Анализ актуальности и состояния современных фишинг-атак на объекты критической информационной инфраструктуры

В.В. Селиверстов[1], *С.А. Корчагин*[2]

[1]*Саратовский государственный технический университет имени Гагарина Ю.А., Саратов*
[2]*Финансовый университет при Правительстве Российской Федерации, Москва*

Аннотация: В статье проводится анализ актуальности и состояния современных фишинг-атак на объекты критической информационной инфраструктуры (ОКИИ). Фишинг, как один из наиболее распространенных видов кибератак, представляет серьезную угрозу для безопасности информационных систем и данных. Целью исследования является выявление основных характеристик и тактик фишинг-атак, а также оценка уровня защищенности ОКИИ от данного типа угроз. В ходе исследования используются данные о последних трендах и методах фишинга, собранные из различных источников, включая отчеты по кибербезопасности, статистику инцидентов и анализ случаев успешных атак. Основное внимание уделяется анализу целевых объектов фишинг-атак в контексте их значимости для обеспечения непрерывной работы критической информационной инфраструктуры. На основе проведенного анализа формулируются рекомендации по улучшению систем защиты от фишинг-атак для объектов критической информационной инфраструктуры. Цель данного исследования заключается в повышении информированности у специалистов в области кибербезопасности и разработчиков политики безопасности о возникающих рисках фишинга. Кроме того, основной задачей является обеспечение эффективной защиты информационных ресурсов, которые являются неотъемлемой частью функционирования критической инфраструктуры.
Ключевые слова: информационная безопасность, фишинг-атаки, информационная инфраструктура, математическое моделирование, программный комплекс.

Введение

В современной эпохе цифровой реальности, когда интернет проникает во все сферы нашей повседневной жизни, фишинговые атаки продолжают оставаться одной из основных угроз информационной безопасности. Эти атаки сочетают в себе эффективную комбинацию социальной инженерии и технических инноваций, которые не только угрожают конфиденциальности данных, но и подрывают доверие пользователей к цифровым системам. Фишинговые атаки являются серьезной проблемой, требующей постоянного внимания и защиты со стороны пользователей и организаций [1].

С каждым годом фишинговые атаки становятся все более хитроумными и тонкими, проникая в самые защищенные сферы [2, 3]. Эта

эволюция требует постоянного обновления и улучшения мер безопасности, а также более глубокого понимания их сути.

Анализ тенденций фишинга становится необходимым инструментом для понимания его эволюции и прогнозирования будущих угроз. Это позволяет специалистам по кибербезопасности разрабатывать более точные и адаптивные стратегии защиты, которые могут эффективно противодействовать всем аспектам фишинговых атак.

Как и ведущие компании, такие как Positive Technologies, Group-IB, APWG, DMARC и другие, регулярно предоставляют комплексную статистику о современных киберугрозах [4-6], необходимо постоянно проводить анализ и адаптироваться к новым методам фишинга, уделяя особое внимание методам социальной инженерии, которые остаются наиболее эффективными из-за уязвимости человеческого фактора.

Однако, помимо технологических решений, существенное внимание следует уделить и образованию пользователей. Повышение киберграмотности становится краеугольным камнем в обеспечении безопасного цифрового пространства. Это не только уменьшает вероятность попадания под атаку, но и содействует созданию более осознанной и ответственной культуры онлайн-безопасности.

Анализ объема фишинговых атак в критических информационных инфраструктурах

В результате анализа данных, опубликованных компанией Group-IB [7], проведенного с целью изучения роста числа фишинговых сайтов в российском сегменте интернета, было установлено, что в 2022 году было выявлено и заблокировано более 59 000 таких сайтов, из которых около 7000 были нацелены на российских пользователей. Этот показатель в два раза

превысил аналогичный показатель предыдущего года, что указывает на увеличение угрозы фишинговых атак в российском интернет-сегменте.

