DOI: 10.55648/1998-6920-2023-17-2-93-103 УДК 004

Технология формирования интегрированной антифишинговой системы в цифровом обществе

А. Б. Архипова, Д. А. Нечаев

Новосибирский государственный технический университет (НГТУ)

Аннотация: В данной работе рассматривается проблема фишинга в интернет-пространстве. Также проанализированы причины актуальности проблемы фишинга, рассмотренные через призму злоумышленника. Далее определено понятие канала связи и его корреляция с явлением фишинга на примере почтовых атак. В работе разработана технология формирования антифишинговой системы на примере модели взаимодействия злоумышленника и пользователя. Проанализированы меры защиты от почтового фишинга. Разработано программное обеспечение PufferPhish, предполагающее интеграцию системы защиты в процесс доставки почтовых сообщений.

Ключевые слова: фишинг, реактивная мера защиты, цифровая безопасность, угроза безопасности, стратегия злоумышленника, социальная инженерия, сценарий атаки, антифишинговая система, интегрированная система защиты.

Для цитирования: Архипова А. Б., Нечаев Д. А. Технология формирования интегрированной антифишинговой системы в цифровом обществе // Вестник СибГУТИ. 2023. Т. 17, № 2. С. 93–103. https://doi.org/10.55648/1998-6920-2023-17-2-93-103.

Статья поступила в редакцию 25.12.2022;
принята к публикации 10.01.2023.

1. Введение

С развитием технологий стремительно увеличивается число товаров и услуг, приобретаемых дистанционно. Процесс цифровизации неизбежно ведет не только к увеличению объема информации в интернет-пространстве, но и увеличению шанса ее компрометации. На этой почве общество все чаще сталкивается с проблемами мошенничества и киберпреступлений [18].

Обращаясь к истории цифровых технологий, можно проследить экспоненциальную динамику роста масштабов киберпреступлений. Начиная с 1960-х годов, когда совершались первые противоправные действия, оказывающие воздействие на информационные системы [14, 18], вариативность подходов к реализации компьютерных атак значительно увеличилась. На данный момент фишинг является одним из самых популярных способов совершения преступных действий в Интернете. И несмотря на то, что вопрос разработки и внедрения различных средств и организационных мер по защите информации стоит наиболее остро, темпов снижения роста киберпреступлений не наблюдается.

2. Тенденции развития киберпреступлений и системы защиты в цифровом обществе

Управление информационной безопасностью является очень важным вопросом для всех, кто работает в области технологий, или для всех, кто подвергается риску нарушения безопасности и понимает последствия этих уязвимостей. Многие организации постоянно находятся под угрозой нарушения безопасности. Организации могут легко столкнуться с компрометацией информации, возникающей в результате утечки данных. В условиях постоянно возникающих угроз безопасности данных организации всегда работают над обеспечением защиты своих данных [2, 8–10].

Сегодня проведение аудита систем управления информационной безопасностью – необходимое и обязательное мероприятие. Ряд организаций, бизнес которых тесно связан с использованием информационных технологий, таких как банки, нефтяные, газовые, энергетические и телекоммуникационные компании, в последнее время активизировались в проведении аудитов систем управления информационной безопасностью.

В нормативной базе РФ нет прямого определения термина «фишинг», однако в банке данных угроз ФСТЭК можно ознакомиться с одним из примеров частного описания реализации фишинга по описанию угрозы безопасности информации УБИ.175: «Угроза «фишинга»». Так, фишинг понимают как процесс убеждения нарушителем, имеющим цель неправомерного ознакомления с защищаемой информацией, пользователя с помощью методов социальной инженерии осуществить переход на поддельный сайт с целью ввода защищаемой информации или открыть вредоносное вложение в письме [13]. Для более точного понимания концепции фишинга стоит внести корректировки. Понятие «фишинг» можно трактовать как процесс получения злоумышленником личной идентификационной информации пользователя с помощью применения методов социальной инженерии и информационных технологий в личных целях. Под личной информацией пользователя в данном контексте понимается вся та информация, которая влечет выгоду для злоумышленника, а именно данные банковских карт, счетов; персональные данные (биометрия); данные учетных записей – логины и пароли.

