МРНТИ 10.77.51
УДК 343.3/.7; 343.9
JEL K14

https://doi.org/10.46914/2959-4197-2026-1-1-204-214

ВОЛЧЕЦКАЯ Т.С.,[1]
д.ю.н., профессор.
e-mail: larty777@gmail.com
ORCID ID: 0000-0001-9870-680X
НУРГАЛИЕВ Б.М.,[2]
д.ю.н., г.н.с., профессор.
e-mail: nbake@mail.ru
ORCID ID: 0000-0002-3017-3610
НУРГАЛИЕВА А.Б.,[3]
докторант.
e-mail: n_zan_kz@mail.ru
ORCID ID: 0000-0001-8797-7399
САДВАКАСОВА А.Т.,*[2]
PhD, с.н.с.
*e-mail: adel_sadvakasova@mail.ru
ORCID ID: 0000-0001-5959-3718
[1]Балтийский федеральный
университет им. И. Канта,
г. Калининград, Россия
[2]Карагандинский университет
Казпотребсоюза,
г. Караганда, Казахстан
[3]Евразийский Национальный
университет имени Л.Н. Гумилева,
г. Астана, Казахстан

ФИШИНГ КАК ПОПУЛЯРНЫЙ СПОСОБ СОВЕРШЕНИЯ КИБЕРМОШЕННИЧЕСТВА: ПОНЯТИЕ, КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА, ЗАРУБЕЖНЫЙ ОПЫТ

Аннотация

Представленная научная статья рассматривает вызовы, обусловленные эволюцией информационно-коммуникационных технологий, породившей новые формы общественных отношений, требующие нормативно-правового регулирования. Активное внедрение Интернета в повседневную жизнь повышает комфорт и безопасность, но создает возможности для совершения компьютерных преступлений. Цель исследования – рассмотрение одного из способов компьютерного мошенничества – фишинга, являющегося одной из самых опасных и распространенных киберугроз. Для достижения данной цели использованы исторический, диалектический, сравнительно-правовой, формально-юридический методы исследования. В центре исследования – анализ фишинга как разновидности кибермошенничества, реализуемого в отношении физических лиц. Приведено наиболее общепринятое понятие фишинга как метода мошенничества, связанного с получением личной информации и конфиденциальных данных путем введения жертвы в заблуждение. Рассмотрены типичные виды фишинга, а также изучены меры, используемые в сфере противодействия данному способу преступной деятельности в отдельных зарубежных странах. Авторами сделан обоснованный вывод о том, что проблема киберпреступности, в частности фишинга, носит глобальный характер и является серьезной проблемой для многих стран мира. Данному негативному уголовно наказуемому деянию способствуют недостаточная образованность населения в сфере информационных технологий, несовершенство законодательства в вопросах регулирования данной сферы общественных отношений, а также широкая доступность к цифровым ресурсам. В заключение авторами предлагается повысить эффективность противодействия фишингу путем принятия комплексных мер, направленных на совершенствование национального законодательства, повышение цифровой грамотности населения, расширение международного сотрудничества правоохранительных органов посредством разработки инновационных технологий безопасности.

Ключевые слова: искусственный интеллект, киберпол, компьютерные преступления, компьютерное мошенничество, фишинг.

Введение

Динамичная эволюция информационно-коммуникационной сферы в современную эпоху детерминировала формирование качественно новых социальных взаимодействий, требующих институционально-правовой регламентации. Активное внедрение систем и сетей Интернета в повседневную жизнь, с одной стороны, повышает комфорт и безопасность для граждан, а с другой – создает новые возможности для совершения противоправных действий и увеличивает угрозы в области информационной безопасности [1, 2].

Анализ многочисленных исследований показывает, что проблема киберпреступности носит глобальный характер. Ключевыми детерминантами интенсификации правонарушений в сфере информационных систем выступают низкий уровень цифровой грамотности населения и дефицит компетенций в области разработки и использования инновационных технологий, а также массовая доступность сети Интернет и разнообразных платформ электронных коммуникаций для широких групп населения.

Часто пожилые люди, не владеющие навыками общения в киберпространстве, становятся легкой «добычей» для киберпреступников.

Компьютерное мошенничество – это серьезная проблема, которая возникла из-за широкого использования информационных технологий и Интернета в повседневной жизни. С каждым годом все больше людей приобщаются к работе с виртуальными данными для осуществления различных дел: совершение покупок, платежей, оказание услуг, общение с близкими и знакомыми. Однако с развитием цифровых услуг такие изменения также принесли новые угрозы. Одной из таких угроз является мошенничество, связанное с использованием компьютерных технологий, что можно назвать кибермошенничеством.

Материалы и методы

Исследование носит междисциплинарный характер, сочетая исторический и диалектический подходы со сравнительно-правовым и формально-юридическим анализом. Криминологическая типология охватывает e-mail-, spear-, smishing-, vishing-, pharming- и spoofing-схемы. Эмпирическая база: международная и национальная статистика (в т.ч. IC3), данные Казахстана за 2024 г., сведения о работе «Киберпола», Центра противодействия мошенничеству и системы «Кибернадзор», а также практики США и Великобритании (учет, тренды). Использованы нормативные акты и стратегии (например, CFAA 1986). Применены контент-анализ, дескриптивная статистика, сравнительный анализ, кейс-стади, правовая герменевтика.

Результаты и обсуждение

По мнению большинства ученых и специалистов в области кибербезопасности, самый распространенный тип кибератак – это фишинг, который осуществляется в отношении отдельных лиц через электронную почту, текстовые сообщения, телефонные звонки и другие формы общения.