При рассмотрении данных за 2021 год можно заметить, что количество заблокированных ресурсов CERT-GIB составило около 32 000 [8]. В то же время, в 2022 году это число возросло до 60 000 [9]. Фишинговые страницы включали в себя подделки известных брендов, сервисов и игр, которые пользуются популярностью среди российских пользователей. Наблюдается более чем вдвое увеличение числа заблокированных страниц в зонах .ru и .рф, с 3 000 до 7 000. Специалисты CERT-GIB за 2022 год обнаружили около 20 000 фишинговых доменов в зонах .ru и .рф (в 2021 году их число составляло около 16 000).

Что касается глобальных тенденций, то в 2022 году APWG зафиксировала около 4,7 миллиона фишинговых атак. С 2019 года наблюдается ежегодное увеличение числа атак более чем на 150%.

На рисунке 1 приводится распределение объема фишинговых атак в период с 2019 по 2023 гг.

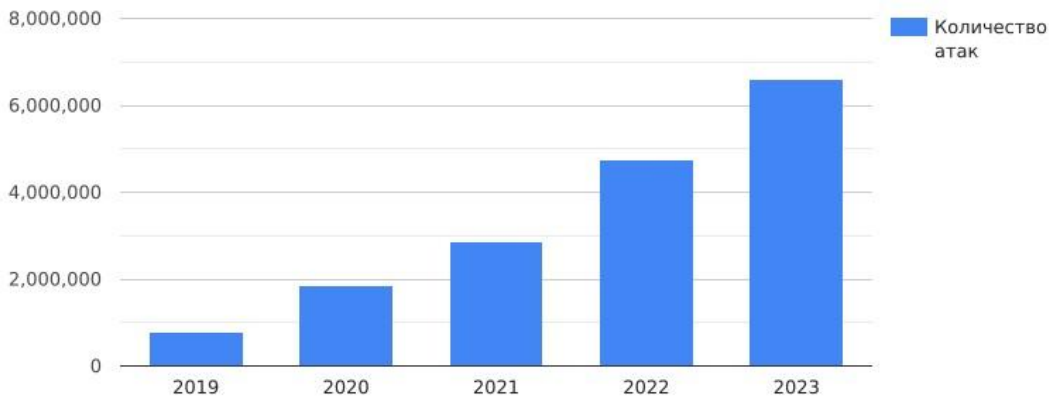

Рис. 1. – Объем фишинговых атак в период с 2019 по 2023 гг.

По данным DMARC, Нидерланды подверглись наибольшему количеству фишинговых атак в 2022 году (17,7% всех атак). За ними следуют Россия, Молдавия, США и Таиланд [10].

На рисунке 2 приводится распределение объема фишинговых атак по странам в период с 2019 по 2023 гг.

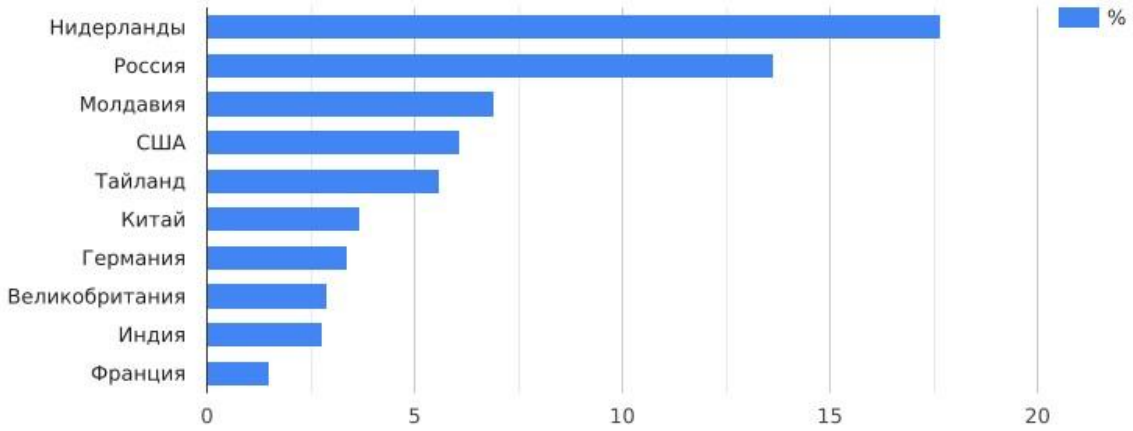

Рис. 2. – Объем фишинговых атак по странам в период с 2019 по 2023 гг.

