УДК 338.242

МОШЕННИЧЕСТВО И ФИШИНГ КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ

Э.Н. Воронько
Г. А. Кушов, *студент, 1 курс*
Полоцкий государственный университет имени Евфросинии Полоцкой, Беларусь

В статье исследуется феномен фишинга в контексте экономической безопасности предприятий. Актуальность темы обусловлена экспоненциальным ростом числа атак и их качественной трансформацией за счет применения AI, что позволяет злоумышленникам проводить масштабные и персонализированные кампании. На основе анализа современных источников выделены ключевые тенденции: целевые отрасли, структура последствий и страны-источники фишинга. В работе систематизируются и детализируются меры противодействия, подтверждая, что стратегия защиты должна быть комплексной и включать три основных компонента: технологический (программные решения), организационный (регламенты и политики) и человеческий (повышение осведомленности и регулярное тестирование).

Ключевые слова*: фишинг, мошенничество, экономическая безопасность, угроза предприятий.*

Экономическая безопасность – компонент антикризисного управления экономикой. Экономические кризисы разной глубины и продолжительности – это следствие любой многоукладной экономики. Кризисы могут выражаться в растущем разрыве между спросом и предложением, обесценении денег, росте стоимости жизни, безработице, т.е. в ухудшении макроэкономических показателей [1].

В течение последних лет из-за взломов банковских карт граждане потеряли несколько десятков миллионов рублей. Этому виной в основном пренебрежительное отношение людей к безопасности распространяемых ими в Интернете данных. А ведь именно получение конфиденциальных данных является целью популярного в настоящее время метода мошенничества – фишинга [2].

Фишинг (англ. phishing, от phone phreaking «взлом телефонных автоматов» и fishing – «рыбная ловля») - получение с помощью обмана или методов социальной инженерии конфиденциальных данных с целью использования в корыстных, преступных целях [2].

Используя фишинг, преступники применяют, например, массовую рассылку на электронные почты пользователей. В письмах содержаться ссылки, ведущие на вредоносные сайты. В основном это подделки общеизвестных соцсетей, маркетплейсов, онлайн-магазинов. На вышеупомянутых страницах содержаться формы для введения реквизитов банковских карт, логинов и паролей, которые, в случае заполнения, передаются злоумышленникам для получения доступа к денежным средствам пользователей [2].

С помощью фишинга преступники могут получать не только личные данные пользователей, но и корпоративную информацию нежелательную для общего разглашения.

В последнее время количество успешных фишинговых увеличивается в связи со стремительным развитием искусственного интеллекта. С его использованием злоумышленники могут массово создавать персонализированные письма, а также копировать голос и в некоторых случаях даже видео с доверенными лицами для убеждения пользователей.

По данным исследования компании Positive Technologies количество фишинговых атак в 2024 году выросло на 33% по сравнению с 2023 годом, а с 2022 годом – на 72% [3].

Атаки направлены на все отрасли экономики, но самыми популярными у злоумышленников в 2024 году были следующие отрасли: государственные учреждения, промышленные предприятия и IT-компании. Их процентное соотношение представлено на рисунке 1.

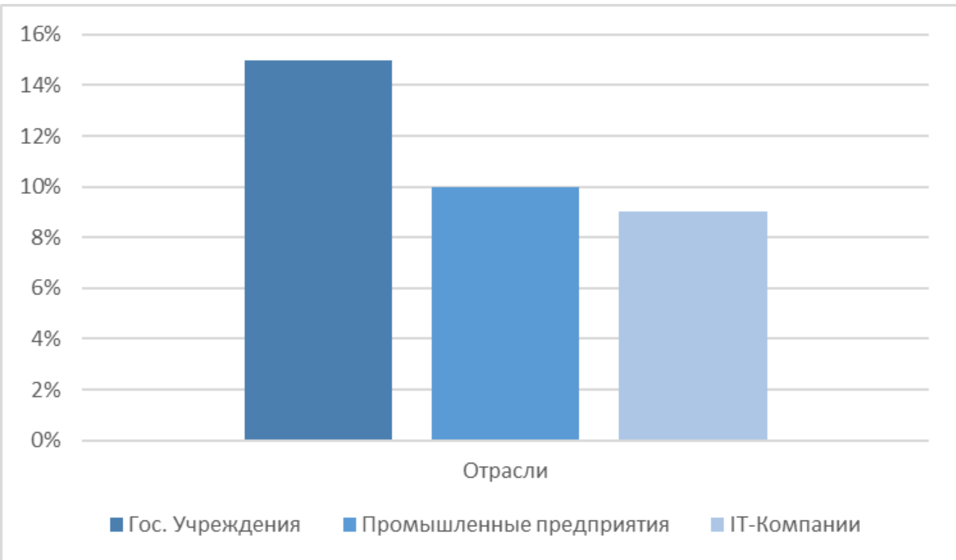

Рисунок 1. – Самые популярные отрасли среди фишинговых атак [3]

Фишинговые атаки в 63% случаев приводят к краже конфиденциальной информации, в 28% случаев к нарушению деятельности организаций, в 6% к ущербу интересам государства, и в 5% случаев к прямым финансовым потерям [3].