Генезис и эволюция фишинга как инструмента социальной инженерии восходят к рубежу XX в. По мере массовой диффузии сети Интернет в 1990-е годы возникли и получили распространение мошеннические модели, эксплуатирующие цифровые коммуникации. Первое зафиксированное употребление термина «фишинг» относится к 2 января 1996 г. и связано с инцидентом, затронувшим сервисы провайдера America Online (AOL): злоумышленники рассылали пользователям имитации корпоративных электронных сообщений с просьбами предоставить учетные данные для доступа к системе [3].

Фишинг – обозначение одной из наиболее распространенных и высокорисковых форм финансового мошенничества. Термин восходит к англ. fishing («ловля рыбы») как метафоре «вылавливания» конфиденциальных данных у жертв [4]. Образно говоря, мошенники на обманные «приманки» в интернет-пространстве ловят доверчивых либо нетерпеливых граждан, неопытных сотрудников компаний. Фишинг, таким образом, представляет собой извлечение мошенниками информации путем вхождения в доверие к лицам, которые далее становятся

потерпевшими [5]. Характерным образцом целевого фишинга выступает массовая отправка на электронные адреса сообщений, побуждающих адресата перейти по гиперссылке на поддельный ресурс либо загрузить программный файл, содержащий троянские модули или иные вредоносные компоненты, без информирования пользователя о таком содержимом. Ключевая установка фишинговых кампаний – посредством введения в заблуждение склонить получателя к совершению действий, выгодных атакующему, в частности к раскрытию платежных сведений, учетных реквизитов доступа к системам либо иной охраняемой информации. В научной литературе фишинг интерпретируется как манипулятивное воздействие на пользователя, формируемое средствами социальной инженерии и побуждающее его взаимодействовать с имитированным веб-ресурсом, в результате чего злоумышленник получает доступ к конфиденциальным сведениям либо инициирует запуск вредоносного программного обеспечения [6]. Фишинг включает в себя психологическую манипуляцию и обман [7], при которых злоумышленники маскируются под авторитетные организации, чтобы ввести пользователей в заблуждение и заставить их раскрыть личную информацию, например номера банковских счетов или данные кредитной карты. Фишинговые атаки становятся все более изощренными и включают в себя различные типы, такие как фишинг по электронной почте, целевой фишинг, смишинг, вишинг и уэйлинг, которые характеризуются определенными каналами и методами выполнения. В большинстве случаев фишинговые посягательства ориентированы как минимум на одну из следующих установок: изъятие охраняемых сведений посредством направления сомнительных сообщений, побуждающих адресата обманным путем разгласить аутентификационные реквизиты либо персональные данные; реализацию классической схемы мошенничества через массовую рассылку корреспонденции, визуально и стилистически имитирующей коммуникации от легитимных организаций [8].

Согласно позиции значительной части исследователей, фишинг относится к ключевым рискам в сфере кибербезопасности. Злоумышленники широко применяют имитационные вебстраницы для несанкционированного получения доступа к банковским счетам и персональным данным адресатов. Дополнительно они распространяют вложения с вредоносным кодом в электронных сообщениях с целью инсталляции зловредного программного обеспечения. К распространенным тактикам относятся атаки с применением разнообразных загрузчиков и инструментов, включая PDF-файлы, кейлоггеры и средства удаленного администрирования. Следует подчеркнуть, что фишинговые кампании демонстрируют растущую сложность, а атакующие постоянно модифицируют арсенал и поведенческие паттерны, снижая предсказуемость и повышая результативность посягательств. Рассматриваемые механизмы фишинга включают атаки-приманки, которые направлены на сбор информации для планирования будущих атак [9]. Они могут принимать форму электронных писем с пустым содержанием или коротких сообщений. Фишинг нацелен на конкретных людей или компании, используя персонализированные данные для создания более убедительных сообщений. Другой тип атаки – вишинг, который заключается в использовании телефонных звонков для обмана потенциальных жертв с целью раскрытия личной информации жертвы [10]. Другой метод, фарминг, заключается в отравлении кеша системы доменных имен для перенаправления пользователей на мошеннические вебсайт. Это хитрый способ обмануть пользователей, чтобы они предоставили личную информацию [11].

Далее, спуфинг представляет собой разновидность сетевого посягательства, при котором нарушитель, имитируя корректное соединение, добивается несанкционированного доступа к информационной инфраструктуре. Проведенный анализ акцентирует критическую значимость противодействия фишингу и необходимость для организаций и частных пользователей поддерживать высокий уровень киберзащиты [12]. С учетом постоянной эволюции техники и приемов фишинга своевременная актуализация средств безопасности, внедрение многофакторных механизмов аутентификации и систематическое обучение персонала выступают обязательными условиями нейтрализации данной серьезной киберугрозы.

Еще один вид – SMS-фишинг, он же смишинг, который является разновидностью фишингового воздействия, нацеленного на пользователей мобильных устройств и реализуемого через сервис коротких сообщений. Злоумышленник формирует текстовое обращение, побуждающее адресата выполнить целевое действие: перейти по гиперссылке, совершить телефонный вы-

зов либо направить электронное письмо. На следующем этапе инициируется запрос на предоставление персональных и аутентификационных сведений либо запускается установка вредоносного программного компонента. Специфика мобильной среды затрудняет своевременную идентификацию угрозы: URL-адреса нередко маскируются посредством сокращенных ссылок, что снижает распознаваемость подмены и повышает вероятность успешной компрометации. Злоумышленники используют также и генераторы голоса, сформированные на основе искусственного интеллекта (ИИ), чтобы звучать как личный авторитет или член семьи во время телефонного звонка. Это еще больше персонализирует попытку фишинга, увеличивая вероятность ее срабатывания. Злоумышленникам просто нужен образец голоса, поэтому используется небольшой аудиоклип менеджера или члена семьи жертвы.