В первой половине 2023 года на конечных точках, отслеживаемых Acronis, количество файлов и URL-адресов в каждом сканированном электронном письме выросло на 15 %. Киберпреступники также воспользовались возможностями растущего рынка искусственного интеллекта, основанного на больших языковых моделях (LLM), для разработки и использования платформ, позволяющих автоматизировать, масштабировать и усовершенствовать новые методы атак путем активного обучения.

Анализ целевых секторов фишинговых атак в критических информационных инфраструктурах

Во временной промежуток с третьего квартала 2022 года по третий квартал 2023 года было отмечено значительное количество фишинговых атак с использованием социальной инженерии в различных отраслях.

В результате проведенного анализа, топ отрасли, наиболее подверженные таким атакам, были идентифицированы на рисунке 3.

Финансовые учреждения занимают первое место, с 44% всех зарегистрированных атак. На втором месте расположились оборонно-промышленные предприятия, с 19% атак, и на третьем месте находятся научные и образовательные организации, с 17% атак.

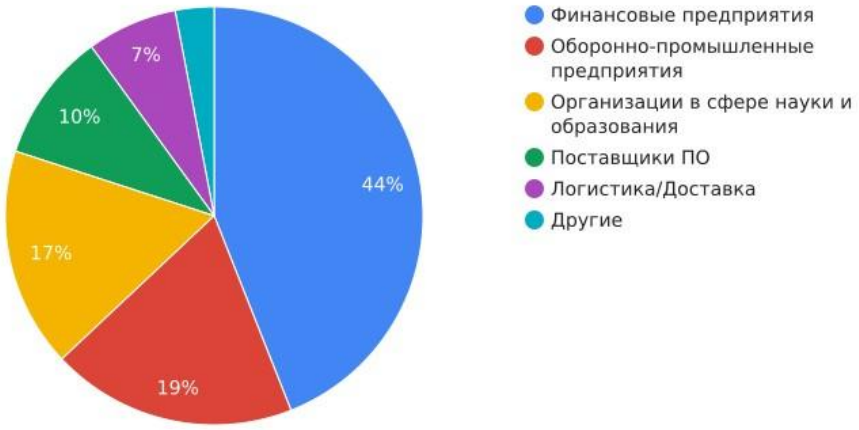

Рис. 3. – Целевые сектора КИИ фишинговых атак.

В 2023 году было зафиксировано значительное количество успешных атак на организации с использованием социальной инженерии. Почти половина (43%) всех таких атак была осуществлена с помощью различных коммуникационных средств, включая электронную почту, СМС-сообщения,

социальные сети и мессенджеры [11]. Эти данные подтверждают эффективность фишинговых атак, которые представляют серьезные угрозы для организаций, как с точки зрения репутационных рисков, так и финансового ущерба.

Атаки, основанные на социальной инженерии, представляют собой утонченные механизмы манипуляции и обмана, которые виртуозно используют различные коммуникационные каналы для проникновения в системы организаций. Особенно примечательно, что 79% таких атак были осуществлены через электронную почту, СМС-сообщения, социальные сети и мессенджеры. Злоумышленники активно используют эти платформы для обмана и получения нежелательного доступа к конфиденциальным данным и системам организаций.

Такие фишинговые атаки не только могут причинить серьезный финансовый ущерб, но и имеют потенциал нанести значительный ущерб репутации организаций. Это связано с возможностью несанкционированного доступа к конфиденциальным данным, финансовым средствам и частной информации клиентов. Главной целью таких атак является получение данных, что составляет около 85% всех фишинговых инцидентов. Это подчеркивает важность защиты конфиденциальной информации и необходимость принятия соответствующих мер для предотвращения таких атак.