По информации компании AAG IT большая часть фишинговых атак приходится на атаки из России, далее идет Германия, США, Китай и Нидерланды [4].

Доля каждой страны представлена ниже (рисунок 2).

Проведенное исследование позволяет сделать выводы, подтверждающие значительную угрозу, которую фишинг представляет для экономической безопасности предприятий и организаций. В настоящее время компании применяют различные меры по борьбе с фишингом, которые включают в себя стратегии, методы и технологии, способствующие защите пользователей от фишинговых атак. Они направлены на обнаружение, блокирование и смягчение последствий различных видов фишинга, одновременно повышая осведомленность как технических, так и нетехнических специалистов.

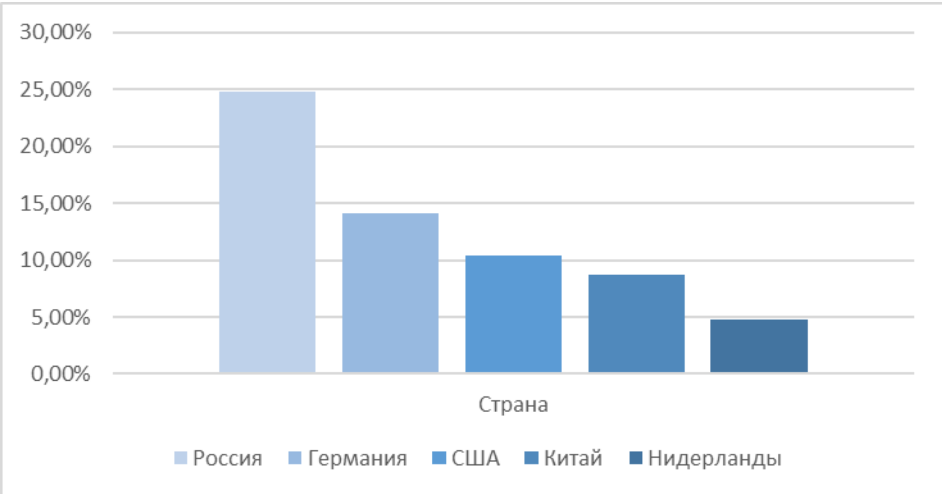

Рисунок 2. – Структура стран-отправителей фишинговых атак [4]

Приведенные в статье данные наглядно демонстрируют масштаб проблем в этой сфере. В связи с этим возникает необходимость выработки управляющих воздействий по противодействию фишингу, которые не могут ограничиваться лишь техническими мерами защиты. Основным методом по борьбе с фишингом в компаниях является осведомление всех сотрудников и их регулярная проверка. Также применяются автоматические системы, которые отмечают подозрительные письма и сообщения и в крупных компаниях могут отправлять их в отдел безопасности для принятия дальнейших решений.

Таким образом, обеспечение экономической безопасности в современных условиях требует от предприятий и организаций формирования целостной системы защиты, где технические решения и организационные меры должны усиливаться за счет высокого уровня осведомленности и ответственности каждого сотрудника.

Список использованных источников

1. Экономическая безопасность : учебник / Н. Д. Эриашвили, Т. Н. Агапова, С. С. Маилян [и др.] ; под науч. ред. В. С. Осипова, Н. Д. Эриашвили ; под общ. ред. А. Е. Суглобова, Т. Н. Агаповой. – 4-е изд., перераб. и доп. – Москва : Юнити-Дана, 2023. – 480 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=712619.
2. Мишнева, Д. А. Фишинг как новый способ мошенничества в интернете: проблемы квалификации и методы защиты / Д. А. Мишнева, И.А. Подройкина // Экономика, политика, право: актуальные вопросы, тенденции и перспективы развития : материалы XX Международной научно-практической онлайн-конференции молодых ученых, студентов, аспирантов, преподавателей вузов, 25 ноября 2022 г. / В. К. Аверин, Н. С. Аверичев, Ю. С. Аверичев [и др.] ; редкол.: А. М. Шевченко, Н. Н. Дунаева, О. И. Карепина, Е. Ю. Коруненко [и др.]. – Ростов-на-Дону : Издательско-полиграфический комплекс РГЭУ (РИНХ), 2022. – 177 с.
3. Positive Technologies. Количество фишинговых атак выросло на треть за год // Positive Technologies. – 2024 / [Электронный ресурс]. – Режим доступа: https://ptsecurity.com/about/news/positive-technologies-kolichestvo-fishingovyh-atak-vyroslo-na-tret-za-god/
4. AG-IT. The latest phishing statistics [Электронный ресурс] // AAG-IT. – 2024. – Режим доступа: https://aag-it.com/the-latest-phishing-statistics/