Согласно результатам исследований Internet Crime Complaint Center (IC3), в мировой статистике распространенности киберпреступности в топ-20 наиболее уязвимых государств, помимо США и Великобритании, входят Австралия, Канада, Греция, Индия, Франция и Южно-Африканская Республика. Страны постсоветского пространства пока не входят в этот рейтинг, однако в последние годы наблюдается стремительный всплеск киберпреступности и особенно таких его проявлений, как фишинг.

Сходная динамика наблюдается и в Республике Казахстан: по итогам 2024 г. зарегистрировано 15 905 уголовных производств, квалифицированных как интернет-мошенничество, из которых раскрыто лишь 3286 дел; таким образом, показатель раскрываемости составляет около 20%. Несмотря на предпринимаемые меры, доля сетевых мошенничеств продолжает увеличиваться и в настоящее время достигает 47% от совокупного массива мошеннических посягательств в стране. В целях усиления противодействия указанным деяниям МВД РК во взаимодействии с Национальным банком и банками второго уровня сформировало специализированный Центр противодействия мошенничеству в финансовой сфере. Функционирование данного центра обеспечивает оперативную блокировку подозрительных банковских транзакций: с начала 2024 г. предотвращено свыше 5000 инцидентов, в «черный список» включено 835 дропперов, на счета которых наложены блокировки на сумму более 300 млн тенге.

Вместе с тем существенная доля телефонных и текстовых мошеннических коммуникаций генерируется из-за пределов страны. По оценке заместителя министра внутренних дел Республики Казахстан С. Сарсенова, функционируют специализированные колл-центры, физически размещенные на территории Казахстана, однако оперативно координируемые из-за рубежа, преимущественно с территории Украины, что значительно осложняет противодействие преступным практикам ввиду использования правонарушителями многоуровневых схем маскировки деятельности, включая международные каналы связи. Эффективная нейтрализация интернет-мошенничества предполагает тесную кооперацию с финансовыми организациями и зарубежными партнерами. По данным, представленным на заседании Межведомственной комиссии по профилактике правонарушений, новое подразделение МВД РК «Киберпол» обеспечило раскрытие более 2,5 тыс. кибердел и содействовало возмещению ущерба на сумму 962 млн тенге. В рамках целевых мероприятий задержано 914 фигурантов, пресечено 58 млн вызовов с подложных абонентских номеров и изъято свыше 6 тыс. незарегистрированных SIM-карт.

Помимо этого, в рамках функционирования специализированного центра по противодействию мошенничеству пресечен вывод средств за рубеж в сумме около 400 млн тг на стадии трансграничной транзакции. По данным Агентства по финансовому мониторингу, за прошедший год в сети выявлено 2024 схемы финансовых пирамид и закрыто 266 чатов в мессенджерах, через которые осуществлялись нелегальные операции. С использованием системы «Кибернадзор» заблокировано свыше 8 тыс. мошеннических веб-ресурсов; гражданам предложен профильный бот в Telegram для верификации компаний и сайтов на признаки пирамид, посредством которого подано более 9 тыс. обращений. Дополнительные меры по пресечению международных вызовов с подмененных номеров способствовали снижению уровня телефонного мошенничества и предотвращению многочисленных попыток вывода активов. Преступные группы активно задействовали фишинг, вишинг и так называемое микширование для несанкционированного доступа к банковским счетам, а также скимминговые устройства для компрометации платежных карт и изъятия реквизитов. В целом проблема интернет-мошенничества в Казахстане стоит остро, и, несмотря на принимаемые меры, количество зарегистрированных

случаев продолжает расти. Для повышения эффективности борьбы с данным видом преступлений требуется дальнейшее усиление межведомственного взаимодействия, международного сотрудничества и использование современных технологий [13].

Россия. Российские ученые с учетом современной геополитической реальности и увеличения компьютерных мошенничеств также уделяют значительное внимание актуальным вопросам борьбы с ними, и в частности с фишингом и различными его разновидностями, количество которых в настоящее время составляют 35% от всех случаев мошенничества с банковскими клиентами. Как и в нашей стране, в России распространены различные виды фишинга: классический фишинг, целенаправленные фишинговые приемы, фишинг против топ-менеджмента, фишинговые рассылки от Google и Dropbox, фишинговые письма с конкурентными вложениями, фарминг. В научном дискурсе преобладает оценка, согласно которой, несмотря на предпринимаемые правоохранительными органами меры, полная элиминация фишинга в обозримой перспективе маловероятна, поскольку ежедневно фиксируются тысячи подобных посягательств. Комплекс профилактики, ориентированный на минимизацию последствий, сводится к своевременному и исчерпывающему информированию пользователей о приемах злоумышленников, формированию критической настороженности к нетипичным и внезапным цифровым коммуникациям, а также к призыву строгого соблюдения регламентов кибергигиены и правил противодействия фишинговым атакам. Предлагается также проанализировать психологические аспекты, влияющие на успешность фишинговых атак, и разработать новые стратегии защиты, основанные на понимании поведения человека. В числе других мер предлагаются также и такие, как изучение и прогноз развития фишинговых технологий, включая новые виды атак, и, соответственно, разработка инновационных методов обнаружения и предотвращения таких угроз. Особое внимание должно быть уделено анализу последствий успешных фишинговых атак для организаций и частных лиц, оценке материального ущерба и разработке рекомендаций по минимизации потерь. Особого внимания заслуживают создание образовательных программ и тренингов для повышения осведомленности пользователей о фишинге с целью повышения их защищенности от интернет-мошенничества или кибермошенничества [14].

