Теоретические и прикладные аспекты кибербезопасности конвергентных когнитивно-информационных технологий

https://doi.org/10.25559/SITITO.021.202502.221-229
УДК 004.056

Осведомленность о фишинге – вопросы обучения

Д. Е. Намиот*, В. А. Васенин

ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова», г. Москва, Российская Федерация

Адрес: 119991, Российская Федерация, г. Москва, ГСП-1, Ленинские горы, д. 1

* dnamiot@gmail.com

Оригинальная статья

Аннотация

Фишинг уже в течение довольно длительного времени остается одной из самых опасных кибератак. Будучи технически простым подходом в реализации для атакующих, будучи довольно хорошо распознаваемым инструментальными средствами, обладая явно распознаваемыми признаками, этот способ атаки все равно остается работающим. Причина – это пользователи, которые продолжают переходить по подготовленным вредоносным ссылкам. Именно люди оказываются слабым звеном, которое и обеспечивает успех фишинга. Отсюда большое внимание, которое уделяется в мире образованию (уведомлению) пользователей об опасности и характерных признаках фишинга. В настоящей статье мы хотим остановиться на существующих в мире программах обучения противодействия фишингу. Такие программы существуют на разных уровнях: национальных, академических, в частных компаниях. Основа таких тренировок – это определение учащимися фишинговых сообщений среди реальных текстов (почтовых сообщений). Особый интерес представляет собой шкала фишинга от NIST, которая позволяет оценивать сложность таких тренировочных примеров.

Ключевые слова: кибербезопасность, фишинг, обучение

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Для цитирования: Намиот Д. Е., Васенин В. А. Осведомленность о фишинге – вопросы обучения // Современные информационные технологии и ИТ-образование. 2025. Т. 21, № 2. С. 221-229. https://doi.org/10.25559/SITITO.021.202502.221-229

© Намиот Д. Е., Васенин В. А., 2025

Контент доступен под лицензией Creative Commons Attribution 4.0 License.
The content is available under Creative Commons Attribution 4.0 License.

Theoretical and Applied Aspects of Cybersecurity of Convergent Cognitive Information Technologies

Phishing Awareness – Training Issues

D. E. Namiot*, V. A. Vasenin

Lomonosov Moscow State University, Moscow, Russian Federation

Address: 1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation

* dnamiot@gmail.com

Original article

Abstract

Phishing has been one of the most dangerous cyberattacks for quite a long time. Being a technically simple approach to implement for attackers, being quite well recognized by tools, having clearly recognizable features, this method of attack still remains operational. The reason is users who continue to follow prepared malicious links. It is people who turn out to be the weak link that ensures the success of phishing. Hence, much attention is paid in the world to educating (notifying) users about the dangers and characteristic features of phishing. In this article, we would like to focus on existing anti-phishing training programs in the world. Such programs exist at different levels: national, academic, in private companies. The basis of such training is the identification of phishing messages by students among real texts (email messages). Of particular interest is the NIST phishing scale, which allows you to assess the complexity of such training examples.

Keywords: cybersecurity, phishing, training

Conflict of interests: The authors declares no conflict of interest.

For citation: Namiot D.E., Vasenin V.A. Phishing Awareness – Training Issues. *Modern Information Technologies and IT-Education.* 2025;21(2):221-229. https://doi.org/10.25559/SITITO.021.202502.221-229

Введение

С 1 июня в России вступают в силу изменения в законодательстве, которые ужесточают меры ответственности за нарушения в области информационной безопасности. Увеличение штрафов, равно как и уголовная ответственность за утечки данных, а также новые требования к защите персональных данных – все это в очередной раз привлечет внимание к киберзащите.

Согласно данным экспертов, число атак вредоносных шифровальщиков увеличилось на 35-45% относительно аналогичного периода предыдущего года. Наблюдается также рост активности преступных организаций, занимающихся похищением секретной информации. Одной из возможных причин роста числа таких преступлений как раз и является изменение законодательства, регулирующего защиту личных сведений, которое вступает в действие с 1 июня 2025 года[1].

Кроме того, заметно усложнились методы хакеров, использующих приемы социальной инженерии – атаки с использованием фальшивых веб-ресурсов участились на 20-35%. Кибермошенники успешно применяют современные события и тематики в качестве приманки. Сейчас значительно возросло количество преступлений против компаний, что свидетельствует о перемене вектора внимания преступников от частных лиц к организациям.

Фишинговые атаки – это вредоносная мошенническая практика, которую используют киберпреступники, чтобы попытаться заставить жертву раскрыть конфиденциальную информацию, такую как имя пользователя, пароль, данные кредитной карты и многое другое. Эти мошенничества обычно осуществляются с помощью электронных писем, текстовых сообщений, телефонной/голосовой почты или веб-сайтов, которые кажутся полученными из надежных источников [1].