Анализ финансовых потерь из-за фишинговых атак в критических информационных инфраструктурах

В докладе IBM о стоимости утечек данных за 2023 год отмечается, что средняя глобальная стоимость утечек данных из-за фишинга составляет 4,76 миллиона долларов [12].

В соответствии с последним отчетом Федерального Бюро Расследований (ФБР), атаки, связанные с компрометацией учетных записей электронной почты (BEC), представляют собой наиболее распространенную и дорогостоящую форму киберпреступности.

По данным ФБР, предприятия в результате таких атак потеряли более 2,7 миллиарда долларов, что на 300 миллионов долларов больше, чем в предыдущем году.

Атаки BEC характеризуются манипуляцией и компрометацией учетных записей электронной почты в целях мошенничества и получения незаконного доступа к финансовым ресурсам предприятий. Эти атаки могут включать поддельные запросы на перевод денежных средств, изменение банковских реквизитов и другие махинации, направленные на обман и финансовое преступление. Результаты последнего отчета ФБР указывают на то, что атаки BEC остаются важным и серьезным вызовом для организаций, приносящим значительные финансовые потери. Следует отметить, что это заявленные потери, и большинство из них остается незарегистрированным.

Исследование, проведенное IBM и Ponemon в 2023 году, сообщает, что нарушения BEC обходятся в среднем в 4,67 миллиона долларов, а для их обнаружения и сдерживания требуется 266 дней. Время играет решающую роль при обнаружении: нарушения, устранение которых занимает более 200 дней, обходятся на 1,02 миллиона долларов дороже, чем те, что устранены менее чем за 200 дней.

По данным Harvard Business Review: стоимость акций публично торгуемых компаний снизилась на 7,5% после утечки данных, а средняя потеря рыночной капитализации составила 5,4 миллиарда долларов [13]. В среднем компании затрачивают 46 дней на восстановление цен своих акций до уровня, существовавшего до инцидента, если вообще могут это сделать.

В статье HBR также отмечается, что 60% организаций, столкнувшихся с утечкой данных, повысили цены на свою продукцию, и потери испытывают клиенты, а не только акционеры. В среднем, компании, столкнувшиеся с серьезным инцидентом утечки данных, отстают от индекса NASDAQ на 8,6% через год, и этот разрыв может увеличиться до 11,9% через два года.

Популярный способ фишинговых атак в критических информационных инфраструктурах

Электронная почта продолжает оставаться основным каналом для распространения фишинговых сообщений (92%), однако наблюдается возрастающая популярность мессенджеров и социальных сетей в качестве альтернативных каналов для проведения фишинговых атак. Для приоритетной доставки вредоносных нагрузок с использованием вложений наиболее часто применяются архивы (37%) и текстовые документы (30%). Фишинговые ссылки часто направляют пользователей на поддельные страницы для ввода личной информации (50%) [14].

Анализ показывает, что 91% фишинговых писем отправляются через учетные записи Gmail. Популярность Gmail среди злоумышленников обусловлена возможностью создания большого количества учетных записей быстро и бесплатно, а также наличием встроенной функции Google "уведомлений о прочтении".

За первую половину 2023 года количество фишинговых атак по электронной почте возросло на 464%. В первом квартале 2023 года 30,3% всех полученных электронных писем оказались спамом, в то время как 1,3% содержали вредоносное ПО или фишинговые ссылки [15].

На рисунке 4 приводится рейтинг кликов и переходов по фишинговым письмам по различным секторам критически важной инфраструктуры.

В фишинговых сообщениях злоумышленники активно прибегают к маскировке своей личности, представляя себя в различных ролях. Согласно статистике, в наибольшей степени они выдают себя за контрагентов (26%), специалистов технической поддержки или ИТ (15%) и представителей государственных органов (13%).

Рис. 4. – Рейтинг переходов по фишинговым письмам по секторам.