Для построения модели взаимодействия между пользователем и злоумышленником стоит определить личность интернет-мошенника, его мотивы, потребности и поведение в интернете. Анализ литературы позволил сформировать образ злоумышленника. К ключевым методам, способствующим реализации атаки, стоит отнести оказание психологического воздействия на потенциальную жертву. Так, например, используя различные манипуляции над чувствами человека, злоумышленник внушает необходимое поведение со стороны жертвы, ведущее к успешности атаки. Среди используемых методов оказания психологического воздействия можно выделить наиболее популярные, такие как:

- претекстинг – использование злоумышленником предлога для того, чтобы привлечь внимание жертвы и заставить ее сообщить необходимую информацию;
- квид про кво – получение злоумышленником информации в обмен на несуществующее получение выгоды жертвой (наследство, приз);
- использование чувств человека (страх, любопытство) для ослабления бдительности жертвы;
- использование полученной информации о пользователе (зачастую из открытых источников) для повышения доверия к себе;
- обратная социальная инженерия – случай, когда жертва сама обращается к злоумышленнику [20].

Что касается мотивации мошенника к исполнению киберпреступления, можно выделить три основных причины: корыстный мотив (получение выгоды), исследовательский интерес и хулиганство. Также стоит отметить ключевые причины, из-за которых злоумышленники становятся киберпреступниками, а именно разницу в опыте в сфере технологий между мошенником и жертвой, а также высокую вероятность безнаказанности за совершенные в сети пре-

ступления [15]. Отметим, что на основе используемой той или иной методики социальной инженерии строится сценарий атаки.

Для реализации фишинга необходима цифровая среда, в которой злоумышленник может осуществлять атаки. В контексте исследования среду реализации фишинга будем детерминировать понятием «канал связи» и определим данный термин как совокупность программно-аппаратных средств, с помощью которых пользователи могут обмениваться информацией между собой. Для наибольшего охвата атакуемой аудитории злоумышленники используют такие каналы связи, как:

- электронная почта;
- социальные сети;
- мессенджеры;
- сотовая связь;
- Wi-Fi-сеть.

Каждый из каналов связи обладает собственными технологиями для организации и реализации передачи информации между субъектами сетевого взаимодействия. В связи с этим возникает потребность в формировании набора защитных мер для обнаружения и предотвращения фишинга. В рамках данного исследования будет рассмотрен фишинг, реализуемый по электронной почте.

Согласно статистике электронная почта является самым распространенным каналом связи [3]. Злоумышленники прибегают к различным техникам для реализации фишинга, а также комбинируют их для наибольшей вероятности успешной атаки. Разберем возможные техники реализации фишинга.

1. Использование вредоносных вложений. Злоумышленники (фишеры) в почтовых сообщениях прикрепляют файлы различных расширений – от стандартных docx, xls, pdf до нетипичных для электронных сообщений – bat, exe. Фишеры используют различные предлоги для того, чтобы пользователь открыл вложение. Если говорить об обмане рядовых пользователей Интернета, то обычно темой писем являются различного рода скидки, приглашение на работу, информация об обновлении системы и т.д. Что касается сотрудников компаний, предлогом для успеха реализации фишинга являются почтовые сообщения об отпуске, проблемах с начислением заработной платы или неправильно заполненных документах. Сам злоумышленник, чтобы войти в доверие, представляется заинтересованным лицом либо создает адрес электронной почты, схожий с корпоративным [16, 19].

2. Ссылка на поддельный веб-сайт. В тексте письма может содержаться ссылка на веб-ресурс, на котором может находиться опасный контент. Злоумышленники могут использовать различные предлоги для использования ссылки на свой поддельный сайт. Одним из вариантов является создание схожего по названию адреса сайта компании путем внесения корректировок в доменное имя в виде дополнительных символов или замены существующих на варианты, схожие по написанию. Также злоумышленник может использовать уникальный по названию сайт, имитирующий работу сервиса, предоставляющего спектр услуг.

3. Поддельный домен отправителя. Использование поддельного домена позволяет злоумышленнику применять методы социальной инженерии, аналогичные технике формирования ссылок на поддельные веб-сайты. Так, например, злоумышленник может использовать домен, схожий с легитимным, используя в адресе символы из других языков, имитирующих базовую латиницу. Также для скорой массовой рассылки злоумышленники могут использовать автоматически сгенерированные последовательности символов в адресе домена [17].

4. Социальная инженерия в тексте сообщения. Злоумышленник применяет техники психологического давления с целью получения идентификационных данных пользователя ответом на свою почту.

5. Email spoofing (спуфинг). Используя программные средства, злоумышленник может выдать себя за другого пользователя, например, указывая при отправке сообщений поддельный почтовый домен.

