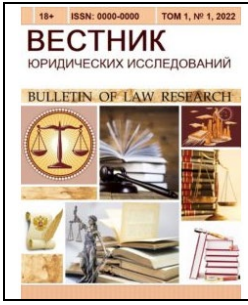

Научно-исследовательский журнал ***«Вестник юридических исследований / Bulletin of Law Research»***
https://blr-journal.ru
2025, Том 4, № 6 / 2025, Vol. 4, Iss. 6 https://blr-journal.ru/archives/category/publications
Научная статья / Original article
УДК 343.98

Опасность: киберугрозы и фишинговые сайты

[1] Хачатурова С.С.,
[1] Российский экономический университет имени Г.В. Плеханова

Аннотация: целью данной работы является изучение одной из ключевых проблем современности — *киберпреступлений и фишинга*. Работа направлена на выявление последствий существующих видов угроз, ознакомление пользователей Интернета с современными способами мошенничества, повышение цифровой грамотности и обеспечение надежной защиты персональных данных.

Автор отмечает, что с приходом новых технологий вместе с простотой выполнения повседневных задач и быстротой связи посредством телефона, мессенджеров и интернета в целом, пришла новая угроза под названием – *киберпреступность*. Эффективность противодействия снижается из-за низкой информированности пользователей и постоянного появления новых форм мошеннических схем, нацеленных на получение конфиденциальной информации с целью последующей эксплуатации её в преступных целях. Несмотря на рост числа жертв киберпреступлений и угроз, пока отсутствуют проверенные и эффективные методы для борьбы с подобными преступлениями. Тем не менее правительства разных стран предпринимают активные шаги для решения указанных проблем.

Очевидно, что даже простая утечка персональных данных может грозить негативными экономическими последствиями. Злоумышленники могут шантажировать жертву, вымогать деньги, взламывать счета в банках [10]. Наибольшую сложность вызывает возможность потери доступа к учетной записи и контроля над личной информацией без восстановления.

В статье приводятся разновидности *киберпреступлений* и способы борьбы с ними, особенности и типы фишинговых сайтов, а также способы защиты личной информации. Автор подчеркивает, что особые меры предосторожности сэкономят время, финансы и здоровье граждан.

Ключевые слова: киберпреступления, фишинг, фишинговые сайты, угроза, информационное общество, Интернет-мошенничество, информационная безопасность

Для цитирования: Хачатурова С.С. Опасность: киберугрозы и фишинговые сайты // Вестник юридических исследований. 2025. Том 4. № 6. С. 75 – 79.

Поступила в редакцию: 9 сентября 2025 г.; Одобрена после рецензирования: 5 ноября 2025 г.; Принята к публикации: 25 декабря 2025 г.

Danger everywhere: cyber threats and phishing sites

[1] Khachaturova S.S.,
[1] Plekhanov Russian University of Economics

Abstract: the purpose of this paper is to examine one of the key contemporary problems—*cybercrime and phishing*. It aims to identify the consequences of existing threats, familiarize internet users with modern fraud methods, improve digital literacy, and ensure reliable protection of personal data.

The author notes that with the advent of new technologies, along with the ease of performing everyday tasks and the speed of communication via telephone, instant messaging, and the internet in general, has emerged a new threat called *cybercrime*. The effectiveness of countermeasures is diminished by low user awareness and the constant emergence of new fraudulent schemes aimed at obtaining confidential information for subsequent criminal exploitation. Despite the growing number of victims of cybercrime and threats, proven and effective methods for combating such crimes are still lacking. Nevertheless, governments around the world are taking active steps to address these issues.

Clearly, even a simple leak of personal data can have negative economic consequences. Attackers can blackmail victims, extort money, and hack bank accounts [10]. The greatest challenge is the potential loss of account access and control over personal information without recovery.

This article describes the types of *cybercrime* and how to combat them, the characteristics and types of phishing sites, and ways to protect personal information. The author emphasizes that special precautions will save citizens time, money, and health.

Keywords: cybercrime, phishing, phishing sites, threat, information society, internet fraud, information security

For citation: Khachaturova S.S. Danger everywhere: cyber threats and phishing sites. Bulletin of Law Research. 2025. 4 (6). P. 75 – 79.

The article was submitted: September 9, 2025; Approved after reviewing: November 5, 2025; Accepted for publication: December 25, 2025.

Введение

В эпоху стремительной цифровой трансформации, когда информационные технологии глубоко проникают во все сферы жизнедеятельности современного общества, включая и юридическую практику, пропорционально возрастает и риск киберпреступлений. Этот процесс, охватывающий все от повседневных коммуникаций до сложных финансовых операций, создает благоприятную почву для развития новых форм киберугроз, направленных на хищение данных, мошенничество и нанесение ущерба как частным лицам, так и организациям.