Прогнозы

Социальные инженерные методы остаются предпочтительным выбором для злоумышленников, которые нацелены на сотрудников компаний, и в последние годы наблюдается увеличение сложности их фишинговых атак. В эпоху генеративного искусственного интеллекта этот тренд усиливается, что подтверждается ростом количества фишинговых атак на 1265% в 2023 году, по данным компании SlashNext Inc. Следует отметить, что большинство тематик фишинга остаются неизменными с течением времени, при этом злоумышленники лишь обновляют детали и адаптируются к изменениям в технологическом ландшафте.

Угроза фишинга продолжает нарастать с использованием новых инструментов и методов, включая искусственный интеллект, фишинг QR-кодов и атаки вроде AitM. Использование больших языковых моделей, таких как ChatGPT, позволяет создавать более убедительные фишинговые сообщения в масштабах, что подтверждается ростом атак.

Искусственный интеллект не только снижает технические барьеры для проведения атак, но также может быть использовано для защиты от сложных угроз, что подчеркивает важность подготовки и принятия соответствующих мер безопасности. Прогнозируя развитие фишинга в период с 2024 по 2025 год, можно выделить несколько ключевых тенденций:

- Атаки станут более изощренными, особенно с использованием инструментов на базе искусственного интеллекта, что позволит злоумышленникам проводить более эффективные и убедительные атаки.
- Появится новое семейство вредоносных программ, заменяющее Qakbot.
- Злоумышленники будут активно использовать менее распространенные языки программирования, такие как Golang и Rust, для избежания обнаружения.

Заключение

В заключение, анализ утечек данных и фишинговых атак за период 2020-2023 года показывает, что это остается одним из самых серьезных вызовов для информационной безопасности как для компаний, так и для частных лиц. Средняя глобальная стоимость утечек данных из-за фишинга продолжает расти, а атаки BEC особенно вредоносны и дорогостоящи. Однако не все потери от фишинговых атак можно измерить в денежных единицах. Утечки данных приводят не только к финансовым потерям

компаний, но и к потере доверия пользователей, повреждению репутации и другим негативным последствиям.

Технические инновации, такие как искусственный интеллект и большие языковые модели, усиливают эффективность фишинговых атак, делая их более сложными и убедительными. Это требует постоянного обновления мер безопасности и повышения киберграмотности пользователей.

В будущем периоде с 2024 по 2025 год можно ожидать усиления фишинговых атак, которые станут еще более изощренными и эффективными.

Для эффективной борьбы с фишингом необходимо внедрение комплексного подхода, который включает в себя как технические меры безопасности, так и обучение пользователей. Повышение осведомленности о рисках и применение передовых методов обнаружения и предотвращения атак помогут сократить уязвимости и защитить цифровые системы от вредоносных действий.

Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситета

Литература

1. Schneider, F. W. et al. Phishing in the Age of Social Media: A Study of the Cybercrime Landscape. // Journal of Cybersecurity Research. – 2018. – Vol. 5, No. 2. – pp. 112-125.
2. Miller, J. R. The Evolution of Phishing Attacks: Trends and Countermeasures. //International Journal of Information Security. – 2019. – Vol. 12, No. 4. – pp. 287-301.
3. Wong, L. H. Phishing Techniques and Strategies: An In-depth Analysis. //Cybersecurity Review. – 2020. – Vol. 8, No. 1.