Заслуживает внимания и предлагаемые нововведения в законодательстве. Так, некоторые авторы предлагают скорректировать классификацию преступлений в уголовном законодательстве, внести уникальные определения и потенциально новые статьи в Уголовный кодекс для надлежащего реагирования на новые методы киберпреступников. Авторы предлагают ввести в Уголовный кодекс РФ специализированную статью, посвященную именно компьютерному мошенничеству, которая четко определяла бы сущность данных преступлений и включала бы квалифицирующие признаки, связанные с использованием компьютерных технологий, что повысило бы общую эффективность правоохранительных органов в этой области [15].

Учет показателей киберпреступности в Великобритании осуществляется различными государственными структурами. До 2018 г. для регистрации фактов кибермошенничества и ряда иных компьютерно опосредованных деяний применялась специальная временная форма, что осложняет сопоставление динамики за 2016–2020 гг. По оценкам опросного исследования Cybercrime Victim Survey, в 2020 г. в стране зафиксировано порядка 1,7 млн инцидентов киберпреступной активности. Экспертные интерпретации увязывают увеличение с расширением двух наиболее распространенных категорий злоупотреблений: фишинга, взломов аккаунтов в социальных сетях и электронной почты (прирост на 26%: с 11 101 до 14 004 случаев), а также распространения вирусов и иного вредоносного программного обеспечения (рост на 30%: с 5536 до 7192 эпизодов). Данная динамика, вероятно, коррелирует с увеличением масштабных утечек данных на глобальном уровне, позволяющих злоумышленникам использовать связки адресов электронной почты и паролей для компрометации учетных записей. Сходные тенденции сохранялись и в 2020–2021 гг., однако временные ряды демонстрировали волнообразный характер колебаний зарегистрированных киберправонарушений. Всего за этот период было зарегистрировано 493 325 сообщений, что свидетельствует, что киберпреступность в Великобритании продолжает оставаться серьезной проблемой. Несмотря на определенные трудности в учете и анализе статистических данных, имеющаяся информация свидетельствует о высоких масштабах киберпреступности и тенденциях ее роста. Наиболее распространенными видами киберпреступности являются различные формы мошенничества, прежде всего фишинг, взлом

аккаунтов социальных сетей и электронной почты, а также распространение вредоносного программного обеспечения. Эффективное противодействие этим угрозам требует комплексных усилий правоохранительных органов, бизнеса и общества в целом [16].

На основе изучения литературы и статистических данных о состоянии и тенденциях киберпреступности в Великобритании эксперты предлагают следующие выводы и предложения. Изучение факторов, влияющих на существенный рост наиболее распространенных видов киберпреступности, таких как фишинг, взлом социальных сетей, взлом электронной почты и распространение вредоносного ПО. Заслуживает внимания рекомендации по изучению влияния утечек персональных данных на распространение киберпреступности, включая взлом аккаунтов и обмен паролями. Ученые предлагают сравнить динамику и структуру киберпреступности в Великобритании с другими странами Европы или мира и оценить эффективность мер, принимаемых правоохранительными органами Великобритании для противодействия киберпреступности и разработки рекомендаций по их совершенствованию. Предлагается также изучение характеристик различных видов киберпреступности, таких как фишинг, и разработка мер по их предотвращению, а также анализ осведомленности и уровня кибербезопасности населения Великобритании и принятие эффективных мер по повышению цифровой грамотности граждан [16].

Подобно ряду европейских и американских юрисдикций, задача противодействия киберпреступности и определение роли правоохранительных институтов в США имеет первостепенное значение. По данным за 2020 г., зарегистрировано свыше 791 тыс. инцидентов, что подтверждает статус проблемы как одного из ключевых вызовов национальной безопасности. Формирование государственной политики в данной сфере восходит к принятию в 1986 г. закона о компьютерном мошенничестве и злоупотреблениях (CFAA). В настоящее время центральные функции координации и пресечения выполняют ФБР, Агентство по кибербезопасности и безопасности инфраструктуры (CISA) и Киберкомандование США. Исследователи выделяют узловые этапы эволюции подходов федеральной власти: утверждение Национальной стратегии защиты киберпространства (2003 г.) и запуск секретной Комплексной инициативы по кибербезопасности (2008 г.), что обеспечило институционализацию приоритетов, расширение межведомственного взаимодействия и усиление превентивных, оперативно-разыскных и технических мер противодействия киберугрозам.

Силовые и иные ведомства, вовлеченные в противодействие фишингу и другим киберпреступлениям, руководствуются стратегическими документами, такими, как Международная стратегия по киберпространству 2011 г. и Национальная стратегия США по развитию искусственного интеллекта 2016 г. Эти инициативы были направлены на построение системы международного сотрудничества по кибербезопасности на основе американских подходов, а также использование технологий ИИ для укрепления национальной безопасности.