Определив техники для реализации фишинговой атаки злоумышленником, построим модель взаимодействия между злоумышленником и жертвой (рис. 1).

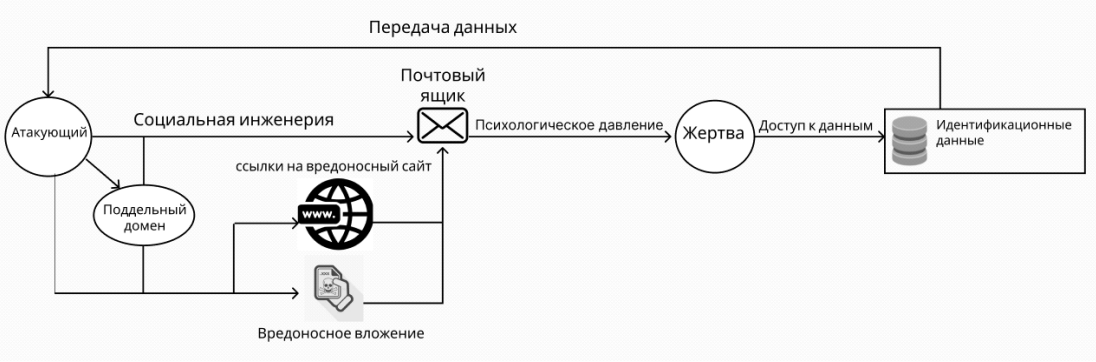

Рис. 1. Модель взаимодействия участников фишинговой атаки без защиты жертвы

В данной модели рассматривается случай фишинговой атаки со стороны злоумышленника, при которой отсутствуют защитные меры со стороны жертвы.

Объекты – атакующий и жертва – трактуются как учетные записи участников взаимодействия, с которых осуществляется формирование, отправка и соответственно прием и чтение электронных почтовых сообщений. Поддельный домен принимает роль спуфингового адреса. Также в модели учитываются три основных тактики для проведения атаки – использование психологического текста, вредоносных ссылок и вложений, причем возможны комбинации тактик, а также совмещение с отправкой со спуфингового адреса для увеличения шанса успешной атаки. Получив письмо, атакуемый пользователь при ознакомлении подсознательно подвергается психологическому давлению, что влияет на последующее срабатывание тактик, которое и приводит к конечной цели фишера – получению идентификационных данных.

Таким образом, модель взаимодействия участников фишинговой атаки без защиты жертвы показывает актуальность проблемы изучения фишинга в существующем цифровом обществе, одной из причин которых является отсутствие средств защиты со стороны жертвы, влияние человеческого фактора и в результате низкий порог входа для мошенников [2, 12].

Отметим, чтобы противостоять проблеме фишинга, пользователи применяют различные меры защиты. В данном исследовании определим три типа применяемых мер – превентивные, реактивные и проактивные меры.

Превентивные меры. В контексте фишинга под превентивными мерами будем понимать применение организационных и технических мер, благодаря которым для атакуемого пользователя отсутствует необходимость в принятии решения относительно того, фишинговое ли сообщение или нет. Так, например, организационной мерой является вовлеченность государства для противодействия фишингу, то есть все сайты подвергаются проверке на фишинг со стороны государственного сервиса [6]. С технической точки зрения предотвратить доставку фишингового сообщения до конечного пользователя можно с помощью системы защиты от спама почтовых агентов, а также таргетированных антифишинговых продуктов, устанавливаемых между доменами отправителей и корпоративной почтой сотрудников компании.

Реактивные меры. Реализация реактивных мер подразумевает, в отличие от превентивных, проверку уже доставленных сообщений. В качестве защиты используют такие средства, как браузерный механизм проверки сайтов, предупреждающий пользователей о потенциально опасном контенте, плагины для браузеров с аналогичным принципом работы, а также программные антифишинговые решения, устанавливаемые на рабочем месте пользователя [1]. Среди организационных мер можно отметить повышение пользователями осведомленности в области информационной безопасности.

Проактивные меры. В случае успешности реализации фишинговой атаки злоумышленник получает идентификационные данные пользователя. Однако и на этом этапе имеется возможность избежать потерь. Проактивными мерами в данном случае можно считать использование двухфакторной аутентификации в сервисах, в которых применяют скомпроме-

тированные идентификационные данные; блокировка карты, а также смена скомпрометированного пароля [7].

Разница между антифишинговыми средствами, относящимися к реактивному и превентивному типу мер, заключается в том, что первое средство устанавливается на рабочее место пользователя, а другая система в основном устанавливается в крупных организациях в одной точке сети для фильтрации входящих писем большого числа пользователей, что экономит время и ресурсы относительно установки приложения на все рабочие места в организации.