4. Chen, S. et al. Behavioral Analysis of Phishing Emails: A Machine Learning Approach. //Journal of Computer Security. – 2021. – Vol. 15, No. 3. – pp. 201-215.
5. Беспалова Н.В., Корчагин С.А., Сердечный Д.В., Селиверстов В.В. Анализ зарубежного опыта применения интеллектуальных методов в задачах защиты объектов критической информационной инфраструктуры финансового сектора // Инженерный вестник Дона, 2024, №5. URL: ivdon.ru/magazine/archive/n5y2024/9196
6. Корчагин С.А., Сердечный Д.В., Раздьяконов Е.С., Беспалова Н.В Разработка концепции обеспечения безопасности критической инфраструктуры финансового сектора // Инженерный вестник Дона, 2024, №4. URL: ivdon.ru/magazine/archive/n4y2024/9176
7. Garcia, M. A. Phishing Resilience in Corporate Environments: A Case Study. //Journal of Information Systems Security. – 2022. – Vol. 7, No. 2. – pp. 88-95.
8. Kim, J. H. Psychological Factors Influencing Phishing Susceptibility: A Meta-analysis. //Journal of Cyberpsychology, Behavior, and Social Networking. – 2022. – Vol. 10, No. 4. – pp. 511-520.
9. Smith, R. E. Phishing Trends in E-commerce: Implications for Online Security. //International Journal of Electronic Commerce. – 2023. – Vol. 18, No. 1. – pp. 45-52.
10. Liu, Q. et al. Machine Learning Approaches for Phishing Detection: A Comparative Study. //Journal of Information Technology Research. – 2023. – Vol. 9, No. 3. – pp. 511-525.
11. Wang, Y. H. Social Engineering Tactics in Phishing Attacks: An Analysis of Recent Cases. //Journal of Computer Crime Investigation. – 2023. – Vol. 14, No. 2. – pp. 76-83.

12. Anderson, K. R. Legal Implications of Phishing: A Comparative Review of International Laws. //Journal of Cyber Law and Policy. – 2023. – Vol. 5, No. 4. – pp. 269-273.
13. Gonzalez, A. M. Phishing Awareness Training Effectiveness: A Longitudinal Study. //Journal of Information Security Education. – 2023. – Vol. 11, No. 1. – pp. 155-162.
14. Lee, C. Y. Phishing Attacks on Mobile Devices: Vulnerabilities and Countermeasures. //Journal of Mobile Security. – 2023. – Vol. 6, No. 3. – pp. 201-215.
15. Ramirez, D. P. Phishing Scams Targeting Financial Institutions: A Case Analysis. //Journal of Financial Crime. – 2023. – Vol. 13, No. 2. – pp. 145-152.

References

1. Schneider, F. W. Journal of Cybersecurity Research, 2018, Vol. 5, No. 2 pp. 112-125.
2. Miller, J. R. International Journal of Information Security, 2019, Vol. 12, No. 4. pp. 287-301.
3. Wong, L. H. Cybersecurity Review, 2020, Vol. 8, No. 1.
4. Chen, S. et al. Journal of Computer Security, 2021, Vol. 15, No. 3. pp. 201-215.
5. Bespalova N.V., Korchagin S.A., Serdechnyj D.V., Seliverstov V.V. Inzhenernyj vestnik Dona, 2024, №5. URL: ivdon.ru/ru/magazine/archive/n5y2024/9196
6. Korchagin S.A., Serdechnyj D.V., Razd'jakonov E.S., Bespalova N.V. Inzhenernyj vestnik Dona, 2024, №4. URL: ivdon.ru/ru/magazine/archive/n4y2024/9176
7. Garcia, M. A. Journal of Information Systems Security, 2022, Vol. 7, No. 2. pp. 88-95.

8. Kim, J. H. Journal of Cyberpsychology, Behavior, and Social Networking, 2022, Vol. 10, No. 4. pp. 511-520.
9. Smith, R. E. International Journal of Electronic Commerce, 2023, Vol. 18, No. 1. pp. 45-52.
10. Liu, Q. Journal of Information Technology Research, 2023, Vol. 9, No. 3. pp. 511-525.
11. Wang, Y. H. Journal of Computer Crime Investigation, 2023, Vol. 14, No. 2. pp. 76-83.
12. Anderson, K. R. Journal of Cyber Law and Policy, 2023, Vol. 5, No. 4. pp. 269-273.
13. Gonzalez, A. M. Journal of Information Security Education, 2023, Vol. 11, No. 1. pp. 155-162.
14. Lee, C. Y. Journal of Mobile Security, 2023, Vol. 6, No. 3. pp. 201-215.
15. Ramirez, D. P. Journal of Financial Crime, 2023, Vol. 13, No. 2. pp. 145-152.

Дата поступления: 16.04.2024

Дата публикации: 30.05.2024