Несмотря на развитую правовую базу и активные усилия государства, проблема роста киберпреступности в США остается актуальной – около 90% крупных американских компаний ежегодно сталкиваются с хакерскими атаками, что влечет за собой финансовые потери более чем в 100 млрд долларов.

Наиболее распространенными видами киберпреступности в США остаются фишинг, кибермошенничество, криптоджекинг и другие. США позиционируют себя как одну из самых безопасных стран мира с точки зрения кибербезопасности, занимая первое место в Индексе кибербезопасности IISS в 2023 г. Несмотря на то что правительство США принимает широкий спектр мер по противодействию глобальной киберпреступности, эти усилия характеризуются стремлением к продвижению американских интересов и гегемонии в киберпространстве.

Указанные выше документы заложили основы структурной и функциональной деятельности различных ведомств по борьбе с киберугрозами, при этом координирующая роль отводится Министерству внутренней безопасности. Резюмируя литературные источники, можно отметить, что правительство США принимает широкий комплекс мер по противодействию глобальной киберпреступности. Это включает в себя разработку правовых норм, обучение кадров, совершенствование технической защиты, налаживание международного сотрудничества. Несмотря на принимаемые меры, проблема киберпреступности остается актуальной для США, особенно в экономической сфере, что свидетельствует о необходимости дальнейшего совершенствования государственной политики в этой области [17].

Заключение

Резюмируя вышесказанное, хотелось бы отметить следующее. Интенсивная трансформация информационно-коммуникационной сферы и формирование качественно новых социальных взаимодействий обуславливают необходимость правового регулирования, соразмерного требованиям складывающейся цифровой реальности. Активное внедрение в повседневную жизнь интернет-систем и сетей повышает комфорт и безопасность граждан, но и создает новые возможности для компьютерных противоправных действий. Анализ многочисленных исследований в этой области показывает, что проблема киберпреступности носит глобальный характер.

Основными факторами, способствующими росту киберпреступности, являются недостаточная образованность населения в области развития информационных технологий, а также легкая доступность компьютеров и Интернета. Пожилые люди, не имеющие навыков работы с компьютером, гаджетами, часто становятся легкой добычей киберпреступников. Динамика интернет-мошенничества в Казахстане подтверждает, что одних лишь репрессивных мер и точечных блокировок недостаточно: почти при половинной доле сетевых схем в общей структуре мошенничества сохраняется низкая результативность их раскрытия и возврата активов. Отсюда вытекает необходимость смещения акцента на предупреждение: регламентированный порядок мгновенной приостановки спорных транзакций, формализованные «плейбуки» взаимодействия следствия и банковского сектора, обязательные «красные флаги» для антифрод-систем и процессуальная фиксация цифровых следов для последующего доказывания.

Одним из самых распространенных и опасных видов рассматриваемого мошенничества является фишинг – разновидность социальной инженерии, когда мошенники пытаются обманом заставить пользователей выдать личную и финансовую информацию. Проведенный анализ генезиса и эволюции фишинга демонстрирует, что данный феномен прошел стадию усложнения и дифференциации: в современном обороте фиксируются многочисленные модификации, включая e-mail-фишинг, адресный (spear-phishing), SMS-вариант (smishing), голосовые схемы (vishing) и другие форматы. Международные ориентиры и заимствование лучших практик. Сопоставление с юрисдикциями, где учет и противодействие киберугрозам институционализированы (Великобритания, США), показывает, что устойчивый эффект достигается там, где соединены единые стандарты отчетности о фишинговых инцидентах, межведомственный центр координации и закрепленная в стратегиях приоритизация профилактики и устойчивости инфраструктуры. Для Казахстана это обосновывает целесообразность создания единого национального реестра фишинговых доменов/телефонии с обязательной интеграцией операторов связи и финсектора и регулярной публикацией сводных индикаторов риска для граждан и бизнеса.

Сформулирован общий вывод исследования: ключевая установка фишинговых кампаний заключается в побуждении адресата к недобровольному разглашению охраняемых сведений – аутентификационных данных, реквизитов банковских карт и счетов. Для достижения этой цели злоумышленники применяют инструменты социальной инженерии, конструируя у жертвы ощущение срочности и неизбежности предоставления информации; далее пользователь перенаправляется на имитационный веб-ресурс, визуально воспроизводящий интерфейс легитимной площадки. Так, эволюция фишинга проявляется в переходе от массовых рассылок к персонализированным сценариям, ориентированным на смартфон пользователя и его голосовую биометрию. Комбинация смишинга с голосовыми подменами, синтезированными ИИ, нивелирует традиционные «подсказки настороженности» и требует отраслевых стандартов: фильтрации ссылок на уровне оператора, обязательной двухфакторной аутентификации по умолчанию в гос- и финсервисах, а также внедрения регулярных фишинг-симуляций для персонала организаций критически важного сектора.

Анализ типологии фишинговых посягательств – от адресных атак на конкретных лиц и организации до вишинга, фарминга и спуфинга – свидетельствует, что наибольший риск для информационной безопасности формирует SMS-фишинг, ориентированный на мобильную экосистему. Дополнительно фиксируется ускоренная диффузия техник, основанных на инструментах искусственного интеллекта: в частности, использование систем синтеза речи для генерации индивидуализированных голосовых обращений, что повышает правдоподобие коммуникации и результативность фишинговых звонков.

