Фишинговые схемы мошенничества

Phishing Fraud Schemes

DOI: 10.12737/2587-9111-2025-13-2-25-29 Получено: 03 февраля 2025 г. / Одобрено: 26 февраля 2025 г. / Опубликовано: 25 апреля 2025 г.

Иванова О.С.

Канд. полит. наук, доцент,
ФГБОУ ВО «Тульский государственный педагогический университет им. Л.Н. Толстого»,
Россия, 300026, г. Тула, проспект Ленина, д. 125,
e-mail: mrs.ivanova@yandex.ru

Иванов А.А.

Магистрант,
ФГАОУ ВО «Российский университет дружбы народов»
Россия, 117198, г. Москва, ул. Миклухо-Маклая, д. 6
e-mail: lenox2006@yandex.ru

Ivanova O.S.

Candidate of Political Sciences, Associate Professor,
Tula State Lev Tolstoy Pedagogical University,
125, Lenina St., Tula, 300026, Russia,
e-mail: mrs.ivanova@yandex.ru

Ivanov A.A.

Master's Degree Student,
Peoples' Friendship University of Russia
6, Miklukho-Maklaya St., Moscow, 117198, Russia,
e-mail: lenox2006@yandex.ru

Аннотация
Фишинг – разновидность интернет-мошенничества с целью похищения идентификационных данных пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации.
Активация вирусов происходит в момент открытия вложения или перехода по ссылке в фишинговом письме. Не стоит забывать и о том, что некоторые из почтовых клиентов поддерживают скрипты, что делает возможным заражение сразу после того, как пользователь открыл подозрительное письмо. Опасность фишинговых ссылок и вирусных писем состоит в том, что их крайне трудно отличить от настоящих, но все же есть типичные фишинговые схемы, знание которых может уберечь от финансовых потерь. В статье произведен анализ статистических данных относительно динамики развития фишинговых схем на территории РФ, выявлены сектора экономики, наиболее пострадавшие от кибермошенников. А также выявлены социальные и экономические факторы, дифференцирующие потенциальных жертв мошенников, отражена общемировая статистика фишинговых атак за 2022–2024 гг. и при помощи алгоритма экспоненциального сглаживания спрогнозирована статистика по атакам через фишинговые сайты и почтовые рассылки на 2025 г.

Ключевые слова: интернет-мошенничество, искусственный интеллект, фишинговые письма, фишинговые атаки.

Abstract
Phishing is a type of Internet fraud aimed at stealing user identification data. This includes theft of passwords, credit card numbers, bank accounts and other confidential information.
Viruses are activated when an attachment is opened or a link is clicked in a phishing e-mail. Do not forget that some of the email clients support scripts, which makes infection possible immediately after the user has opened a suspicious email. The danger of phishing links and viral emails is that they are extremely difficult to distinguish from real ones, but still there are typical phishing schemes, knowledge of which can save you from financial losses.
The article analyzes statistical data regarding the dynamics of the development of phishing schemes in the Russian Federation. Social and economic factors that differentiate potential victims of fraudsters have also been identified, global statistics on phishing attacks for 2022–2024 have been reflected, and statistics on attacks through phishing sites and email campaigns have been predicted for 2025 using an exponential smoothing algorithm.

Keywords: internet fraud, artificial intelligence, phishing emails, phishing attacks.

Введение

С начала 2022 по август 2024 г. в России было совершено около 1,5 млн преступлений в ИТ-сфере. При этом кибермошенники похитили у россиян более 350 млрд руб. Такие данные в начале сентября 2024 г. раскрыл следственный департамент МВД РФ.

По оценкам финансовых аналитиков, в РФ в 2023 г. и первой половине 2024-го наибольшее количество атак пришлось на промышленные предприятия (11%), телекоммуникации (10%), госучреждения (9%) и ИТ-компании (7%). Эксперты установили, что основными последствиями успешных атак на организации стали утечки конфиденциальной информации (41%) и нарушение основной деятельности (37%). Атаки на частных лиц чаще всего заканчивались утечкой чувствительных данных (69%) и непосредственным финансовым ущербом (32%). В 2023 г. в России было совершено около 680 тыс. преступлений с использованием информационных технологий, что на 30% больше, чем годом ранее. Ущерб от них превысил 156 млрд руб. Об этом президент РФ Владимир Путин сообщил 2 апреля 2024 г. на заседании коллегии Министерства внутренних дел России.

