СОВРЕМЕННЫЕ ТРЕНДЫ КИБЕРУГРОЗ

Световая Софья Вячеславовна, Шпырна Елизавета Григорьевна,
Научный руководитель – Перова Марина Викторовна, заведующий кафедрой информационных технологий ЮРИУ РАНХиГС
Южно-Российский институт управления – филиал РАНХиГС, г. Ростов-на-Дону

Аннотация: *киберугрозы становятся все более актуальной проблемой для организаций различных секторов, и понимание современных трендов в этой области имеет решающее значение для обеспечения безопасности данных и систем. В статье рассматриваются ключевые тенденции, которые ожидаются в ближайшие годы, включая рост числа атак на основе искусственного интеллекта, увеличение числа целевых атак на малый и средний бизнес, а также эволюцию методов социальной инженерии. Особое внимание уделяется таким новым подходам в кибербезопасности, как адаптивная защита и использование машинного обучения для обнаружения угроз. Кроме того, обсуждаются правовые и этические аспекты, связанные с киберугрозами, а также необходимость повышения осведомленности сотрудников о рисках. В статье подчеркивается, что, несмотря на усиливающиеся угрозы, компании могут эффективно противостоять им, внедряя современные технологии и формируя культуру безопасности*.
Ключевые слова: *киберугрозы, фишинг, социальная инженерия, хакерские атаки, кибербезопасность, многофакторная аутентификация, антивирусы*.

MODERN CYBER THREATS TRENDS

Svetovaya Sofia Vyacheslavovna, Shpyrna Elizaveta Grigorievna,
Scientific Supervisor – Perova Marina Viktorovna, Head of the Department of Information Technologies, South Russian Institute of Management, RANEPA Branch
South Russian Institute of Management – RANEPA Branch, Rostov-on-Don

Abstract*: Cyber threats are becoming an increasingly pressing issue for organizations across various sectors, and understanding current trends in this area is critical to ensuring the security of data and systems. This article examines key trends expected in the coming years, including the rise of artificial intelligence-based attacks, the increase in targeted attacks on small and medium businesses, and the evolution of social engineering techniques. Particular attention is paid to new approaches in cybersecurity, such as adaptive defense and the use of machine learning to detect threats. In addition, the legal and ethical aspects associated with cyber threats are discussed, as well as the need to increase employee risk awareness. The article emphasizes that despite the increasing threats, companies can effectively counter them by implementing modern technologies and forming a security culture.*
Keywords: *cyber threats, phishing, social engineering, hacker attacks, cybersecurity, multi-factor authentication, antiviruses.*

В современном мире кибербезопасность стала одной из ключевых областей для защиты данных и инфраструктуры в условиях быстрого развития технологий. Из-за перехода на цифровые технологии во всем мире кибербезопасность создает новые возможности и риски, связанные с киберугрозами.

Киберугрозы сегодня представляют серьезную опасность для цифрового мира. Развитие технологий и повсеместное внедрение интернета привели к тому, что информация и цифровые системы становятся уязвимыми для атак злоумышленников. Киберугрозы принимают различные формы и требуют от стран не только технологических решений, но и комплексного подхода к обеспечению безопасности. В Российской Федерации используются нормативно правовые акты, необходимые для защиты персональных данных, регулирования деятельности IT-специалистов, а также обеспечения безопасности деятельности как индивидов, так и организаций в информационной сети. [1]

Основу нормативно-правовой базы цифровизации составляют законы, регулирующие информационные технологии и защищающие от киберугроз.

1.Закон Российской Федерации 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

2.Указ Президента России 2013г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ»

За 2024 год число атак шифровальщиков выросло на 44%, а прогосударственных киберпреступных APT-группировок, которые атакуют цели в России, — почти в два раза. При этом в 10% подобных инцидентов целью киберпреступников был не выкуп, а диверсия для нанесения максимального ущерба жертве, отметили в F.A.C.C.T [2]

Рост числа кибератак напрямую связан с несколькими факторами:

1.Увеличение числа устройств и сетей. Чем больше устройств подключено к интернету, тем больше возможностей для взлома.

2.Сложные цифровые технологии. Современные системы создаются с высокой степенью интеграции, что часто приводит к появлению уязвимостей.

3.Расцвет киберпреступности. Хакерские инструменты и услуги стали доступны на теневом рынке, что позволяет совершать атаки даже неподготовленным пользователям.

4.Удаленный формат работы. Переход на дистанционную занятость усилил проблемы с безопасностью из-за слабой защиты домашних сетей.