В совокупности полученные результаты подтверждают, что фишинг относится к наиболее массовым и высокорисковым формам киберпреступности современности. Несмотря на реализуемые контрмеры, число соответствующих инцидентов демонстрирует устойчивую тенденцию к росту. Эффективное противодействие требует интегральной междисциплинарной стратегии, сочетающей модернизацию нормативно-правовой базы, системное повышение цифровой грамотности пользователей, разработку и внедрение проактивных технологий киберзащиты, а также расширение международной кооперации компетентных органов. Критически значимым элементом профилактики выступает оперативное и достоверное информирование населения о механизмах фишинговых посягательств вкупе с формированием обоснованной настороженности к нетипичным и подозрительным коммуникациям, что способно существенно снизить вероятность успешной реализации данных мошеннических схем.

Информация о финансировании. Статья подготовлена в рамках выполнения договора на грантовое финансирование, заключенного с Комитетом науки Министерства науки и высшего образования Республики Казахстан (ИРН проекта AP26198915).

ЛИТЕРАТУРА

1 Ханов Т.А., Жиенбеков Ж.Е. Система обеспечения информационной безопасности // Актуальные проблемы современности. – 2016. – № 2(12). – С. 37–43.

2 Ogonji M., Okeyo G., Wafula J. A survey on privacy and security of Internet of Things // Computer Science Review. 2020. Vol. 38. URL: https://www.sciencedirect.com/science/article/abs/pii/S1574013720304123 (accessed: 04.09.2025)

3 Orunsolu A.A., Abayomi-Alli O.O., Misra S. A predictive model for phishing detection // Journal of King Saud University – Computer and Information Sciences. 2022. Vol. 34. Issue 2. P. 232–247.

4 Ribeiro L., Sousa Guedes I., Cardoso C. Which factors predict susceptibility to phishing? An empirical study // Computers & Security. 2024. URL: https://www.sciencedirect.com/science/article/pii/S0167404823004686 (accessed: 04.09.2025)

5 Alkhalil Z., Hewage C., Nawaf L., Khan I. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy // Frontiers in Computer Science. 2021. URL: https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.563060/full (accessed: 04.09.2025)

6 Naqvi B., Perova K., Farooq A., Makhdoom I., Oyedeji S., Porras J. Mitigation strategies against the phishing attacks: a systematic literature review // Computers & Security. 2023. Vol. 123. URL: https://strathprints.strath.ac.uk/87505/1/Naqvi-etal-CS-2023-Mitigation-strategies-against-the-phishing-attacks.pdf (accessed: 05.09.2025)

7 Иванова Ю.А., Сарбаев Г.М. К вопросу о киберпреступности // Цифровые трансформации экономики и права. Сборник научных тезисов Национальной научно-практической конференции. – Волгоград, 2022. – С. 58–64.

8 Архипова А.Б., Нечаев Д.А. Технология формирования интегрированной антифишинговой системы в цифровом обществе // Вестник СибГУТИ. – 2023. – Т. 17. – № 2. – С. 93–103. DOI:10.55648/1998-692 0-2 023-17-2-93-103

9 Клевчук О. Обзор угроз: атаки-приманки. URL: https://blog.barracuda.com/2021/11/10/threat-spotlight-bait-attacks. (дата обращения: 12.09.2025)

10 Зигмунт О.А. Компьютерная преступность в Германии // Преступность и социальный контроль в обществе постмодерна: Сб. материалов международной Балтийской криминолог. конф. Ч. 1. – СПб.: Алеф-Пресс, 2015. – С. 157–159.

11 Chimuco F.T., Sequeiros J.B.F., Lopes C.G., Simões T.M.C., Freire M.M., Inácio P.R.M. Secure cloud-based mobile apps: attack taxonomy, requirements, mechanisms, tests and automation // International Journal of Information Security. 2023. Vol. 22. Issue 5. P. 1121–1158. URL: https://link.springer.com/article/10.1007/s10207-023-00669-z (accessed: 05.09.2025)

12 Sethuraman S.C., Devi Priya V.S., Reddi T., Reddy M.S.T., Khan M.K. A comprehensive examination of email spoofing: Issues and prospects for email security // Computers & Security. 2024. Vol. 137. URL: https://dl.acm.org/doi/10.1016/j.cose.2023.103600 (accessed: 06.09.2025).

13 Киберпреступность и киберконфликты: Казахстан. URL: https://tadviser.com/index.php/Article:Cybercrime_and_cyber_conflicts:_Kazakhstan#.2A_Online_Fraud_Detection_-_20.25 (дата обращения 12.09.2025).

14 Борисов В.Р. Иинформационные технологии и цифровизация как среда деятельности кибермошенников // Инновационное развитие экономики. – 2021. – № 6(66). – С. 69–79.

15 Кобец П.Н. Характеристика современных особенностей противоправных проявлений, совершаемых в киберпространстве // Современная наука. – 2022. – № 3. – С. 18–21.