Материалы и методы

Основные этапы исследования:

- проведен анализ основных фишинговых схем мошенничества;
- произведено сравнение статистических данных о произведенных фишинговых атаках в мире за 2022–2024 гг., на основе которых построены соответствующие линии трендов;
- используя алгоритм экспоненциального сглаживания, дан прогноз относительно количества фишинговых атак на 2025 г.

Результаты

Существует огромное количество фишинговых схем, все из них описать невозможно. К самым распространенным относятся:

- мошенники присылают письмо с поддельного адреса и приглашают войти в систему для того, чтобы восстановить аккаунт, который якобы за-

блокирован из соображений безопасности. В случае перехода по ссылке, ваши данные к учетной записи *Microsoft* похищаются;
- письмо об удалении файлов от *Microsoft Office*. Вам приходит сообщение, в котором оповещают об удалении из аккаунта большого объема файлов. Для того чтобы их восстановить, предлагается ссылка, переход по которой приводит к утечке ваших учетных данных;
- поддельное сообщение от банка, в котором предложена ссылка на веб-форму для внесения реквизитов карты или счета для верификации аккаунта. Такие ссылки надо всегда игнорировать и оповестить банк о подобных мошеннических письмах;
- письма от друзей. Злоумышленник представляются вашим знакомым, которому очень нужна помощь в виде денежного перевода. В этом случае, прежде чем отправить средства, позвоните другу с целью личного подтверждения информации;
- сообщение о получении выигрыша или наследства от дальнего родственника, которое также содержит ссылку для внесения конфиденциальной информации, реквизитов и данных, якобы необходимых для получения приза или верификации права на наследство;
- обещание возврата налога или получения бонуса. Данная схема наиболее популярна ввиду своей актуальности, поскольку налоги обязаны платить большинство граждан. Письмо может содержать как обещание возврата денежных средств, так и обращение с претензией от налоговой инспекции. Для оформления возврата необходимо указать свои полные данные в запросе и заполнить налоговую декларацию. После этого злоумышленники либо похищают ваши деньги, либо продают ваши личные данные третьим лицам, либо и то и другое [1, с. 57].

На сегодняшний день огромное количество компаний и даже частных пользователей подвергаются фишинговым атакам, целью которых является незаконный сбор конфиденциальных данных. Наиболее часто мошенники применяют:
- копье-фишинг — адресная форма фишинговой атаки, когда вредоносное письмо отправляется конкретному сотруднику, про которого у мошенников собрана информация и не составляет никакого труда составить письмо так, что оно максимально актуально, приходит от якобы легитимного источника, поэтому «жертве» крайне сложно различить обман, настолько все выглядит правдоподобно;
- фишинг китов. В качестве объекта мошенничества выбираются высокопоставленные руководители, знаменитости или топ-менеджеры. Целью также является завладение личными или профессиональными данными;
- фишинг электронной почты. Жертва получает письма, содержание которых для нее актуально, например, они содержат информацию от налоговых служб, банков или медицинских учреждений. Отправитель тоже кажется ей известным. Поэтому такие письма, как правило, спокойно открываются, осуществляется переход по имеющимся ссылкам и скачивается нужная мошенникам информация;
- фишинг при помощи клонирования. мошенники создают максимально похожую копию на ранее доставленные письма, которые содержат какие-либо вложения или ссылки, затем производится их подмена на вирусные, при этом отличить их от оригинала практически невозможно. Переход по ссылке грозит захватом систем компании, фишер пользуется этим и может использовать данные обманутого сотрудника, сделав его легитимным отправителем для отправки фишинговых писем другим сотрудникам компании. Невидящие пользователи либо кликают на ссылку, либо открывают вложение, позволяя злоумышленникам захватить их системы. После этого фишер может подделать личность жертвы, маскируясь под надежного отправителя для других жертв в той же организации;
- фишинг с использованием голоса (вишинг). Мошенники по телефону связываются с жертвой, представляются официальными лицами и грамотно провоцируют раскрыть свои личные данные или перевести денежные средства;
- *SMS*-фишинг. В качестве канала связи выступают СМС-сообщения, содержащие мошеннические ссылки. Подобно вишингу, СМС-фишинг отправляет мошеннические сообщения с призывом к получателям перейти по вредоносным ссылкам или предоставить личные данные [5, с. 77];
- «ловля сома», или кетфишинг. Схема, при которой мошенниками создаются ложные аккаунты якобы реально существующей личности, как правило, платформой выступают социальные сети или сайты знакомств, данная офлайн-личность старается завести любовные или дружеские отношения и затем обманом вытягивает деньги или получает доступ к личным данным [2, с. 200].