5.Ошибка человеческого фактора. Низкий уровень цифровой грамотности пользователей часто становится причиной успешных атак через фишинг и обман.

Таким образом, в условиях растущего числа угроз вопросы кибербезопасности требуют особого внимания. Без эффективных мер защиты риски потери данных и финансовых ресурсов будут только увеличиваться.

Эксперты «Лаборатории Касперского» отмечают увеличение атак с использованием ransomware [3]. Ransomware остается одной из наиболее опасных угроз, при которой злоумышленники блокируют доступ к данным и требуют выкуп за их восстановление. Ожидается, что количество таких атак продолжит расти по следующим причинам: Автоматизация процессов и распространение готовых инструментов для создания вредоносного ПО. Фокус на облачные хранилища и корпоративные сети, особенно с удаленным доступом. Целевая направленность атак на крупные компании и критически важные системы с высокой стоимостью потерь.

Способы защиты от ransomware:

- Регулярное резервирование данных на автономных носителях.
- Своевременное обновление программного обеспечения и устранение уязвимостей.
- Многофакторная аутентификация для защиты доступа.

•Обучение сотрудников правилам безопасности для предотвращения фишинга.

•Использование современных антивирусных программ и систем обнаружения вторжений.

Аналитики «TADVISER» акцентируют внимание на увеличении атак на критически важную инфраструктуру [4]. Объекты критической инфраструктуры, такие как энергетика, транспорт, медицина и связь, становятся все более уязвимыми для кибератак. Популярность таких атак обусловлена:

•Зависимостью общества от ключевых систем, где сбой может привести к серьезным последствиям.

•Политическими и экономическими целями, когда атаки используются для шантажа или давления.

•Устаревшими системами, не способными противостоять современным угрозам.

Меры защиты инфраструктуры:

•Модернизация оборудования и внедрение продвинутых средств безопасности.

•Создание резервных каналов и резервных копий критически важных данных.

•Постоянный мониторинг сетей и оперативное реагирование на подозрительные действия.

Руководитель исследовательской группы отдела аналитики ИБ «Positive Technologies» Ирина Зиновкина также отмечает фишинг и социальную инженерию [5]. Фишинг остается одним из самых распространенных методов атак, направленных на человеческий фактор. Доля рассылок фишинговых писем в общем количестве киберпреступлений составила 69%. В первой половине 2024 года самым популярным оказалось шпионское ПО AgentTesla, а после его ликвидации — FormbookFormgrabber, инструмент для кражи учетных записей и персональных данных, а также загрузчик CloudEyE. «Киберпреступники практически отказались от использования ссылок для доставки вредоносного ПО. В 82% вредоносных писем получатели увидят во вложении архив, содержащий вредоносное вложение, чаще всего в виде исполняемого файла», — предупредили в компании.

Современные техники становятся все более сложными:

•Spear-phishing – точечные атаки на конкретных сотрудников с использованием персонализированных писем.

•Vishing – мошеннические звонки для получения конфиденциальной информации.

•Smishing – распространение вредоносных ссылок через SMS-сообщения.

•Deepfake – создание поддельных аудио- и видеоматериалов для введения в заблуждение.

Методы защиты от фишинга:

•Использование почтовых сервисов с продвинутыми фильтрами спама.

•Регулярное обучение сотрудников по выявлению подозрительных писем и сообщений.

•Проверка ссылок и вложений перед их открытием.

•Внедрение многофакторной аутентификации для защиты учетных записей.

Компания «Anti-Malware» составила прогнозы на 2025 год [6]. Ожидается рост атак на критическую информационную инфраструктуру, увеличения фишинговых атак, направленных на многослойную аутентификацию, а также появление новых мошеннических схем.

Согласно прогнозам, увеличится число атак на мобильные устройства и способов обхода многофакторной аутентификации. Использование AI в кибератаках уже стало нормой, и следующие годы могут принести новые, более изощренные методы нападений, включая автоматизацию фишинга и создание глубоко фальсифицированных визуальных материалов.

С каждым годом мы видим, как киберпреступность адаптируется к новым условиям. Поэтому бизнесам, особенно малому и среднему, необходимо инвестировать не только в традиционные меры защиты, но и в новые технологии кибербезопасности. А цифровая грамотность сотрудников компании становится необходимым условием для сопротивления киберугрозам.