Фишинговые атаки с технической точки зрения, возможно, представляют собой один из самых простых способов кибератак. Привлекательный для атакованного текст и ссылка на вредоносный ресурс – и это все. Именно фишинговые атаки стали одним из первых применений генеративного Искусственного интеллекта (больших языковых моделей – LLM) в кибератаках [2]. При этом, как отмечается в литературе, основное, что привносят LLM – это масштабирование процесса [3]. Составлять заманчивые тексты стало проще и дешевле.

Распространению фишинга способствует и цифровизация. Когда-то, в англоязычной литературе отмечалось как большое «достижение» атакующих составление персональных посланий о проблемах с заказами на Amazon (крупнейшем на то время сайте электронной коммерции). Сегодня же практически все пользователи Интернет в России, например, являются клиентами Озон, Яндекс Маркет, Wildberries, так что отправка письма с информацией о проблемах с оплатой, заказом и т.п. будет выглядеть вполне естественно. Учитывая огромный объем утечек, нахождение имени адресата также не является проблемой. Часто сами цифровые сервисы подсказывают действия атакующим. Например, сайт Госуслуги начал рассылку уведомлений о поступлении счетов на оплату ЖКХ, указывая в письмах ссылку для входа. Очевидно, что такой сайт в России только один и нет необходимости указывать ссылку на него, провоцируя создание фишинговых рассылок. Банки, например, тратят много усилий на разъяснение того, что не нужно перезванивать «банковским служащим», а звонить нужно только по телефонам банка.

Фишинговые ссылки имеют вполне ясные и обычно явно представленные и легко различимые признаки (об этом пойдет речь во второй части статьи). Инструментальны средства, как правило, достаточно точно могут распознавать вредоносные ссылки. Тем не менее, пользователи продолжают переходить по таким ссылкам и фишинг работает. Именно конечные пользователи оказываются тем слабым звеном, которое и обеспечивает успех фишинга. Отсюда проистекает такое внимание к обучению (фактически – убеждению) пользователей внимательно относится к переходам по ссылкам. Одна из европейских учебных компаний так и назвалась "Think Before U Click" *(Подумайте, прежде чем кликнуть)*. Фактически – это необходимость выработки у конечных пользователей своего рода аналога Zero Trust в отношении переходов по ссылкам[2].

В настоящей статье мы хотим остановиться именно на обзоре существующих зарубежных программ обучения в направлении Phishing awareness, что можно перевести как Осведомленность о фишинге, которые существуют уже как на академическом, корпоративном и даже государственном уровне. Многие интересные элементы этих программ могут быть адаптированы и переиспользованы в локальном варианте [4-8]. Такого рода приложения появляются уже и на отечественном рынке, например, Phishman [18]. Другой пример – это сканер безопасности, описанный в работе [19]. Цель данного обзора – это ознакомление разработчиков с лучшими практиками и помощь в реализации Phishing awareness программ на отечественном рынке [9, 10]. Потребность в такого рода системах очевидна, количество (и качество) фишинговых атак растет, постегиваемое развитием LLM, а также уже и специализированных ИИ-агентов [20]. Помимо традиционных email-писем, растет фишинговое использование SMS (*smishing* [21]), QR-кодов [22], голоса (*vishing* [24]) и так называемого мошенничества с компрометацией деловой электронной почты (*BEC – Business Email Compromise scams*)[3].

Говоря о важности таких тренировок, можно отметить, что согласно обзору [25], на долю новых сотрудников приходится 25% случаев фишинга, несмотря на то, что они составляют менее 10% от общего числа

[1] Мельников К. Ужесточение законодательства и новые угрозы: как бизнесу адаптироваться к вызовам кибербезопасности в 2025 году [Электронный ресурс] // itWeek. 10.04.2025. URL: https://www.itweek.ru/security/article/detail.php?ID=231999&newspp=1&newsid=9950 (дата обращения: 30.04.2025).

[2] Zero Trust Architecture / S. Rose [et al.]. NIST Special Publication 800.207. NIST, 2020. https://doi.org/10.6028/NIST.SP.800-207

[3] Walker L. Who Bears the Risk of Loss When Your Business Email Is Hacked? An Overview of Business Email Compromise Scams and the Potential Risks // Com. L. World. 2023. No. 37. P. 34.

сотрудников. Сотрудники старшего возраста и нетехнический персонал подвержены фишинговым атакам чаще, чем молодые, технически подкованные работники.

Цель тренировок программ осведомленности – это научить пользователей распознавать фишинговые ссылки и информировать о них службы кибербезопасности. Последнее очень важно, поскольку позволяет отслеживать ведущиеся атаки и настраивать средства защиты. Поэтому эффективность тренировок оценивается именно по уведомлениям от пользователей.