Анализ данных различных исследований позволяет сделать вывод, что более 50% жертв фишинга стали таковыми посредством автоматизированного

фишинга с использованием искусственного интеллекта, который открыл новые границы для мошенников, позволяя создавать визуальный образ, включая фотографии или даже видео с обращением от того, кому доверяет жертва [3, с. 133]. Увидев фото знакомого или опубликованное видео, на котором от просит вас о помощи, вряд ли кто-то захочет осуществлять дополнительную проверку и может легко отправить личные данные или денежные средства.

Используя вышеперечисленные фишинговые схемы, мошенники похитили у россиян и вывели за пределы страны более 350 млрд руб. В частности, за семь месяцев 2024 г. ущерб от подобных преступлений в России составил 99 млрд руб., а за весь 2023 г. — около 156 млрд руб. В январе–июле 2024-го зарегистрированы 577 тыс. ИТ-преступлений, из которых 437 тыс. — это мошенничество и хищения. По оценкам Банка России, мошенники похитили у россиян в 2023 г. 15,8 млрд руб., а в первом квартале 2024-го — 4,3 млрд руб.

Рассмотрим статистику за 2022–2024 гг., предоставляемую международным консорциумом по борьбе с фишингом *Anti-Phishing Working Group* (*APWG*). Стоит отметить, что данная организация на сегодняшний день является мировым лидером по борьбе с фишинговыми опасностями и осуществляет свою деятельность совместно с такими мировыми IT-гигантами, как *Microsoft, PayPal, Adobe* и др. Консорциум *APWG* регулярно предоставляет комплексную статистику о современных киберугрозах, в том числе данные компании выступают в качестве источников информации и статистики по фишинговым атакам [6].

На основе вышеперечисленных данных построим диаграммы и линии тренда по статистике уникальных фишинговых веб-сайтов и фишинговых веб-атак за период 2022–2024 гг.

Из полученной статистики и построенных графиков видно, что имеется тенденция к тому, что как атаки через фишинговые веб-сайты, так и через e-mail-рассылки имеют тенденцию к снижению. Причиной этому служат повышение уровня грамотности интернет пользователей, улучшение средств защиты от подобного рода атак, а также широкое использо-

Таблица 1

Общемировая статистика фишинговых атак за 2022 г.

	Янв.	Февр.	Март	Апр.	Май	Июнь	Июль	Август	Сент.	Окт.	Нояб.	Дек.
Уникальные фишинговые веб-сайты (атаки)	331 698	309 979	384 291	362 852	353 242	381 717	425 112	430 141	415 630	440 508	450 390	459 139
Фишинговые кампании по электронной почте	15 275	14 176	24 187	21 540	20 339	23 550	64 696	38 228	23 994	101 104	77 469	74 250
Бренды, подвергшиеся фишинговым атакам	608	621	673	621	612	637	621	612	637	599	610	577

Таблица 2

Общемировая статистика фишинговых атак за 2023 г.

	Янв.	Февр.	Март	Апр.	Май	Июнь	Июль	Август	Сент.	Окт.	Нояб.	Дек.
Уникальные фишинговые веб-сайты (атаки)	495 690	509 394	619 060	597 789	381 572	306 847	327 294	331 962	340 700	356 538	350 776	370 187
Фишинговые кампании по электронной почте	40 863	45 259	40 742	41 083	30 717	22 610	29 110	32 162	32 740	22 750	24 621	20 642
Бренды, подвергшиеся фишинговым кампаниям	561	549	576	544	521	498	477	499	508	477	442	420

Таблица 3

Общемировая статистика фишинговых атак за 2024 г.