3. Технология формирования антифишинговой системы

Целью формирования технологии создания антифишинговой системы является интеграция приложения в процесс получения почтовых сообщений. Данная система относится к реактивному типу применяемых мер защиты, так как, в отличие от антифишинговых средств, благодаря которым до пользователя не доходят фишинговые письма, пользователи имеют возможность ознакомиться с мошенническим письмом. Целевой аудиторией системы являются обычные пользователи Интернета либо организации с малым или средним штатом, имеющие рабочие места в количестве нескольких единиц.

Преимуществом такой системы можно считать тот факт, что пользователь, получив фишинговое или потенциально опасное сообщение, сможет ознакомиться с указанной вредоносной или потенциально опасной сигнатурой и тем самым постепенно повышать уровень осведомленности в области информационной безопасности. Что касается недостатков такого подхода к построению системы, пользователь имеет возможность подвергнуться атаке, даже после проведенного системой анализа сообщения.

Достоинством предложенной системы защиты от фишинга является наличие таких функций, как использование нескольких почтовых адресов, проверка почтовых сообщений и их отображение по нажатию с результатами анализа опасного содержимого.

3.1. Модель приложения

На рис. 2 определена модель антифишинговой системы в виде программного приложения (PufferPhish). Можно заметить, что данное программное средство становится посредником в процессе доставки сообщения, поэтому пользователь может ознакомиться с содержимым письма без взаимодействия с оригиналом почтового агента, тем самым можно определить PufferPhish как имитатор почтового сервиса. В связи с этим можно выделить решение о создании защищенного почтового агента для исключения посреднической передачи данных, однако в рамках данной работы это решение рассматривается лишь как метод защиты.

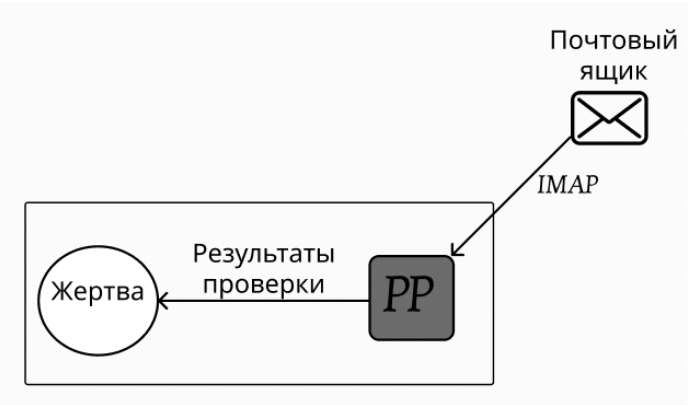

Рис. 2. Модель приложения программного продукта PufferPhish

Структура приложения. На рис. 3 представлена структура программного продукта с взаимодействием основных блоков и подблоков. Приложение с точки зрения классификации архитектуры является монолитным, так как оно написано как одна единица кода, чьи компоненты предназначены для совместной работы, используют одни и те же ресурсы и место на диске. Использование локального сервера исключает возможность компрометации информации приложения из внешних сервисов. Ядром системы является объект App веб-фреймворка следующего поколения Koa. FrontEnd- и BackEnd-части приложения написаны на языке JavaScript с использованием кроссплатформенной среды выполнения с открытым кодом Node.js. Пользователю при наличии возможности доступа и к серверной, и к веб-части достаточно взаимодействовать лишь с пользовательским интерфейсом приложения. Что касается серверной логики, при запуске приложения компонент index.ts запускает в работу компонент Router, посредством которого осуществляется связь с модулем проверки поступающих почтовых сообщений, базой данных, содержащей идентификационные данные проверяемых почтовых ящиков, данные о почтовых сообщениях – результаты проверки, а также id необходимых писем. Именно модуль Router осуществляет необходимую связь с веб-интерфейсом приложения через поступающие запросы.