Месяц кибербезопасности в Европе

Агентство Европейского союза по кибербезопасности (ENISA) сотрудничает с Комиссией и государствами-членами в проведении #CyberSecMonth: ежегодной кампании ЕС, посвященной продвижению кибербезопасности среди граждан и организаций ЕС и предоставлению актуальной информации по вопросам безопасности в Интернете посредством мероприятий по повышению осведомленности и обмена передовым опытом[4].

С момента первого мероприятия в 2012 году, Европейский месяц кибербезопасности объединяет европейцев под лозунгом «Кибербезопасность – это общая ответственность» для объединения в борьбе с киберугрозами. Каждый год кампания пропагандирует более безопасное использование Интернета для граждан ЕС, а организаторы предоставляют знания и инструменты для этого.

В 2020 году пандемия COVID19 изменила сферу деятельности ECSM, потребовав фундаментального перехода к цифровой среде. ENISA запустила амбициозную онлайн-кампанию под названием «Подумайте, прежде чем кликнуть» *(Think Before U Click)*, которая оказалась успешной и привлекла в три раза больше внимания, чем в предыдущем 2019 году. Всего было проведено 419 мероприятий (в основном онлайн) с увеличением охвата на 9,8 млн. пользователей и увеличением упоминаний на 265%.

В 2024 году темой месяца Кибербезопасности была как раз осведомленность о фишинге[5]. Отмечается, что ENISA считает важнейшим вопросом именно осведомленность о фишинге, поскольку фишинговые атаки являются одними из самых распространенных и эффективных методов, используемых киберпреступниками для кражи конфиденциальной информации. Учебные материалы и тесты для самопроверки доступны на сайте ENISA[6].

Опираясь на миссию ENISA по созданию надежной и кибербезопасной Европы, Агентство проводит кампании по повышению осведомленности для продвижения надлежащих практик кибербезопасности и содействия поведенческим и культурным изменениям. ENISA организует широкий спектр тематических кампаний в сотрудничестве с заинтересованными сторонами государственного и частного секторов, которые выступают в качестве мультипликаторов для обеспечения большего охвата.

С помощью этих кампаний ENISA не только распространяет и продвигает свою работу в конкретных областях кибербезопасности, но и обучает заинтересованные стороны и общественность нормативным разработкам и последним техническим достижениям. Ключевым направлением этих усилий является улучшение кибергигиены, предоставление отдельным лицам и организациям знаний и привычек, необходимых для выявления и смягчения повседневных киберрисков. Конечная цель – создание разнообразной, устойчивой и киберосведомленной экосистемы, где надлежащая кибергигиена внедрена как стандартная практика во всех секторах.

Помимо мероприятий месячника кибербезопасности, в программу осведомленности ENISA входят также инструменты для малого бизнеса и руководство по созданию собственных программ осведомленности в кибербезопасности *(AR-in-a-box)*.

Малые и средние предприятия (МСП) являются основой экономики ЕС. Они представляют 99% всех предприятий в ЕС и обеспечивают работой около 100 миллионов человек – отсюда и проистекает внимание к ним. На них также приходится более половины ВВП Европы, и они играют ключевую роль в добавлении стоимости во все секторы экономики ЕС. Они служат как факторами цифровой трансформации, так и основным элементом социальной структуры ЕС.

Пандемия COVID-19 заставила МСП переосмыслить свое цифровое мышление. Им пришлось принять меры по обеспечению непрерывности бизнеса, такие как адаптация к облачным сервисам, модернизация своих интернет-сервисов, улучшение своих веб-сайтов и предоставление сотрудникам возможности работать удаленно. ENISA опросила европейские МСП во время пандемии, наиболее распространенными выявленными киберинцидентами были атаки с использованием программ-вымогателей, кража ноутбуков, фишинговые атаки и мошенничество со стороны генеральных директоров. Из числа опрошенных ENISA МСП 90% заявили, что проблемы кибербезопасности окажут серьезное негативное влияние на их бизнес в течение недели после возникновения проблем, а 57% заявили, что, скорее всего, обанкротятся или прекратят свою деятельность.

В период увеличения удаленной работы и роста киберугроз МСП сталкиваются с серьезными проблемами кибербезопасности. Низкий бюджет безопасности, отсутствие навыков кибербезопасности и рост кибератак могут серьезно повлиять на конкурентоспособность МСП и поставить под угрозу цепочку создания стоимости, к которой они подключены. Вот почему для МСП принципиально важно начать предпринимать правильные шаги для защиты своего бизнеса.

