Назарова Анастасия Алексеевна, студентка, факультет информационных технологий и анализа больших данных, Финансовый университет при Правительстве Российской Федерации, г. Москва
Почта: anna21113@gmail.com

КИБЕРБЕЗОПАСНОСТЬ В УСЛОВИЯХ УДАЛЕННОЙ РАБОТЫ

Аннотация. В данной статье исследуются актуальные угрозы и решения в области кибербезопасности для распределённых IT-команд. С массовым переходом на удалённую работу возросло количество атак на корпоративные сети, облачные сервисы и личные устройства сотрудников. В статье анализируются современные технологии защиты данных в условиях гибридной работы: от многофакторной аутентификации (MFA) и zero-trust архитектур до автоматизированных систем мониторинга угроз на основе ИИ. Особое внимание уделяется уязвимостям, связанным с использованием личных устройств (BYOD), публичных Wi-Fi и облачных приложений, а также методам противодействия социальной инженерии. Практические рекомендации дополнены кейсами из опыта ведущих IT-компаний, что делает материал полезным для специалистов по информационной безопасности и руководителей цифровых проектов.

Annotation. This article explores current threats and solutions in the field of cybersecurity for distributed IT teams. With the widespread shift to remote work, the number of attacks on corporate networks, cloud services, and employees' personal devices has significantly increased. The article analyzes modern data protection technologies in the context of hybrid work environments — from multi-factor authentication (MFA) and zero-trust architectures to AI-powered automated threat monitoring systems. Special attention is given to vulnerabilities related to the use of personal devices (BYOD), public Wi-Fi networks, and cloud applications, as well as methods to counter social engineering. Practical recommendations are supplemented with case studies from leading IT companies, making the material valuable for cybersecurity professionals and digital project managers.

Ключевые слова: Кибербезопасность, удалённая работа, искусственный интеллект

Keywords: Cybersecurity, remote work, artificial Intelligence

С переходом значительной части бизнеса на удалённый или гибридный формат работы информационная безопасность оказалась перед новыми вызовами. Централизованная инфраструктура, ранее обеспечивавшая контроль за сетевой активностью и доступом к корпоративным ресурсам, уступила место децентрализованным моделям, где каждый сотрудник становится потенциальной точкой уязвимости. Основным фактором роста атак стало широкое распространение использования личных устройств в профессиональных целях (модель BYOD — *Bring Your Own Device*), что существенно осложнило контроль доступа и привело к появлению множества потенциальных точек входа для злоумышленников. Кроме того, многие домашние сети не обеспечивают достаточного уровня защиты, а сотрудники, не обладающие техническими навыками в области кибербезопасности, часто становятся мишенью фишинга и других форм социальной инженерии. Всё это способствовало резкому увеличению числа инцидентов, связанных с компрометацией данных, утечками и несанкционированным доступом к корпоративным системам. На фоне снижения защищённости корпоративной ИТ-инфраструктуры наблюдается диверсификация и усложнение самих киберугроз.

Одним из наиболее распространённых и эффективных методов остаётся фишинг — целенаправленная рассылка писем или сообщений, содержащих вредоносные ссылки, файлы либо имитирующих легитимные запросы от имени банков, руководства или сервисных служб. Атаки становятся всё более персонализированными: злоумышленники используют информацию из открытых источников (например, социальных сетей), чтобы повысить доверие жертвы. В условиях удалённой работы, когда сотрудники находятся вне физического пространства офиса, без возможности быстро свериться с

коллегами или ИТ-отделом, вероятность успеха фишинговой атаки возрастает. Особенно уязвимыми становятся новички и сотрудники без опыта работы с угрозами социальной инженерии.

Следующий серьёзный вектор угроз — использование незащищённых беспроводных сетей, особенно при подключении через общественные Wi-Fi-точки доступа в кафе, гостиницах, транспорте или коворкингах. Многие пользователи пренебрегают базовыми мерами предосторожности, включая шифрование трафика или использование VPN. Это создаёт благоприятную среду для атак «man-in-the-middle», при которых злоумышленник незаметно перехватывает передаваемую информацию: логины, пароли, внутренние документы и даже видеозвонки. Дополнительную опасность представляет техника создания фальшивой сети («evil twin»), когда поддельная точка доступа маскируется под легитимную — пользователь подключается к ней автоматически, открывая полный доступ к своим данным.