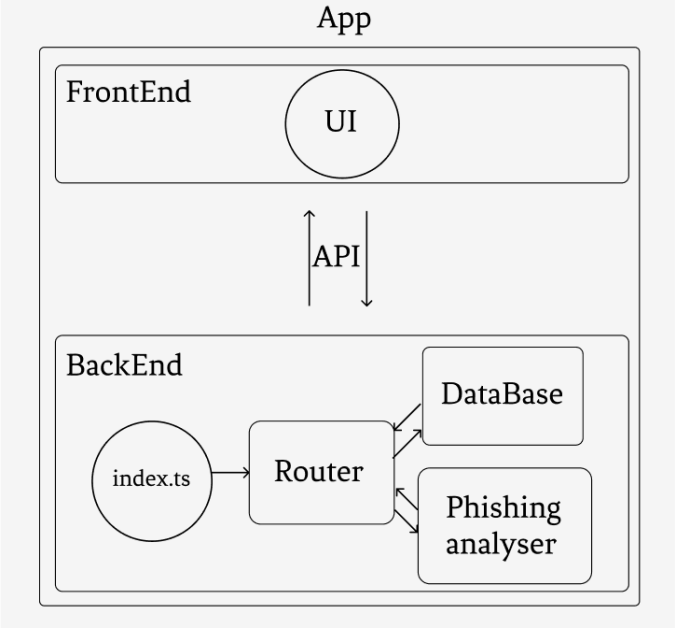

Рис. 3. Структура приложения

На рис. 4 представлена обновленная модель взаимодействия участников фишинговой атаки с интеграцией программного обеспечения. Стоит заметить, что доступ к идентификационным данным для злоумышленника доступен, так как в любом случае имеется возможность с помощью пользователя запустить вредоносное вложение или же перейти по ссылке.

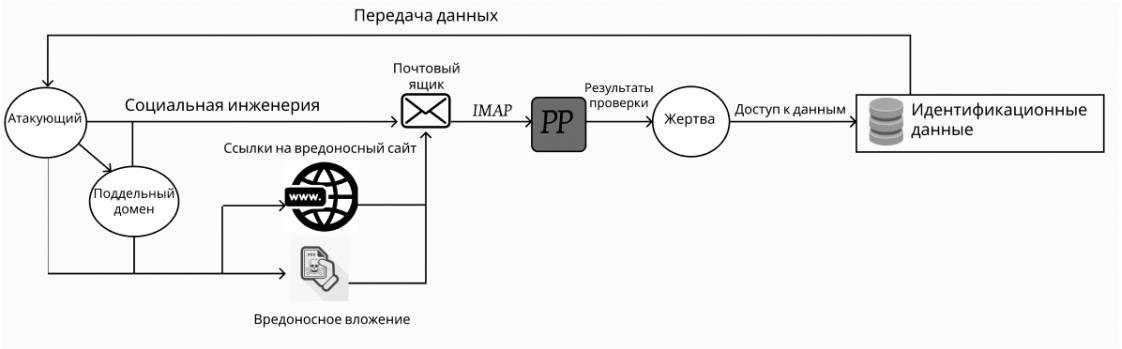

Рис. 4. Модель взаимодействия участников фишинговой атаки с интегрированной системой защиты

Разработанные модель взаимодействия (рис. 4) и технология формирования интегрированной антифишинговой системы могут также иметь применение на практике в учебном процессе для специалистов по информационной безопасности в формате игропрактик (ролевые игры, квесты по информационной безопасности, киберучения) [4, 11, 12, 20]. Использование ролевых игр для задач информационной безопасности имеет множество преимуществ. Помимо чёткой задачи моделирования реальной ситуации, можно отметить снятие психологических барьеров во взаимодействии игроков, а также получение доступа к практическим случаям, которые сложно интегрировать в другие виды игр.

4. Заключение

Фишинг является серьезной проблемой, так как затрагивает всех пользователей Интернета, тем самым становясь актуальной угрозой на международном уровне. В силу стремительного развития технологий и непоспевающего развития техник защиты киберпреступники надежно закрепились в цифровом пространстве и обладают много большей свободой действий и площадью для атаки, чем обычные преступники, в связи с чем у мирового сообщества возникает необходимость в принятии оперативных действий по противодействию киберпреступлениям и фишингу в частности. Важно понимать, что одним лишь набором технических средств защиты от фишинга обойтись невозможно, так как, например, такой вид атаки, как фишинг использует для реализации киберпреступления социальную инженерию, эксплуатируя человеческий фактор, являющийся более предпочтительным в качестве вектора атаки. Поэтому неотъемлемой частью рекомендованных для использования мер защиты является собственное понимание концепции фишинга пользователями и постоянное повышение осведомленности в области информационных технологий и информационной безопасности в частности. Получив набор различных принимаемых мер для защиты от фишинга, пользователь имеет возможность качественно защититься от фишинга. Однако стоит учитывать, что полная защита невозможна в силу постоянного развития технологий и возникновения новых сценариев атаки, а также по причине невозможности полного исключения человеческого фактора. Поэтому конечной целью противодействия фишингу является использование сочетания различных мер для минимизации вероятности реализации фишинга. Одним из возможных методов снижения риска фишинга является разработанная система защиты PufferPhish, реализующая функцию проверки почтовых сообщений на фишинг. При проведении приложением анализа осуществляется проверка возможных используемых в сообщении тактик реализации фишинга. Также для получения наиболее эффективных результатов интеграции системы защиты в приложении используется функция отображения следов фишинга для повышения осведомленности пользователя в области информационной безопасности.