ENISA последовательно продвигает инициативы, помогающие МСП интегрировать кибербезопасность в

[4] European Cybersecurity Month [Электронный ресурс] // ENISA, 2025. URL: https://www.enisa.europa.eu/topics/cyber-hygiene/european-cybersecurity-month (дата обращения: 30.04.2025).
[5] Phisihn awareness [Электронный ресурс] // Health Service Executive, 2025. URL: https://www.ehealthireland.ie/news-media/news/2024/cyber-security-and-phishing-awareness/ (дата обращения: 30.04.2025).
[6] European Cybersecurity Month [Электронный ресурс] // ENISA, 2025. URL: https://www.enisa.europa.eu/topics/cyber-hygiene/european-cybersecurity-month (дата обращения: 30.04.2025).

свою цифровую среду. На протяжении многих лет Агентство предоставляло практические инструменты, методологии и рекомендации для поддержки МСП в решении проблем и возможностей кибербезопасности. Эти усилия включают ресурсы по оценке рисков, непрерывности бизнеса, безопасности облачных вычислений и защите данных, чтобы предоставить МСП знания, необходимые для защиты их операций.

ENISA выпустило ряд советов, которые помогут предприятиям противостоять быстро меняющейся цифровой сфере во время пандемии: Советы по выбору и использованию инструментов онлайн-коммуникации; Советы по кибербезопасности при покупке и продаже в Интернете; Советы по кибербезопасности при работе из дома; Десять лучших советов по кибергигиене для МСП во время пандемии COVID-19. Агентство ЕС по кибербезопасности и Национальный альянс по кибербезопасности опубликовали совместный контрольный список для МСП в ноябре 2020 года, предлагая предприятиям по обе стороны Атлантики базовое руководство по поддержанию цифровой безопасности. В 2021 году ENISA сосредоточилось на выпуске структурированных публикаций для поддержки МСП в защите сотрудников и предприятий от кибератак: отчет «Кибербезопасность для МСП – проблемы и рекомендации», руководство по кибербезопасности для МСП – 12 шагов к защите вашего бизнеса и инструмент SecureSME. Инструмент «SecureSME» – это новый интерактивный онлайн-инструмент, специально разработанный для МСП. Инструмент призван оказать практическую поддержку МСП в навигации по различным советам, руководствам, инструментам, отчетам и рекомендациям ENISA. Он будет действовать как единый центр для МСП в Европе, поддерживая их рекомендациями и руководствами по кибербезопасности в удобной и простой форме.

AR-in-a-Box – это комплексное решение для мероприятий по повышению осведомленности о кибербезопасности, разработанное для удовлетворения потребностей государственных органов, операторов основных услуг, а также крупных и малых частных компаний. Набор теоретических и практических знаний о том, как разрабатывать и внедрять эффективные программы повышения осведомленности о кибербезопасности, в том числе:

- Руководство по созданию индивидуальных программ повышения осведомленности для внутреннего использования в организации.
- Руководство по созданию целевых кампаний по повышению осведомленности для внешних заинтересованных сторон.
- Инструкции по выбору соответствующих инструментов и каналов для эффективного охвата целевой аудитории.
- Инструкции по разработке ключевых показателей эффективности для оценки эффективности программы или кампании.
- Руководство по разработке стратегии коммуникации, имеющей решающее значение для достижения целей повышения осведомленности.
- Викторина по повышению осведомленности для проверки понимания и усвоения ключевой информации.
- Игра по повышению осведомленности, представленная в разных версиях и стилях, а также руководство по игре.

С помощью AR-in-a-Box ENISA предоставляет организациям необходимые инструменты и ресурсы для эффективного повышения осведомленности о кибербезопасности в рамках их деятельности, предлагая динамическое решение, которое будет регулярно обновляться и обогащаться.

Примером поддерживаемой ENISA программы служит проект NERO [23]. Это инструментарий кибербезопасности для малого бизнеса, который, среди прочего, содержит и учебные программы, которые разделены на две отдельные группы: обучение на основе геймификации и киберполигоны.

В рамках NERO обучение на основе геймификации использует захватывающие игровые сценарии и симуляции для передачи базовых знаний в области киберзащиты, одновременно совершенствуя навыки принятия решений пользователями при выявлении и реагировании на кибератаки.

С другой стороны, киберполигоны NERO предоставляют динамическую моделируемую среду, специально разработанную для тестирования и совершенствования защитных стратегий от имитируемых кибератак. Это позволяет организациям эффективно оценивать и укреплять свои механизмы реагирования.

Академические программы

Примером академической программы является Программа осведомленности о фишинге в университете Стэнфорда[7]. Цель программы – помочь сообществу Стэнфорда защитить себя и университет, научившись распознавать вредоносные электронные письма. Программа повышения осведомленности о фишинге состоит из трех основных аспектов: имитация фишинговых писем, информирование и возможности обучения.