Стоит заметить, что различные государства предлагают разные трактовки понятию *киберпреступление,* исходя из особенностей своего законодательства.

Например, в США под *киберпреступлениями* понимаются любые противоправные нарушения законодательства с помощью информационных девайсов, имеющих соединение с сетью. Такие преступления подразделяются на три категории, когда электронная техника является: целью, оружием и источником хранения.

Законодательство Федеративной Республики Германия относит данные виды преступления к имущественным, но с учетом использования технических устройств, как средства совершения правонарушения.

Российское законодательство обладает рядом правовых инструментов, которые позволяют осуществлять эффективное противодействие киберпреступлениям, защищая интересы граждан, организаций и государства в целом. Эти инструменты включают в себя положения Уголовного кодекса Российской Федерации, предусматривающие ответственность за различные виды преступлений, которые могут быть совершены с использованием киберугроз.

Материалы и методы исследований

Для изучения *киберпреступлений* и *фишинга* используются разнообразные научные и практические методы, такие как анализ кейсов и судебной практики, использование специальных инструментов и программного обеспечения, позволяющие выявить следы преступной активности, а также возможности восстановления удаленных файлов и исследования механизмов распространения вредоносного программного обеспечения.

Методы исследований позволяют комплексно изучить природу *киберпреступлений* и *фишинговых атак*, а также разработать эффективные меры безопасности, профилактики и противодействия проблемным деяниям.

Киберпреступление определяется как преступная деятельность, в рамках которой компьютер, компьютерная сеть или сетевое устройство являются либо целью, либо инструментом для совершения других противоправных действий [4].

Статья 159 Уголовного кодекса Российской Федерации [9], посвященная мошенничеству, играет ключевую роль в преследовании киберпреступлений, поскольку определяет противоправные действия, направ-

ленные на хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Статья 273 Уголовного кодекса Российской Федерации [9], озаглавленная «Создание, использование и распространение вредоносных компьютерных программ», играет важную роль в борьбе с фишингом, поскольку значительная часть фишинговых атак связана с применением вредоносного программного обеспечения (ПО). Завладение данными пользователей – это ключевая цель фишеров, и для достижения этой цели они нередко прибегают к разработке, распространению и использованию вредоносных программ, способных причинить существенный вред компьютерным системам и информации, хранящейся на них [5].

Жертвой правонарушителей в сети Интернет становятся люди независимо от возраста, образования или профессиональной деятельности. Граждане и организации, пострадавшие от фишинговых атак и понесшие в результате имущественный ущерб или моральный вред, обладают законным правом на защиту своих интересов и вправе обратиться в суд с исками к лицам, совершившим данные преступные действия, с требованием о возмещении причиненных убытков и компенсации морального вреда. Этот механизм правовой защиты позволяет жертвам фишинга добиваться восстановления своих нарушенных прав и компенсации понесенных потерь, независимо от привлечения виновных лиц к уголовной ответственности [3].

Результаты и обсуждения

Фишинг – это вид *киберпреступлений*, в основе которого лежит добыча конфиденциальной информации жертв, посредством создания фальшивых веб-сайтов, массовой рассылки писем с вложениями или ссылками, при переходе по которым происходит заражение программного обеспечения девайса.

Фишинг-мошенничество увеличивается с каждым месяцем. В настоящее время фишинговая атака нацелена на аудиторию, размер которой варьируется в широких пределах – от массовых рассылок (до миллионов адресов электронной почты по всему миру) до целевых групп клиентов, перечисленных на небольших по размерам розничных веб-сайтах с кликами, имеющих пробелы в области безопасности [1].

Мошенники создают благоприятную атмосферу с жертвой, воздействуя на ее психологическую сторону, посредством втирания в доверие с помощью убедительности слов, достоверной на первый взгляд информации или же создания условий, про которых пользователь должен мгновенно отреагировать во избежание пагубных последствий [6].

Одним из методов реализации *фишинга* является создание *фальшивых сайтов*. Обычно странички известных организаций требуют совершения платежей, поэтому именно их киберпреступникам выгодно в точности копировать, дабы невнимательный клиент переводил им свои денежные средства.

Социальные сети открывают перед мошенниками двери для массового распространения их посланий, к примеру, в личных сообщениях, в комментариях, в постах. Такие извещения содержат вредоносные ссылки или вложения, при переходе по которым осуществляется передача личных данных преступникам. Примером данного метода является вид *фишинга – Email/spam/smishing*, благодаря которому осуществляется массовое распространение сообщений.

Не стоит забывать о телефонных звонках, в которых злоумышленники уверяют жертву в вымышленных проблемах и агитируют незамедлительно решить ее с их помощью и необходимо предоставить персональные данные. Такой вид *фишинга* называется *Vishing*, что означает обман по телефону, голосовой фишинг, целью которого также являются добыча персональной информации.