	Янв.	Февр.	Март	Апр.	Май	Июнь	Июль	Август	Сент.
Уникальные фишинговые веб-сайты (атаки)	358 107	314 974	290 913	318 651	292 428	266 457	289 324	301 507	342 092
Фишинговые кампании по электронной почте	50 837	24 086	41 550	31 005	33 874	31 173	33 424	27 643	25 358
Бренды, подвергшиеся фишинговым кампаниям	314	309	301	324	320	301	299	315	322

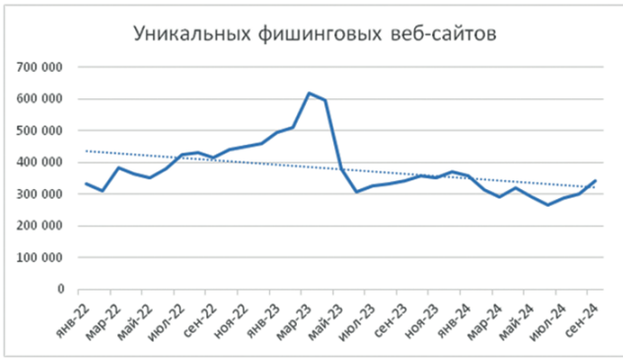

Рис. 1. График и линия тренда уникальных фишинговых веб-сайтов

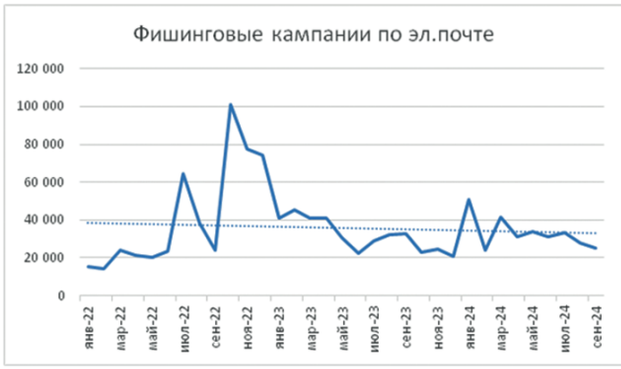

Рис. 2. График и линия тренда уникальных фишинговых e-mail-рассылок

вание в качестве каналов для интернет-мошенничества социальных сетей и мессенджеров.

С помощью алгоритма экспоненциального сглаживания спрогнозируем статистику по атакам через фишинговые сайты и почтовые рассылки на 2025 г.

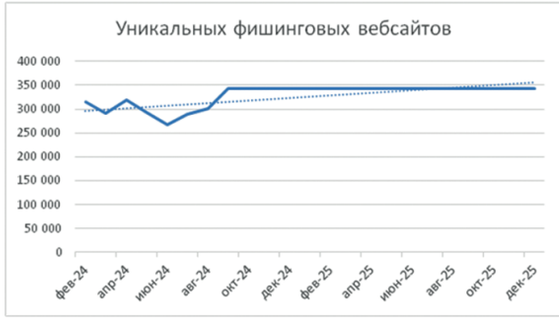

Рис. 3. График и линия тренда прогноза уникальных фишинговых веб-сайтов в 2025 г.

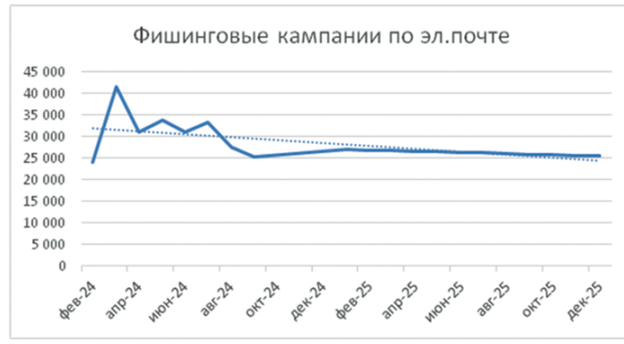

Рис. 4. График и линия тренда прогноза уникальных фишинговых e-mail-рассылок в 2025 г.

По спрогнозированным данным можно сделать вывод, что в 2025 г. количество фишинговых веб-сайтов будет незначительно, но расти, в то время как количество фишинговых e-mail-рассылок будет снижаться. Уменьшение вредоносных рассылок по электронной почте можно объяснить, как было сказано ранее, повышенной активностью мошенников в социальных сетях и мессенджерах.

Выводы

В феврале 2024 г. МВД РФ сообщало, что в 2023 г. в стране было зафиксировано 677 тыс. ИТ-преступлений против 522,1 тыс. годом ранее. По оценкам министерства, количество правонарушений с применением Интернета в 2023 г. выросло с 381 тыс. до 526,7 тыс. Следом идут преступления, совершённые с использованием средств мобильной связи и пластиковых карт. Увеличилось и число правонарушений с применением компьютерной техники, программных средств и фиктивных электронных платежей.