Письма-имитации фишинга периодически отправляет участвующим аудиториям электронные письма, которые напоминают фишинговые сообщения. Этот метод предназначен для создания безопасной образовательной среды, в которой получатель может практиковать идентификацию фишинговых писем без каких-либо штрафных санкций в случае нажатия на ссылку. Индивидуальные результаты никогда не разглашаются.

Постоянные информационные ресурсы и сообщения программы по оповещению о фишинге предназначены для того, чтобы держать пользователей в курсе событий. Например, там содержатся уведомления об атаках (рис. 1) и различные информационные материалы. Например:

- Анатомия фишингового письма
- Недавние примеры фишинга и т.д.

Здесь же находятся ссылки на учебные курсы (тренировочные программы).

[7] Stanford Phishing Awareness Program [Электронный ресурс] // Stanford University, 2025. URL: https://uit.stanford.edu/service/phishingawareness (дата обращения: 30.04.2025).

Схожая программа в Гарварде[8] базируется на имитации фишинга. Авторы отмечают, что когда дело доходит до обнаружения фишинговых писем, важна практика. Имитационные упражнения по осведомленности о фишинге и отчетности разработаны для того, чтобы дать сообществу Гарварда опыт распознавания фишинговых сообщений. Эти упражнения предоставляют имитацию фишинга на основе реальных попыток фишинга, обнаруженных в университете. То есть, основой упражнений служит пополняемая коллекция реальных фишинговых писем.

Р и с. 1. Программа Стэнфордского университета по повышению осведомленности о фишинге[9]
F i g. 1. Stanford Phishing Awareness Program

Структура предлагаемых тренингов примерно одинакова:

- Что такое фишинг?
- Типы фишинговых атак
- Результаты успешных фишинговых атак (к чему они могут привести)
- Советы по выявлению фишинга
- Примеры фишинговых писем
- Лучшие практики

NIST – осведомленность о фишинге

Материалы NIST, конечно, всегда имеют особую ценность. В данном случае речь идет о шкале фишинга от NIST в работе[10]. Встроенные программы обучения по повышению осведомленности о фишинге, в рамках которых сотрудникам рассылаются имитированные фишинговые письма, предназначены для подготовки сотрудников этих организаций к борьбе с реальными сценариями фишинга. Специалисты по кибербезопасности и обучению повышению осведомленности о фишинге используют результаты этих программ, в частности, для оценки риска безопасности своих организаций. Шкала фишинга NIST – это метод, разработанный для этих специалистов по оценке сложности обнаружения фишинга в электронных письмах, совершаемого человеком, в рамках их программ обучения по кибербезопасности и фишингу. В данном руководстве пользователя полностью излагается шкала фишинга, а также содержатся инструкции по ее применению к фишинговым письмам. Кроме того, приложения включают в себя:

1) рабочие листы, помогающие специалистам по обучению применению шкалы фишинга,
2) подробную информацию о свойствах электронных писем и связанных с ними исследованиях в литературе.

Как результат – хорошее руководство по составлению тренировочных писем.

Шкала фишинга состоит из двух основных компонентов, используемых совместно для определения сложности обнаружения фишинга человеком [11]:

1. Система оценки наблюдаемых характеристик самого фишингового письма.
2. Система оценки соответствия предпосылки фишингового письма целевой аудитории.

Первый компонент измеряется путем оценки визуальных индикаторов (сигналов), присутствующих в письме, которые могут предупредить получателей письма о фишинге, таких как количество сигналов, характер сигналов и их повторение. Второй компонент – соответствие предпосылке – основан на текущих событиях, организационной среде, а также ролях и обязанностях получателя. Оба компонента сначала измеряются, а затем интерпретируются совместно, что приводит к общему рейтингу сложности обнаружения фишингового письма человеком.

Первый компонент шкалы фишинга представляет собой систему оценки наблюдаемых характеристик самого фишингового письма, называемых сигналами электронной почты [11].

Сигналы – это свойства электронного письма, которые либо побуждают пользователя кликнуть на мошенническую ссылку или вложение, либо предупреждают пользователя о том, что письмо может быть фишинговым. Меньшее количество сигналов в фишинговом письме указывает на то, что письмо сложнее распознать как фишинговое; большее количество сигналов указывает на более легкое распознавание.

Сигналы в электронном письме дают объективную оценку самого письма; количество сигналов, присутствующих в электронном письме, классифицируется в этом компоненте шкалы фишинга. Эта категория сигналов наряду с категорией соответствия предпосылке электронного письма используются для определения сложности обнаружения. При классификации количества сигналов в фишинговом письме важно сначала понять типы сигналов, которые могут присутствовать в фишинговом письме, а также где они встречаются.