16 Correia S.G. Making the most of cybercrime and fraud crime report data: a case study of UK Action Fraud // International Journal of Population Data Science. 2022. Vol. 7. No.1. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC9152840/ (accessed: 06.09.2025)

17 Fahey E. The evolution of EU – US cybersecurity law and policy // Journal of European Integration. 2024. No. 46(7). P. 1073–1088. URL: https://www.tandfonline.com/doi/full/10.1080/07036337.2024.2411240#abstract (accessed: 13.09.2025)

REFERENCES

1 Hanov T.A., Zhienbekov Zh.E. (2016) Sistema obespechenija informacionnoj bezopasnosti // Aktual'nye problemy sovremennosti. No. 2 (12). P. 37–43. (In Russian)

2 Ogonji M., Okeyo G., Wafula J. (2020) A survey on privacy and security of Internet of Things // Computer Science Review. Vol. 38. URL: https://www.sciencedirect.com/science/article/abs/pii/S1574013720304123 (accessed: 04.09.2025) (In English)

3 Orunsolu A.A., Abayomi-Alli O.O., Misra S. (2022) A predictive model for phishing detection // Journal of King Saud University – Computer and Information Sciences. Vol. 34. Issue 2. P. 232–247. (In English)

4 Ribeiro L., Sousa Guedes I., Cardoso C. (2024) Which factors predict susceptibility to phishing? An empirical study // Computers & Security. URL: https://www.sciencedirect.com/science/article/pii/S0167404823004686 (accessed: 04.09.2025) (In English)

5 Alkhalil Z., Hewage C., Nawaf L., Khan I. (2021) Phishing Attacks: A Recent Comprehensive Study and a New Anatomy // Frontiers in Computer Science. URL: https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.563060/full (accessed: 04.09.2025) (In English)

6 Naqvi B., Perova K., Farooq A., Makhdoom I., Oyedeji S., Porras J. (2023) Mitigation strategies against the phishing attacks: a systematic literature review // Computers & Security. Vol. 123. URL: https://strathprints.strath.ac.uk/87505/1/Naqvi-etal-CS-2023-Mitigation-strategies-against-the-phishing-attacks.pdf (accessed: 05.09.2025) (In English)

7 Ivanova Ju.A., Sarbaev G.M. (2022) K voprosu o kiberprestupnosti // Cifrovye transformacii jekonomiki i prava. Sbornik nauchnyh tezisov Nacional'noj nauchno-prakticheskoj konferencii. Volgograd. P. 58–64. (In Russian)

8 Arhipova A.B., Nechaev D.A. (2023) Tehnologija formirovanija integrirovannoj antifishingovoj sistemy v cifrovom obshhestve // Vestnik SibGUTI. Vol. 17. No. 2. P. 93–103. DOI:10.5564 8/1998-692 0-2 023-17-2-93-103 (In Russian)

9 Klevchuk O. Obzor ugroz: ataki-primanki. URL: https://blog.barracuda.com/2021/11/10/threat-spotlight-bait-attacks. (data obrashhenija: 12.09.2025) (In Russian)

10 Zigmunt O.A. (2015) Komp'juternaja prestupnost' v Germanii // Prestupnost' i social'nyj kontrol' v obshhestve postmoderna: Sb. materialov mezhdunarodnoj Baltijskoj kriminolog. konf. Ch. 1. – SPb.: Alef-Press. P. 157–159. (In Russian)

11 Chimuco F.T., Sequeiros J.B.F., Lopes C.G., Simões T.M.C., Freire M.M., Inácio P.R.M. (2023) Secure cloud-based mobile apps: attack taxonomy, requirements, mechanisms, tests and automation // International Journal of Information Security. Vol. 22. Issue 5. P. 1121–1158. URL: https://link.springer.com/article/10.1007/s10207-023-00669-z (accessed: 05.09.2025) (In English)

12 Sethuraman S.C., Devi Priya V.S., Reddi T., Reddy M.S.T., Khan M.K. (2024) A comprehensive examination of email spoofing: Issues and prospects for email security // Computers & Security. Vol. 137. URL: https://dl.acm.org/doi/10.1016/j.cose.2023.103600 (accessed: 06.09.2025) (In English)

13 Kiberprestupnost'ikiberkonflikty:Kazahstan.URL:https://tadviser.com/index.php/Article:Cybercrime_and_cyber_conflicts:_Kazakhstan#.2A_Online_Fraud_Detection_-_20.25 (data obrashhenija 12.09.2025) (In Russian)

14 Borisov V.R. (2021) Iinformacionnye tehnologii i cifrovizacija kak sreda dejatel'nosti kibermoshennikov // Innovacionnoe razvitie jekonomiki. No. 6 (66). P. 69–79. (In Russian)

15 Kobec P.N. (2022) Harakteristika sovremennyh osobennostej protivopravnyh projavlenij, sovershaemyh v kiberprostranstve // Sovremennaja nauka. No. 3. P. 18–21. (In Russian)

16 Correia S.G. (2022) Making the most of cybercrime and fraud crime report data: a case study of UK Action Fraud // International Journal of Population Data Science. Vol. 7. No.1. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC9152840/ (accessed: 06.09.2025) (In English)

17 Fahey E. (2024) The evolution of EU – US cybersecurity law and policy // Journal of European Integration. No. 46(7). P. 1073–1088. URL: https://www.tandfonline.com/doi/full/10.1080/07036337.2024.2411240#abstract (accessed: 13.09.2025) (In English)

ВОЛЧЕЦКАЯ Т.С.,[1]
з.ғ.д., профессор.
e-mail: larty777@gmail.com
ORCID ID: 0000-0001-9870-680X
НУРГАЛИЕВ Б.М.,[2]
з.ғ.д., бас ғылыми қызметкер, профессор.
e-mail: nbake@mail.ru
ORCID ID: 0000-0002-3017-3610
НУРГАЛИЕВА А.Б.,[3]
докторант.
e-mail: n_zan_kz@mail.ru
ORCID ID: 0000-0001-8797-7399
САДВАКАСОВА А.Т.,*[1]
PhD, аға ғылыми қызметкер.
*e-mail: adel_sadvakasova@mail.ru
ORCID ID: 0009-0008-5744-336X
[1]И. Кант атындағы Балтық
федералды университеті,
Калининград қ., Ресей
[2]Қазтұтынуодағы Қарағанды университеті,
Қарағанды қ., Қазақстан
[3]Л.Н. Гумилев атындағы Еуразия
ұлттық университеті,
Астана қ., Қазақстан