Эксперты «Лаборатории Касперского» предлагают следующие меры по защите от киберугроз: [7]

1.Обучение и повышение осведомленности пользователей

Основная причина большинства кибератак – человеческая ошибка, поэтому важно:

•Проводить практические тесты, чтобы оценить готовность сотрудников к потенциальным атакам.

•Регулярно проводить тренинги по кибербезопасности для сотрудников.

•Обучать распознаванию фишинга, подозрительных ссылок и писем.

•Знакомить персонал с новыми видами угроз, включая социальную инженерию и поддельные видео (deepfake).

2.Технические меры защиты

Технические решения обеспечивают базовый уровень безопасности:

•Антивирусы и фаерволы – защита от вредоносного ПО и несанкционированного доступа.

•Многофакторная аутентификация (MFA) – дополнительная проверка для повышения безопасности доступа.

•Своевременные обновления программного обеспечения – устранение уязвимостей до их использования злоумышленниками.

•Мониторинг и обнаружение угроз – внедрение систем для контроля трафика и обнаружения подозрительных активностей.

•Резервное копирование данных – регулярное создание копий информации для восстановления в случае атаки.

3.Организационные меры и правила безопасности

Эффективная защита требует четкой организации процессов и контроля:

•Разработка и внедрение внутренних политик безопасности с четкими правилами работы с корпоративной информацией.

•Ограничение прав доступа сотрудников, чтобы каждый пользователь имел доступ только к необходимым данным и ресурсам.

•Периодическое проведение аудитов безопасности и тестов на проникновение (пентестов).

•Подготовка плана реагирования на инциденты для оперативного устранения последствий атак.

•Организация безопасного удаленного доступа через VPN и использование защищенных корпоративных устройств.

Комплексный подход к защите, сочетающий осведомленность персонала, технические инструменты и организационную дисциплину, позволит значительно снизить риски кибератак и защитить критически важные данные.

В последние годы разнообразие и сложность киберугроз значительно возросли, что заставляет как организации, так и пользователей уделять больше внимания вопросам защиты информации. Увеличение частоты кибератак и усовершенствование инструментов злоумышленников, включая технологии искусственного интеллекта и Интернета вещей, создают новые вызовы для обеспечения безопасности данных.

Понимание современных тенденций в области киберугроз помогает заранее выявлять потенциальные риски и разрабатывать действенные способы защиты. Организациям необходимо реализовывать комплексные подходы к безопасности, включая обучение сотрудников, применение новейших технологий защиты и регулярное обновление информационных систем.

Кроме того, ключевым фактором в формировании безопасной цифровой среды является коллаборация между государственными учреждениями и частным сектором. Постоянный мониторинг и оценка угроз позволяют эффективно реагировать на изменения и смягчать последствия кибератак.

В конечном счете поддержание безопасного цифрового пространства зависит от уровня осведомленности и готовности к действию участников процесса. Осознание современных угроз и применение лучших практик в кибербезопасности помогут успешно справиться с вызовами нашего времени.

Список литературы:

1.Гранкина А. Я., Баймедетов С. Д. Кибербезопасность в современном мире: Актуальные угрозы и методы защиты. //Международный научный журнал «Вестник Науки». 2024. – Том 1, №11(80). – С. 864-870.

2.Эксперты F.A.C.C.T. назвали основные киберугрозы 2024 года. - 2024. – [Электронный ресурс] - Режим доступа: https://www.rbc.ru/technology_and_media/16/12/2024/675ed7419a79475fb7eb1cb3 (дата обращения 17.12.2024)

3.Распознавание программ-вымогателей (ransomware): чем отличаются трояны-шифровальщики. - 2024. – [Электронный ресурс] - Режим доступа: https://www.kaspersky.ru/resource-center/threats/ransomware-attacks-and-types (дата обращения 17.12.2024)

4.Кибератаки на критическую информационную инфраструктуру. - 2023. – [Электронный ресурс] - Режим доступа: http://surl.li/yiiyqc (дата обращения 17.12.2024)

5.Кибербезопасность в 2023–2024 гг.: тренды и прогнозы. Часть четвертая. - 2024. – [Электронный ресурс] - Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-chetvertaya/ (дата обращения 17.12.2024)

6.Прогноз развития киберугроз и средств защиты информации — 2024. – [Электронный ресурс] - Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/2024-Forecast (дата обращения 17.12.2024)

7.Защита от киберугроз. - 2024. – [Электронный ресурс] - Режим доступа: https://content.kaspersky-labs.com/se/media/ru/business-security/Kaspersky_Threat_Protection_Datasheet_RU.pdf (дата обращения 17.12.2024)