Научная работа поддержана Благотворительным фондом Владимира Потанина № ГК23-000864.

Литература

1. *Mohammed A., Bakar A., Azaliah N., and Fiza R.* Anti-Phishing Tools: State of the Art and Detection Efficiencies // Applied Mathematics & Information Sciences. 2022. № 16. P. 929–934. DOI: 10.18576/amis/160609.
2. *Arkhipova A. B.* Multisociometrical readiness characteristics in information security management // CEUR Workshop Proceedings. 2022. V. 3094: Advanced in Information Security Management and Applications (AISMA 2021), Stavropol–Krasnoyarsk, 1 Oct. 2021. P. 25–34. URL: http://ceur-ws.org/Vol-3094/paper_2.pdf (access date: 28.03.2022).

3. *Blagojević I.* Phishing Statistics // 99 firms. [Электронный ресурс]. URL: https://99firms.com/blog/phishing-statistics/.
4. *Karagiannis S., Maragkos E., Magkos E.* An Analysis and Evaluation of Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools // Proc. IFIP World Conference on Information Security Education, 2020. DOI: 10.1007/978-3-030-59291-25.
5. *Krokhaleva A. B., Belov V. M.* The human factor in the system of socially significant activity // Mathematical structures and modeling. 2017. № 4 (44). P. 85–99.
6. *Kucek, S., Leitner, M.* An Empirical survey of functions and configurations of open source capture the Flag (CTF) environments // Journal of Network and Computer Applications. 2019. 102470. https://doi.org/10.1016/j.jnca.2019.102470.
7. *Sinha R., and Hemant K.* A Study on Preventive Measures of Cyber Crime. 2018. DOI: 10.13140/RG.2.2.14212.04480.
8. *Snyman D. P., Kruger H. A.* Information Security Behavioural Threshold Analysis in Practice: An Implementation Framework / In: Clarke, N., Furnell, S. (eds) Human Aspects of Information Security and Assurance. HAISA 2020. IFIP Advances in Information and Communication Technology. 2020. V. 593. Springer, Cham. https://doi.org/10.1007/978-3-030-57404-8_11.
9. *Somepalli S. H. et al.* Information Security Management // HOLISTICA – Journal of Business and Public Administration. 2020. V. 11, Is. 2. P. 1–16. DOI: 10.2478/hjbpa-2020-0015.
10. *Sri Harsha Somepalli, Sai Kishore Reddy Tangella, Santosh Yalamanchili*. Information Security Management // Journal of Business and Public Administration. 2020. № 11 (2). P. 1–16. DOI: 10.2478/hjbpa-2020-0015.
11. *Zolotarev V. V., Arkhipova A. B., Parotkin N. Y., Lvova A. P.* Strategies of social engineering attacks on information resources of gamified online education projects // CEUR Workshop Proceedings. 2021. V. 2861: International Scientific Conference on Innovative Approaches to the Application of Digital Technologies in Education (SLET), Stavropol, 12–13 Nov. 2020. P. 386–391. URL: http://ceur-ws.org/Vol-2861/.
12. *Архипова А. Б., Нечаев Д. А.* К вопросу построения модели фишинговой атаки на базе теории некооперативных игр // Материалы IX Всероссийской молодежной школы-семинара по проблемам информационной безопасности «Перспектива-2021», Красноярск, 30 сентября – 03 октября 2021 года. С. 6–12.
13. БДУ – Угрозы // Федеральная служба по техническому и экспортному контролю. [Электронный ресурс]. URL: https://bdu.fstec.ru/threat/ubi.175 (дата обращения: 01.10.2022).
14. *Грачев А. В.* История возникновения киберпреступлений // Материалы внутривузовской конференции «Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи», Магнитогорск, 09–12 октября 2015 г. С. 162–175.
15. *Комаров А. А.* Криминологические аспекты мошенничества в глобальной сети Интернет: специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»: диссертация на соискание ученой степени кандидата юридических наук. Саратов, 2011. 262 с.
16. Маскировка вирусов // ilyarm. [Электронный ресурс]. URL: https://ilyarm.ru/txt-maskirovka-virusov-exe-to-txt-zamaskirovat-exe-pod-jpg.html (дата обращения: 03.10.2022).
17. *Меньшаков С.* Разминируем почту. Простое руководство по выявлению фишинга. / xakep. [Электронный ресурс]. URL: https://xakep.ru/2021/06/16/mail-phishing/ (дата обращения: 04.10.2022).
18. *Плотникова Т. В., Харин В. В.* Киберпреступность – угроза XXI века // Вестник общественной научно-исследовательской лаборатории «Взаимодействие уголовно-исполнительной системы с институтами гражданского общества: историко-правовые и теоретико-методологические аспекты». 2018. № 12. С. 153–161.