В МВД перечислили пять регионов, которые по итогам 2023 г. лидировали по темпам роста числа ИТ-преступлений: Ненецкий автономный округ, Калмыкия, Ингушетия, Новгородская и Калининградская области.

Следует признать, что схемы мошенников становятся все сложнее, они активно используют методы социальной инженерии, заставляя граждан добровольно отдавать свои средства, задействуют новые приемы обмана. Украденные при помощи фишинга

Таблица 4

Прогноз статистики фишинговых атак на 2025 г.

	Янв.	Февр.	Март	Апр.	Май	Июнь	Июль	Август	Сент.	Окт.	Нояб.	Дек.
Уникальные фишинговые веб-сайты (атаки)	342 493	342 616	342 739	342 862	342 984	343 107	343 230	343 353	343 475	343 598	343 721	343 844
Фишинговые кампании по электронной почте	27 106	26 961	26 816	26 671	26 527	26 382	26 237	26 092	25 947	25 803	25 658	25 513
Бренды, подвергшиеся фишинговым атакам	318	317	316	315	314	313	312	311	310	309	308	307

персональные данные позволили мошенникам в январе–марте 2023 г. провести 252,1 тыс. операций без согласия клиентов.

Из украденных 4,5 млрд руб. в первой четверти 2023 г. российские банки смогли вернуть клиентам только 4,3% средств. Годом ранее эта доля была больше и составляла 6,2%. Банк России не раз объяснял, что такой низкий уровень возврата похищенных средств связан с высокой долей социальной инженерии, когда граждане самостоятельно переводят средства злоумышленникам или раскрывают банковские данные. В таких случаях хищения банки по закону не обязаны возвращать деньги. В связи с этим мы видим серьезную необходимость совершенствования механизмов борьбы с фишинговыми правонарушениями.

Литература

1. *Тарасова Ю.А*. Анализ проблемы фишинга в цифровом пространстве [Текст] / Ю.А. Тарасова // Международный журнал прикладных и фундаментальных исследований. — 2023. — № 11. — С. 56–60.
2. *Крюкова И.В.* Фишинг как вид интернет-мошенничества [Текст] / И.В. Крюкова, Э.Н. Алимамедов // Наукосфера. — 2021. — № 2–2. — С. 196–201.
3. *Чернышева А.В*. Фишинг как угроза современному информационному обществу [Текст] / А.В. Чернышева, С.И. Самойлов // Научный потенциал. — 2021. — № 3. — С. 131–136.
4. *Селиверстов В.В*. Анализ актуальности и состояния современных фишинг-атак на объекты критической информационной инфраструктуры [Текст] / В.В. Селиверстов, С.А. Корчагин // Инженерный вестник Дона. — 2024. — № 6.
5. *Стеценко Ю.А*. Мошенничество в сети Интернет [Текст] / Ю.А. Стеценко, Н.С. Холодковская // Вестник Таганрогского института имени А.П. Чехова. — 2021. — № 2. — С. 75–80.
6. Рабочая группа по борьбе с фишингом (APWG) офиц. сайт. — URL: https://apwg.org/trendsreports

References

1. Tarasova Yu.A. Analysis of the problem of phishing in the digital space // International Journal of Applied and Fundamental Research. 2023, no. 11, pp. 56–60. (in Russian)
2. Kryukova I.V., Alimamedov E.N. Phishing as a type of Internet fraud // Naukasphere. 2021, no. 2-2, pp. 196–201. (in Russian)
3. Chernysheva A.V., Samoilov S.I. Phishing as a threat to the modern information society // Scientific potential. 2021, no. 3, pp. 131–136. (in Russian)
4. Seliverstov V.V., Korchagin S.A. Analysis of the relevance and state of modern phishing attacks on critical information infrastructure objects // Engineering Bulletin of the Don. 2024, no. 6.
5. Stetsenko Yu.A., Kholodkovskaya N.S. Fraud on the Internet // Bulletin of the Taganrog Institute named after A.P. Chekhov. 2021, no. 2, pp. 75–80.
6. Anti-Phishing Working Group (APWG) official website. URL: https://apwg.org/trendsreports