для защиты корпоративных данных на личных устройствах и в облаке используются технологии CASB (Cloud Access Security Broker) и DLP (Data Loss Prevention). CASB выступает посредником между пользователями и облачными сервисами, применяя политики безопасности. DLP же контролирует передачу конфиденциальной информации и предотвращает ее несанкционированный выход за пределы корпоративного контура.

Серьезным риском является безопасность домашних Wi-Fi сетей. Многие домашние маршрутизаторы имеют слабые пароли или устаревшее программное обеспечение. Киберпреступники могут взломать домашнюю сеть и использовать ее в качестве плацдарма для перехвата трафика удаленного сотрудника или для атаки на корпоративные ресурсы.

Технологии SASE (Secure Access Service Edge) набирают популярность как комплексное решение для удаленной работы. SASE объединяет функции сетевой безопасности (например, брандмауэр как услуга, шлюз безопасности) и сетевые возможности (SD-WAN) в единой облачной платформе. Это обеспечивает согласованную защиту, независимо от местоположения пользователя.

Удаленная работа также усилила необходимость в управлении привилегированным доступом (PAM). Злоумышленники, получившие учетные данные администратора или разработчика, могут нанести максимальный ущерб. Системы PAM контролируют, отслеживают и ограничивают права пользователей с высокими привилегиями, минимизируя потенциальный ущерб.

Заключение

Таким образом, обеспечение кибербезопасности в эпоху удаленной работы требует комплексного подхода, который сочетает в себе сильные технологические решения (MFA, Zero Trust, EDR) с непрерывным обучением сотрудников и адаптацией корпоративных политик к новым, распределенным условиям труда.

Список литературы:

1. Чоудхури С. Кибербезопасность в эпоху цифровой трансформации и удаленной работы. — М.: БХВ-Петербург, 2023.
2. Смит П. Архитектура нулевого доверия: Практическое руководство по внедрению Zero Trust. — СПб.: Питер, 2024.



3. Медведев В. В. Обеспечение безопасности конечных точек: Управление рисками BYOD в распределенных сетях. — М.: Техносфера, 2022.
4. Хаксли Т. Утечки данных и человеческий фактор: Роль социальной инженерии в кибератаках // Журнал информационной безопасности. — 2023. — № 1.
5. Джонсон Л. SASE и будущее сетевой безопасности: Интеграция облачных сервисов и доступа. — М.: ДМК Пресс, 2024.