19. Самые опасные вложенные файлы // Warp Theme Framework. [Электронный ресурс]. URL: http://security.mosmetod.ru/moshennichestvo-v-seti/152-opasnye-vlozhennye-fajly (дата обращения: 07.10.2022).
20. *Фомина Н. А*. Использование методов социальной инженерии при мошенничестве в социальных сетях // Материалы внутривузовской конференции «Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи», Магнитогорск, 09–12 октября 2015 г. С. 443–453.

Архипова Анастасия Борисовна

к.т.н., доцент кафедры защиты информации, Новосибирский государственный технический университет (НГТУ, 630073, Новосибирск, пр. Карла Маркса, 20), e-mail: arhipova@corp.nstu.ru, ORCID: 0000-0003-0791-8087, Scopus Author ID: 57223676445, Author ID (РИНЦ): 593263, SPIN-код (РИНЦ): 3885-1932.

Основное направление научных исследований – математическое моделирование в информационной безопасности.

Нечаев Дмитрий Александрович

студент кафедры защиты информации, специальность 10.05.03 «Информационная безопасность автоматизированных систем», Новосибирский государственный технический университет, e-mail: dimanechaev9@gmail.com, ORCID: 0000-0001-8861-9147, Author ID (РИНЦ): 593263.

Авторы прочитали и одобрили окончательный вариант рукописи.

Авторы заявляют об отсутствии конфликта интересов.

Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

Technology for the Formation of an Integrated Anti-phishing System in a Digital Society

Anastasiya B. Arkhipova, Dmitry A. Nechaev

Novosibirsk State Technical University (NSTU)

Abstract: The problem of phishing in the Internet space is considered in this paper. The reasons for the urgency of the phishing problem, considered through the prism of an attacker, are also analyzed. Furthermore, the concept of a communication channel and its correlation with the phenomenon of phishing is defined by the example of mail attacks. The technology of the formation of an anti-phishing system is developed on the example of a model of interaction between an attacker and a user. The measures of protection against mail phishing are analyzed. PufferPhish software has been developed, which offers the integration of a security system into the process of delivering mail messages.

Keywords: Phishing, reactive security measure, digital security, security threat, attacker strategy, social engineering, attack scenario, anti-phishing system, integrated protection system.

For citation: Arkhipova A. B., Nechaev D. A., Technology of formation of an integrated anti-phishing system in a digital Society (in Russisn). *The SibSUTIS Bulletin*, 2023, vol. 17, no. 2, pp. 93-103. https://doi.org/10.55648/1998-6920-2023-17-2-93-103.

The article was submitted: 25.12.2022;
accepted for publication 10.01.2023.