Выделим основные методики и технику *фишинга* [7]:

- ✓ *spear phishing* – данный тип означает персональную рассылку. Сообщение с вирусной ссылкой или вложением отправляется определенному лицу в организации, чтобы создалась визуальная связь с отправителем и получателем для построения доверительных отношений в целях получения требуемой информации;
- ✓ *whaling* – суть данного вида *фишинга* заключается в вредоносных сообщениях с ссылками – вложениями, но нацеленными не на рядовых сотрудников, а на руководство организации, поскольку они, в свою очередь, имеют более обширный круг информации о компании. Чтобы привлечь внимание такого значимого лица, сообщение как правило содержит сверхважные данные, находящиеся в сфере его функциональных обязанностей.
- ✓ *BCO* – данный тип *фишинга* подразумевает под собой *аферу*, производимую злоумышленником, который незаконным образом получает доступ к аккаунту руководителя организации и впоследствии осуществляет рассылку писем подчиненным для осуществления денежного потока или с инструкцией на работу, которая нанесет компании большой ущерб.
- ✓ *clone Phishing* – данный тип подразумевает копирование письма из оригинального сервера. Злоумышленники подделывают точно такое же письмо, заменяя ссылки на вирусные, и отправляют его по-

вторно, якобы с того же официального канала. Вторую рассылку объясняют допущенными ошибками в первом письме, что, казалось бы, не должно создавать вопросов и вызывает чувство доверия.

- ✓ *evil twin phishing* - суть данного типа *фишинга* заключается в том, что мошенники создают фальшивую сеть Wi-Fi, которая является двойником оригинальной. Обычно, такие сети не зашифрованы паролем. Подключаясь к ней, пользователя перебрасывает на специальный мошеннический сайт, запрашивающий персональную информацию для осуществления входа. Получается, преступник захватывает данные, подключается к сети и получает необходимую ему информацию из-за незащищенности трафика.
- ✓ *Web Based Delivery* – это один из видов *фишинга*, который сложно предугадать. Правонарушитель находится между поддельной вирусной страницей и официальным сайтом, в котором покупатель проводит оплату за товар, но при этом не догадываясь о том, что мошенник все это время следит за его действиями, в результате чего получает информацию о данных банковской карты.
- ✓ *content injection* – данный вид *фишинга* осуществляется мошенником посредством замены части информации на сайте официального источника. Сложно предугадать, что ссылка на доверенных страничках может перенести пользователя с надежного ресурса на фишинговый сайт посредством заполнения персональными данными.

Выводы

Ознакомившись с серьезностью *киберпреступлений*, верным решением является принятие комплекса мер надежной защиты персональных данных от несанкционированного доступа:

- ✓ использование современных антивирусных программ;
- ✓ постоянное обновление программного обеспечения;
- ✓ бдительность при вводе и передаче личных данных по сети Интернет;
- ✓ проверка доменов сайтов перед введением платежных данных;
- ✓ использование проверенных Wi-Fi соединений, др.

Согласно мерам профилактики, предлагаемым «Лабораторией Касперского», необходимо использовать разные пароли к разным сайтам, рекомендуется воспользоваться двухфакторной аутентификацией, избегать чрезмерного общения в социальных сетях и мессенджерах [8], не переходить по ссылкам, полученным на электронную почту

Фишинговые атаки, нацеленные на личностей, могут нанести сильный урон. Само по себе незаконное присвоение доступа к данным третьими лицами является риском, поскольку мошенники наносят вред не только финансовому положению, но и моральному состоянию жертвы. Фотографии или видеоролики могут использоваться для публичной демонстрации, вызывая недопонимание окружающих или провоцируя травлю - буллинг. Такое поведение неизбежно оказывает негативное влияние на психическое состояние потерпевших, а для известных персон и публичных фигур подобный инцидент способен привести к значительным репутационным потерям, включая потерю статуса и доверия аудитории вследствие распространения ложной информации.

Фишинговые атаки осуществляются и в отношении организаций, нанося большой непоправимый ущерб. Компании отвечают за конфиденциальность данных клиентов, а при утечке этих сведений, организация может столкнуться с судебным разбирательством и потерей доверия со стороны потребителей. Потеря корпоративных данных, «перегрузка сайта» из-за которых организация не может исправно функционировать, тем самым теряя клиентов, вредят бизнесу, вплоть до его банкротства.

К сожалению, от фишинга не существует универсального, абсолютно надежного способа защиты, гарантирующего полную неприкосновенность личной информации. Однако, несмотря на это, существует целый ряд эффективных мер и практических рекомендаций, которые позволяют значительно снизить риск стать жертвой фишинга и обезопасить свои персональные данные. Главное оружие в борьбе с фишингом – это постоянная бдительность и критическое мышление при работе в интернете [2].