ФИШИНГ КИБЕР АЛАЯҚТЫҚ ЖАСАУДЫҢ ТАНЫМАЛ ТӘСІЛІ РЕТІНДЕ: ТҰЖЫРЫМДАМА, КРИМИНОЛОГИЯЛЫҚ СИПАТТАМА, ШЕТЕЛДІК ТӘЖІРИБЕ

Аңдатпа

Ұсынылған ғылыми мақала нормативтік-құқықтық реттеуді қажет ететін қоғамдық қатынастардың жаңа формаларын тудырған ақпараттық-коммуникациялық технологиялардың эволюциясына байланысты сын-қатерлерді қарастырады. Интернетті күнделікті өмірге белсенді енгізу жайлылық пен қауіпсіздікті арттырады, бірақ компьютерлік қылмыс жасауға мүмкіндік береді. Компьютерлік алаяқтықтың бір әдісін қарастыру – ең қауіпті және кең таралған киберқауіптердің бірі болып табылатын фишинг. Осы мақсатқа жету үшін тарихи, диалектикалық, салыстырмалы-құқықтық, ресми-құқықтық зерттеу әдістері қолданылды. Жеке тұлғаларға қатысты жүзеге асырылатын кибер алаяқтықтың бір түрі ретінде талдау, жәбірленушіні адастыру арқылы жеке ақпарат пен құпия деректерді алуға байланысты алаяқтық әдісі ретінде фишингтің ең көп қабылданған тұжырымдамасы келтірілген. Фишингтің типтік түрлері қаралды, сондай-ақ жекелеген шет елдерде қылмыстық қызметтің осы әдісіне қарсы іс-қимыл саласында қолданылатын шаралар зерттелді. Авторлар киберқылмыс, атап айтқанда фишинг мәселесі жаһандық сипатқа ие және әлемнің көптеген елдері үшін маңызды мәселе болып табылады деген негізделген қорытынды жасады. Бұл теріс қылмыстық жазаланатын әрекетке халықтың ақпараттық технологиялар саласындағы білімінің жеткіліксіздігі, қоғамдық қатынастардың осы саласын реттеу мәселелерінде заңнаманың жетілмегендігі, сондай-ақ цифрлық ресурстарға кең қолжетімділік ықпал етеді. Қорытындылай келе, авторлар ұлттық заңнаманы жетілдіруге, халықтың цифрлық сауаттылығын арттыруға, қауіпсіздіктің инновациялық технологияларын әзірлеу арқылы Құқық қорғау органдарының халықаралық ынтымақтастығын кеңейтуге бағытталған кешенді шаралар қабылдау арқылы фишингке қарсы іс-қимылдың тиімділігін арттыруды ұсынады.

Тірек сөздер: жасанды интеллект, киберпол, компьютерлік қылмыстар, компьютерлік алаяқтық, фишинг.

VOLCHETSKAYA T.,[1]
d.l.s., professor.
e-mail: larty777@gmail.com
ORCID ID: 0000-0001-9870-680X
NURGALIYEV B.M.,[2]
d.l.s., chief researcher, professor.
e-mail: nbake@mail.ru,
ORCID ID: 0000-0002-3017-3610
NURGALIYEVA A.B.,[3]
PhD student.
e-mail: n_zan_kz@mail.ru
ORCID ID: 0000-0001-8797-7399
SADVAKASSOVA A.T.,*[2]
PhD, senior researcher.
*e-mail: adel_sadvakasova@mail.ru,
ORCID ID: 0000-0001-5959-3718
[1]Immanuel Kant
Baltic Federal University,
Kaliningrad, Russia
[2]Karaganda University of Kazpotrebsoyuz,
Karaganda, Kazakhstan
[3]Eurasian National University
named after L.N. Gumilyov,
Astana, Kazakhstan

PHISHING AS A POPULAR METHOD OF COMMITTING CYBERBULLYING: CONCEPT, CRIMINOLOGICAL CHARACTERISTICS, FOREIGN EXPERIENCE

Abstract

The article examines issues arising from the development of information and communication technologies, which have generated new social relations requiring legal regulation. The pervasive adoption of the Internet enhances everyday comfort and safety but also creates opportunities for computer crime. The study's purpose is to analyze phishing, one of the most dangerous and widespread cyber threats. To achieve this aim, the research employs historical, dialectical, comparative-legal, and formal-legal methods. The subject is phishing as a method of computer fraud perpetrated against individuals via email, text messages, phone calls, or other forms of digital communication. The commonly accepted definition of phishing is presented as a fraud method that obtains personal information and confidential data by deceiving the victim. Typical phishing variants are described. The paper also reviews measures used to counter this form of criminal activity in selected foreign jurisdictions. The authors conclude that cybercrime is global in scope and a serious challenge for many countries. Contributing factors include low public literacy in information technology, imperfect legislation regulating this sphere of social relations, and widespread access to digital resources. The conclusion proposes improving anti-phishing effectiveness through comprehensive measures: refining legislation, raising digital literacy, expanding international law-enforcement cooperation, and developing innovative security technologies.

Keywords: artificial intelligence, cyberpole, computer crimes, computer fraud, phishing.

Дата поступления статьи в редакцию: 19.10.2025