Сигналы фишинговых писем делятся на пять типов [11]:

1. Ошибки – связанные с орфографическими и грамматическими ошибками и несоответствиями, содержащимися в сообщении;
2. Технические индикаторы – относящиеся к адресам электронной почты, гиперссылкам и вложениям;
3. Индикаторы визуального представления – относящиеся к брендингу, логотипам, дизайну и форматированию;
4. Язык и содержание – например, стандартное приветствие и отсутствие данных подписчика, использование цейтнота и угрожающего языка;
5. Распространенные тактики – использование

[8] Phishing Awareness [Электронный ресурс] // Harvard, 2025. URL: https://privsec.harvard.edu/phishing-awareness (дата обращения: 30.04.2025).
[9] Там же.
[10] Dawkins S., Jacobs J. NIST Phish Scale User Guide. NIST Series TN 2276. National Institute of Standards and Technology, Gaithersburg, MD, 2023. 39 p. https://doi.org/10.6028/NIST.TN.2276

гуманитарных призывов, предложений «слишком хорошо, чтобы быть правдой», ограниченных по времени предложений, выдача себя за друга, коллегу или авторитетного человека и т. д.

23 возможных сигнала разбиты на типы, перечисленные в Таблице 1. На самом деле, для систем машинного (глубокого) обучения такого рода сигналы есть признаки («фичи») при обучении моделей распознавания. На рисунке 2 для примера показан собранный в обзоре [12] список технических индикаторов для детекторов фишинговых писем. А анализ тактик – это тема для NLP приложений [13]. Отметим, что в плане определения тактик точно присутствуют моменты, связанные с языком и культурным кодом, поэтому они не могут быть полностью универсальными.

Т а б л и ц а 1. **Фишинговые сигналы**
T a b l e 1. **Phishing Signals**

Тип	**Сигналы**
Ошибки	Грамматические ошибки Несоответствия
Технические признаки	Тип вложения Отображаемое имя и адрес электронной почты отправителя Гиперссылка URL Подмена домена
Визуальное представление	Отсутствие или минимальное количество фирменного стиля и логотипов Имитация логотипа или устаревший фирменный стиль/логотипы Непрофессиональный дизайн или форматирование Индикаторы и значки безопасности
Язык и содержание	Юридическая терминология/информация об авторских правах/отказ от ответственности Отвлекающие детали Просьбы о конфиденциальной информации Чувство срочности Угрожающий язык Общее приветствие (нет персонализации) Отсутствие данных подписчика
Тактики	Гуманитарные призывы Слишком хорошие, чтобы быть правдой предложения Вы особенный (выделение получателя) Ограниченное по времени предложение Имитирует рабочий или бизнес-процесс Выдаёт себя за друга, коллегу, руководителя, авторитетную личность

Источник: составлено авторами.
Source: Compiled by the authors.

По сути, эта часть документа NIST [10] может рассматриваться как пример инженерии признаков. В документе довольно подробно описана их группировка и определение значимости.

Шкала фишинга включает три категории, которые соответствуют общему количеству признаков:

Мало – фишинговое письмо содержит мало (1-8) признаков, что снижает вероятность идентификации письма как фишинга.

Умеренно – фишинговое письмо содержит умеренное количество признаков (9-14).

Много – фишинговое письмо содержит большое количество признаков (>15), что повышает вероятность идентификации письма как фишинга.

S/N	Features
1	Links in tags
2	Abnormal URLs
3	Age of domain
4	Port
5	Right click disabled
6	Pop up windows
7	Embedded brand name
8	Subdomain level
9	Redirect page
10	IP address
11	Pct Ext resource URLs
12	Insecure forms
13	Double slash redirecting
14	Frequent domain name mismatch
15	URL length RT
16	Ext meta script link RT
17	Using pop-up windows
18	Double slash in path
19	Missing title
20	Page rank
21	SSL final state
22	Fake link in status bar
23	Random string
24	Host name length
25	Query length
26	No HTTPS
27	Links pointing to a page
28	Num hash
29	IFrame or frame
30	Insecure forms

Р и с. 2. Признаки, используемые в моделях детектирования [12]
F i g. 2. Features Used in Detection Models [12]

Заключение

В статье рассмотрены учебные программы осведомленности о фишинге, призванные убедить пользователей ответственно относиться к возможным переходам по ссылкам в получаемой корреспонденции. Несмотря на всю простоту фишинговых атак, именно конечные пользователи оказываются слабым звеном, которое обеспечивает их успех. Основой обучения служат реальные примеры фишинговых атак (сообщений), которые, соответственно, должны постоянно обновляться, чтобы отслеживать последние усилия атакующих и специально созданные примеры, на которых проверяются обучающиеся.