Не менее уязвимыми остаются облачные сервисы, стремительно вошедшие в обиход как инструмент совместной работы. Популярность таких решений, как Google Workspace, Microsoft 365, Slack, Zoom и других, обеспечила организациям гибкость, но одновременно привела к росту атак, связанных с ошибками конфигурации, утечками доступа и недостаточной аутентификацией. Многие инциденты происходят по причине банального человеческого фактора — сотрудники забывают отключить общий доступ к файлам, используют один и тот же пароль в разных системах или не включают двухфакторную защиту. В ряде случаев атаки на облачные платформы осуществляются через уязвимости в API или утерянные ключи доступа, что позволяет злоумышленнику получить административный контроль над всей рабочей средой компании.

Таким образом, в современных условиях характер угроз меняется — от изолированных технических попыток вторжения к многоуровневым сценариям, сочетающим социальную инженерию, сетевые уязвимости и недостаточную киберграмотность пользователей. Это требует от организаций

пересмотра стратегий защиты и перехода от реактивных мер к комплексным и проактивным подходам.

В ответ на рост количества и сложности киберугроз компании начали активно внедрять современные технологии и архитектурные подходы к защите цифровой инфраструктуры. Одним из наиболее доступных и при этом эффективных инструментов остаётся многофакторная аутентификация (MFA). В отличие от традиционного пароля, который может быть перехвачен или угадан, MFA требует дополнительных факторов подтверждения личности: одноразовых кодов, биометрии, push-уведомлений или физических токенов. Это позволяет существенно снизить риск несанкционированного доступа даже в случае компрометации основного пароля. Особенно актуальна эта мера для сотрудников, получающих доступ к корпоративным ресурсам с личных или домашних устройств, где зачастую отсутствуют средства корпоративной защиты.

Более продвинутым подходом, получившим широкое распространение в последние годы, стала архитектура "нулевого доверия" (Zero Trust). Её принцип заключается в отказе от традиционной модели "периметра безопасности", где доступ внутри сети считается безопасным. В Zero Trust каждый пользователь и каждое устройство должны проходить проверку при каждом взаимодействии с системой, вне зависимости от их физического или сетевого расположения. Это особенно важно в условиях гибридной работы, когда сотрудники подключаются к системам из разных географических точек и с разных типов устройств. Внедрение Zero Trust требует значительных изменений в архитектуре ИТ-систем, включая сегментацию сетей, постоянный мониторинг поведения пользователей, контроль доступа на основе ролей и политик, а также обязательную проверку всех взаимодействий по принципу "никому не доверять по умолчанию".

Наряду с этим возрастающее значение приобретают системы мониторинга и реагирования на инциденты, основанные на искусственном интеллекте и машинном обучении. Такие решения позволяют в реальном

времени отслеживать поведение пользователей, анализировать аномалии и выявлять подозрительную активность до того, как она перерастёт в инцидент. Благодаря способности обрабатывать большие объёмы данных и выявлять сложные паттерны поведения, ИИ-системы становятся ключевым элементом проактивной защиты в условиях распределённых команд. Они способны выявить, например, нетипичный вход сотрудника из другой страны, скачивание большого объёма данных вне рабочее время или подозрительные попытки обхода политик безопасности.

Комплексная защита в условиях удалённой работы также включает использование виртуальных частных сетей (VPN), систем шифрования данных, централизованного управления устройствами (MDM), а также автоматизированных решений для резервного копирования и восстановления данных. В совокупности эти инструменты позволяют создать многослойную модель безопасности, где каждый элемент ИТ-инфраструктуры защищён независимо от других. Такой подход значительно повышает устойчивость компаний к внешним атакам и снижает потенциальные последствия внутренних инцидентов.

В условиях постоянной цифровой трансформации и ускоренного внедрения облачных технологий формируется необходимость в переходе от реактивных мер защиты к проактивным стратегиям управления рисками, интегрированным во все процессы жизненного цикла ИТ-систем. Это требует не только технических решений, но и организационных изменений — пересмотра ролей, ответственных за безопасность, внедрения новых политик доступа и постоянного обучения сотрудников.

Несмотря на техническую оснащённость современных систем кибербезопасности, человеческий фактор остаётся одной из ключевых причин успешных атак. Ошибки пользователей, неосознанные действия, доверчивость к фишинговым сообщениям и незнание базовых принципов защиты информации — всё это может свести на нет даже самые продвинутые технологические меры. В этой связи важнейшим направлением обеспечения

информационной безопасности становится систематическое обучение сотрудников. Речь идёт не только о разовых инструктажах, но о создании постоянной культуры цифровой гигиены. Эффективные программы обучения включают в себя моделирование фишинговых атак, регулярные тестирования, интерактивные курсы и обратную связь по инцидентам. Важно также адаптировать содержание таких программ под разные уровни ответственности и цифровой компетенции сотрудников: то, что нужно знать рядовому пользователю, может существенно отличаться от требований к менеджеру или разработчику.