Эффективная борьба с киберпрестплениями требует комплексного подхода, сочетающего в себе технические, организационные и правовые меры. Важным фактором является повышение осведомленности пользователей о фишинговых угрозах и обучение их правилам безопасного поведения в интернете. Только совместными усилиями государственных органов, юридических организаций и частных лиц можно создать надежную систему защиты от фишинговых атак и обеспечить безопасность информационной среды.

Список источников

1. Акулич М. URL https://www.livelib.ru/book/390610/readpart-fishing-imarketing-margarita-akulich?ysclid=man02x3k3225787869. https://www.livelib.ru/book/390610/readpart-fishing-imarketing-margarita-akulich?ysclid=man02x3k3225787869 (дата обращения: 11.08.2025)
2. Антонова Т.С., Смирнов В.М. Фишинг как неизученное киберпреступление // StudNet. 2021. Т. 4. № 6.
3. Батюшкин М.В. "Фишинг" – компьютерное мошенничество? // Символ науки: международный научный журнал. 2021. № 1. С. 90 – 93.
4. Булгаков С.С., Поздняков А.Н. О новых терминах в сфере отечественной правоохранительной деятельности: "киберпреступность" // Труды Академии управления МВД России. 2022. № 4 (64). С. 76 – 82.
5. Гриднев Н.С. Профилактика киберпреступлений в Российской Федерации // Научный альманах «В зеркале права»: Сборник научных трудов. Липецк: Липецкий государственный педагогический университет им. П.П. Семенова-Тян-Шанского, 2024. С. 322 – 324.
6. Гусейнов Т.А. Проблемы и особенности расследования киберпреступлений // Вопросы российской юстиции. 2020. № 6. С. 348 – 357.
7. Кетов А.А., Смоленцева Л.В. Что такое фишинг и как от него защититься // Сборник трудов молодых ученых УВО "Университет управления "ТИСБИ": Сборник статей. Казань: Университет управления "ТИСБИ" (Татарский институт содействия бизнесу), 2022. С. 177 – 182.
8. Лаборатория Касперского»: официальный сайт [Электронный ресурс]. URL: https://www.kaspersky.ru/ (дата обращения: 26.03.2025)
9. Уголовный кодекс Российской Федерации // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/?ysclid=man142ywv1327451144 (дата обращения: 11.08.2025)
10. Ясуев И.Р., Евсвтефеев М.М., Верщицкая Г.В. Особенности расследования экономических киберпреступлений // Человек. Социум. Общество. 2023. № 5. С. 139 – 145.

References

1. Akulich M. URL https://www.livelib.ru/book/390610/readpart-fishing-imarketing-margarita-akulich?ysclid=man02x3k3225787869. https://www.livelib.ru/book/390610/readpart-fishing-imarketing-margarita-akulich?ysclid=man02x3k3225787869 (date of access: 11.08.2025)
2. Antonova T.S., Smirnov V.M. Phishing as an unstudied cybercrime. StudNet. 2021. Vol. 4. No. 6.
3. Batyushkin M.V. "Phishing" – computer fraud? Symbol of Science: International Scientific Journal. 2021. No. 1. P. 90 – 93.
4. Bulgakov S.S., Pozdnyakov A.N. On New Terms in the Sphere of Domestic Law Enforcement: "Cybercrime". Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia. 2022. No. 4 (64). P. 76 – 82.
5. Gridnev N.S. Prevention of Cybercrimes in the Russian Federation. Scientific Almanac "In the Mirror of Law": Collection of Scientific Papers. Lipetsk: Lipetsk State Pedagogical University named after P.P. Semenov-Tyan-Shansky, 2024. P. 322 – 324.
6. Guseinov T.A. Problems and Features of Cybercrime Investigation. Issues of Russian Justice. 2020. No. 6. P. 348 – 357.
7. Ketov A.A., Smolentseva L.V. What is phishing and how to protect yourself from it. Collection of works of young scientists of the UVO "University of Management "TISBI": Collection of articles. Kazan: University of Management "TISBI" (Tatar Institute for Business Assistance), 2022. P. 177 – 182.
8. Kaspersky Lab: official website [Electronic resource]. URL: https://www.kaspersky.ru/ (date of access: 03.26.2025)
9. Criminal Code of the Russian Federation. ConsultantPlus. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/?ysclid=man142ywv1327451144 (date of access: 08/11/2025)
10. Yasuev I.R., Evsvtefeev M.M., Vershchitskaya G.V. Features of the investigation of economic cybercrimes. Man. Society. Obshchestvo. 2023. No. 5. P. 139 – 145.

Информация об авторе

Хачатурова С.С., кандидат экономических наук, доцент, Российский экономический университет имени Г.В. Плеханова