Говоря об эффективности таких тренировок, можно отметить следующие данные из отчетов: после тренировки уровень сообщений об угрозах увеличился с 7% до 60% в течение года, а 64% сотрудников сообщили, по крайней мере, об одной реальной угрозе в течение первого года.

Шкала фишинга от NIST позволяет оценивать сложность таких писем и является хорошим кандидатом на локализацию.

Благодарности

Авторы благодарны сотрудникам кафедры информационной безопасности факультета ВМК МГУ имени М.В.Ломоносова за ценные обсуждения. Работа написана в рамках развития программы

«Кибербезопасность» на факультете ВМК МГУ [14]. Традиционно, отмечаем публикации В.П. Куприяновского и его многочисленных соавторов, положивших начало рассмотрению цифровой повестки в российской научной периодике [15-17].

References

1. Alabdan R. Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet*. 2020;12(10):168. https://doi.org/10.3390/fi12100168
2. Bethany M., et al. Large Language Model Lateral Spear Phishing: A Comparative Study in Large-Scale Organizational Settings. *arXiv:*2401.09727. 2024.
3. Lebed S.V., Namiot D.E., Zubareva E.V., et al. Large Language Models in Cyberattacks. *Doklady Mathematics*. 2024;110(Suppl 2):S510-S520. https://doi.org/10.1134/S1064562425700012
4. Tempestini G., Merà S., Palange M.P., Bucciarelli A., Di Nocera F. Improving the Cybersecurity Awareness of Young Adults through a Game-Based Informal Learning Strategy. *Information.* 2024;15(10):607. https://doi.org/10.3390/info15100607
5. Kaur R., Gabrijelčič D., Klobučar T. Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*. 2023;97:101804. https://doi.org/10.1016/j.inffus.2023.101804
6. Ogochukwu O., Chinedum A. Awareness of Phishing Attacks in Institutions of Higher Learning: A Review of Types and Technical Approaches. *International Journal of Research and Innovation in Applied Science*. 2024;9(10):309-333. https://doi.org/10.51584/IJRIAS.2024.910031
7. Manoharan A., Sriskantharajah A., et al. MetaHuman based phishing attacks in the metaverse realm: Awareness for cyber security education. *Education and Information Technologies*. 2025;30:12939-12965. https://doi.org/10.1007/s10639-025-13326-w
8. Koza E., Öztürk A., Willer M. Phishing. In: Social Engineering and Human Hacking. Berlin, Heidelberg: Springer; 2025. p. 157-168. https://doi.org/10.1007/978-3-662-72084-4_16
9. Ciupe A., Orza B. Reinforcing Cybersecurity Awareness through Simulated Phishing Attacks: Findings from an HEI Case Study. In: 2024 IEEE Global Engineering Education Conference (EDUCON). Kos Island, Greece: IEEE Press; 2024. p. 1-4. https://doi.org/10.1109/EDUCON60312.2024.10578700
10. Le-Nye E.N.M., Yaacoub Ch., Possik J. Evaluating Phishing Awareness Strategies: A Comparative Study of Education-based approaches and Game-based learning. *Procedia Computer Science*. Procedia Computer Science. 2024;251:666-671. https://doi.org/10.1016/j.procs.2024.11.166
11. Steves M.P., Greene K.K., Theofanos M.F. A Phish Scale: Rating Human Phishing Message Detection Difficulty. In: Workshop on Usable Security (USEC) 2019. San Diego, CA, USA; 2019. p. 1-14. https://dx.doi.org/10.14722/usec.2019.23028
12. Tanimu J., Shiaeles S., Adda M. A Comparative Analysis of Feature Eliminator Methods to Improve Machine Learning Phishing Detection. *Journal of Data Science and Intelligent Systems.* 2024;2(2):87-99. https://doi.org/10.47852/bonviewJDSIS32021736
13. Sayyafzadeh S., Weatherspoon M., Yan J., Chi H. Securing Against Deception: Exploring Phishing Emails Through ChatGPT and Sentiment Analysis. In: 2024 IEEE/ACIS 22nd International Conference on Software Engineering Research, Management and Applications (SERA). Honolulu, HI, USA: IEEE Press; 2024. p. 159-165. https://doi.org/10.1109/SERA61261.2024.10685564
14. Sukhomlin V.A. The Concept and Main Characteristics of the Master's Degree Program "Cybersecurity" of the faculty of Computational Mathematics and Cybernetics of Lomonosov Moscow State University. *International Journal of Open Information Technologies.* 2023;11(7):143-148. (In Russ., abstract in Eng.) EDN: MPHLSQ
15. Kupriyanovsky V., et al. Digital Economy and the Internet of Things – Negotiating Data Silo. *International Journal of Open Information Technologies.* 2016;4(8):36-42. (In Russ., abstract in Eng.) EDN: WFVAPB
16. Kupriyanovsky V., et al. On Retail Trade in the Digital Economy. *International Journal of Open Information Technologies.* 2016;4(7):1-12. (In Russ., abstract in Eng.) EDN: WCMIWN
17. Volkov A.A., Namiot D., Schneps-Schneppe M. Building an Effective Infrastructure for Environment. *International Journal of Open Information Technologies*. 2013;1(7):1-10. (In Russ., abstract in Eng.) EDN: ROMIZX
18. An D.S., Zufarova A.S. Simulation of phishing attacks as a method of increasing cyber literacy and preparing to respond to threats. *Education Management Review*. 2025;15(6-1):127-139. (In Russ., abstract in Eng.) https://doi.org/10.25726/b2476-6563-8129-i
19. Astakhova L.V., Medvedev I.A. An information tool for increasing the resistance of employees of an organization to social engineering attacks. *Scientific and Technical Information Processing*. 2021;48(1):15-20. https://doi.org/10.3103/S0147688221010020
20. Liaqat M.S., Mumtaz G., Rasheed N., Mubeen Z. Exploring Phishing Attacks in the AI Age: A Comprehensive Literature Review. *Journal of Computing & Biomedical Informatics*. 2024;07(02):567. https://doi.org/10.56979/702/2024
21. Ustundag Soykan E., Bagriyanik M. The effect of SMiShing attack on security of demand response programs. *Energies*. 2020;13(17):4542. https://doi.org/10.3390/en13174542