Особое внимание вопросам кибербезопасности следует уделять руководителям цифровых проектов, которые координируют работу распределённых команд и внедрение новых решений. Их зона ответственности охватывает не только контроль над технической реализацией, но и обеспечение соответствия проекта стандартам безопасности, защита пользовательских и клиентских данных, а также реагирование на инциденты. При этом важно, чтобы управление безопасностью не воспринималось как внешняя функция, делегируемая ИТ-отделу, а стало частью повседневного управленческого процесса. Руководителям необходимо учитывать риски при выборе подрядчиков, оценивать степень защищённости облачных платформ, обеспечивать соблюдение политик доступа и проводить регулярный аудит всех используемых цифровых инструментов.

Кроме того, они должны стремиться к балансу между гибкостью и безопасностью. Чрезмерно жёсткие меры могут тормозить работу команды и вызывать сопротивление сотрудников, в то время как излишняя открытость создаёт благоприятные условия для атак. Таким образом, эффективное управление киберрисками требует не только технической осведомлённости, но и развитых управленческих компетенций, способности адаптироваться к изменяющимся условиям и понимания стратегической роли информационной безопасности в развитии цифровых продуктов.

В условиях стремительной цифровизации и перехода к распределённым моделям работы организации сталкиваются с кардинально новым ландшафтом угроз. Рост числа атак, связанных с фишингом, уязвимостями облачных сервисов, публичными сетями и использованием личных устройств, требует от компаний системного подхода к обеспечению информационной безопасности. Многоуровневая защита, основанная на принципах Zero Trust, использовании многофакторной аутентификации, мониторинге с применением ИИ и постоянном обучении сотрудников, становится неотъемлемой частью устойчивой цифровой инфраструктуры.

Особое значение приобретает вовлечённость руководства в процессы управления безопасностью, а также готовность организаций к постоянному пересмотру своих политик и стратегий в ответ на меняющуюся природу угроз. Только интеграция технических, организационных и образовательных мер позволяет выстроить эффективную систему противодействия киберугрозам в эпоху гибридной работы и глобальной взаимосвязанности.

Литература

1. Карманов А. Г., Галимов Т. А. Средства многофакторной аутентификации в современной инфраструктуре безопасности информационных систем //Информация и космос. – 2012. – №. 1. – С. 94-97.

2. Jalolov T. S. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КИБЕРБЕЗОПАСНОСТЬ В СИСТЕМАХ ПРИМЕНЯТЬ УГРОЗЫ //Advanced methods of ensuring the quality of education: problems and solutions. – 2024. – Т. 1. – №. 3. – С. 66-72.

3. Исрафилов А. Кибербезопасность в государственных структурах: стратегии защиты от кибератак //Дневник науки. – 2024. – №. 5.

4. Ахмедов Х. У. ПРЕИМУЩЕСТВА И РИСКИ ИСПОЛЬЗОВАНИЯ ОБЛАЧНЫХ ТЕХНОЛОГИЙ //Academic research in educational sciences. – 2024. – Т. 5. – №. CSPU Conference 1 Part 1. – С. 54-57.

5. Горохов А. В., Мартынов В. А., Гаврин В. А. Искусственный интеллект // Скиф. Вопросы студенческой науки. – 2022. – №. 4 (68). – С. 159-162.

Literature

1. Karmanov A. G., Galimov T. A. Means of multi-factor authentication in the modern infrastructure of information systems security //Information and Space. – 2012. – No. 1. – P. 94–97.

2. Jalolov T. S. ARTIFICIAL INTELLIGENCE CYBERSECURITY IN SYSTEMS APPLYING THREATS //Advanced methods of ensuring the quality of education: problems and solutions. – 2024. – Vol. 1. – No. 3. – P. 66–72.

3. Israfillov A. Cybersecurity in government structures: strategies for protection against cyberattacks //Science Diary. – 2024. – No. 5.

4. Akhmedov Kh. U. ADVANTAGES AND RISKS OF USING CLOUD TECHNOLOGIES //Academic research in educational sciences. – 2024. – Vol. 5. – No. CSPU Conference 1 Part 1. – P. 54–57.

5. Gorokhov A. V., Martynov V. A., Gavrin V. A. Artificial Intelligence // Scythian. Questions of Student Science. – 2022. – No. 4 (68). – P. 159–162.