22. Sharevski F., Devine A., Pieroni E., Jachim P. Phishing with Malicious QR Codes. In: Proceedings of the 2022 European Symposium on Usable Security (EuroUSEC '22). New York, NY, USA: Association for Computing Machinery; 2022. p. 160-171. https://doi.org/10.1145/3549015.3554172
23. Klitis C., et al. NERO: Advanced Cybersecurity Awareness Ecosystem for SMEs. In: Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES '24). New York, NY, USA: Association for Computing Machinery; 2024. Article number: 174. https://doi.org/10.1145/3664476.3670447
24. Musa B.B., et al. Emerging Trends in Phishing: A Look at Smishing, Vishing, Quishing. *International Journal of Technology & Emerging Research*. 2025;01(03):274-289. https://doi.org/10.64823/ijter.2503033
25. Toth R., et al. Sustaining Cyber Awareness: The Long-Term Impact of Continuous Phishing Training and Emotional Triggers. *arXiv:*2510.27298. 2025. https://doi.org/10.48550/arXiv.2510.27298

Поступила 16.05.2025; одобрена после рецензирования 21.06.2025; принята к публикации 04.07.2025.

Submitted 16.05.2025; approved after reviewing 21.06.2025; accepted for publication 04.07.2025.

Об авторах:

Намиот Дмитрий Евгеньевич, ведущий научный сотрудник лаборатории открытых информационных технологий кафедры информационной безопасности факультета вычислительной математики и кибернетики, ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова» (119991, Российская Федерация, г. Москва, ГСП-1, Ленинские горы, д. 1), доктор технических наук, **ORCID: https://orcid.org/0000-0002-4463-1678,** dnamiot@gmail.com

Васенин Валерий Александрович, заведующий кафедрой математического моделирования и компьютерных исследований механико-математического факультета; заведующий лабораторией автоматизации экспериментальных исследований НИИ механики МГУ, ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова» (119991, Российская Федерация, г. Москва, ГСП-1, Ленинские горы, д. 1), доктор физико-математических наук, профессор, **ORCID: https://orcid.org/0000-0003-2499-6132,** vasenin@msu.ru

Все авторы прочитали и одобрили окончательный вариант рукописи.

About the authors:

Dmitry E. Namiot, Senior Researcher of the Open Information Technologies Lab, Department of Information Security, Faculty of Computational Mathematics and Cybernetics, Lomonosov Moscow State University (1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation), Dr. Sci. (Eng.), **ORCID: https://orcid.org/0000-0002-4463-1678,** dnamiot@gmail.com

Valery A. Vasenin, Head of the Chair of Mathematical Modeling and Computer Research, Faculty of Mechanics and Mathematics; Head of the Laboratory of Automation of Experimental Research, Institute of Mechanics of MSU, Lomonosov Moscow State University (1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation), Dr. Sci. (Phys.-Math.), Professor, **ORCID: https://orcid.org/0000-0003-2499-6132,** vasenin@msu.ru

All authors have read and approved the final manuscript.