References

1. Alghenaim, M. F., Abu Bakar N.A., Abdul Rahim F. Anti-Phishing Tools: State of the Art and Detection Efficiencies. *Applied Mathematics & Information Sciences*, vol. 16, no. 6 (November. 2022), pp:929-934.
2. Arkhipova A. B. Multisociometrical readiness characteristics in information security management. *Advanced in Information Security Management and Applications*, proc. of the intern. workshop on advanced in information security management and applications (AISMA 2021), Stavropol–Krasnoyarsk, 1 October, 2021, pp. 25-34.
3. Ivan Blagojević. Phishing Statistics. available at: https://99firms.com/blog/phishing-statistics/.
4. Karagiannis S. An Analysis and Evaluation of Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools. *IFIP World Conference on Information Security Education*, 2020.
5. Krokhaleva A. B., Belov V. M. The human factor in the system of socially significant activity. *Mathematical structures and modeling*, 2017, no. 4(44), pp. 85-99.
6. Kucek, S., Leitner, M.: An Empirical survey of functions and configurations of open source capture the Flag (CTF) environments. *Journal of Network and Computer Applications*, 102470 (2019).
7. Sinha Raj, Hemant Kumar. A Study on Preventive Measures of Cyber Crime, Internationai Journal of Research in Social Sciences, vol. 8, iss. 11(1), November 2018, DOI: 10.13140/RG.2.2.14212.04480.
8. Snyman D.P., Kruger H.A. Information Security Behavioural Threshold Analysis in Practice: An Implementation Framework. *Human Aspects of Information Security and Assurance*. HAISA 2020. IFIP Advances in Information and Communication Technology, vol 593. Springer.
9. Somepalli S. H. Information Security Management. *Journal of Business and Public Administration*, vol. 11, iss. 2, 2020. pp. 1-16. DOI: 10.2478/hjbpa-2020-0015.
10. Sri Harsha Somepalli, Sai Kishore Reddy Tangella, Santosh Yalamanchili. Information Security Management. *Journal of Business and Public Administration*, vol. 11, iss. 2, pp.1-16, 2020. DOI: 10.2478/hjbpa-2020-0015.
11. Zolotarev V. V., Arkhipova A. B., Parotkin N. Y., Lvova A. P. Strategies of social engineering attacks on information resources of gamified online education projects. *International Scientific Conference on Innovative Approaches to the Application of Digital Technologies in Education (SLET–2020)*, Stavropol, 12-13 Novemder, 2020, pp. 386-391.
12. Arhipova A. B. K voprosu postroeniya modeli fishingovoj ataki na baze teorii nekooperativnyh igr [On the issue of constructing a phishing attack model based on the theory of non-cooperative games]. *Perspektiva-2021, Materialy IX Vserossijskoj molodezhnoj shkoly-seminara po problemam informacionnoj bezopas-nosti*, Krasnoyarsk, 30 September – 03 October, 2021, pp. 6-12.
13. BDU – Ugrozy [DBU – Threats]. *Federal'naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu*, available at: https://bdu.fstec.ru/threat/ubi.175 (accessed 01.10.2022).
14. Grachev A. V. Istoriya vozniknoveniya kiberprestuplenij [The history of cybercrime]. *Informacionnaya bezopasnost' i voprosy profilaktiki kiberekstremizma sredi molodezhi*, Materialy vnutrivuzovskoj konferencii, Magnitogorsk, Magnitogorskij gosudarstvennyj tekhnicheskij universitet, 09-12 October, 2015, pp. 162-175.
15. Komarov A. A. *Kriminologicheskie aspekty moshennichestva v global'noj seti Internet: special'nost' 12.00.08 "Ugolovnoe pravo i kriminologiya; ugolovno-ispolnitel'noe pravo"* [Criminological aspects of fraud in the global Internet: specialty 12.00.08 "Criminal law and criminology; penal enforcement law"]. Abstract of Ph. D. thesis. Saratov, 2011. 262 p.
16. Maskirovka virusov [Virus masking], available at: https://ilyarm.ru/txt-maskirovka-virusov-exe-to-txt-zamaskirovat-exe-pod-jpg.html (accessed 03.10.2022)

17. Men'shakov S. *Razminiruem pochtu. Prostoe rukovodstvo po vyyavleniyu fishinga*. [We clear the mail. A simple guide to detecting phishing], available at: https://xakep.ru/2021/06/16/mail-phishing/ (accessed 04.10.2022).
18. Plotnikova T. V., Harin V. V. Kiberprestupnost' - ugroza XXI veka [Cybercrime - the threat of the XXI century]. *Vestnik obshchestvennoj nauchno-issledovatel'skoj laboratorii «Vzaimodejstvie ugo-lovno-ispolnitel'noj sistemy s institutami grazhdanskogo obshchestva: istoriko-pravovye i teoretiko-metodologicheskie aspekty»*, 2018, no. 12, pp. 153-161.
19. Samye opasnye vlozhennye fajly [The most dangerous attachments], available at: http://security.mosmetod.ru/moshennichestvo-v-seti/152-opasnye-vlozhennye-fajly (accessed 07.10.2022).
21. Fomina, N. A. Ispol'zovanie metodov social'noj inzhenerii pri moshennichestve v so-cial'nyh setyah [The use of social engineering methods in fraud in social networks]. *Informacionnaya bezopasnost' i vo-prosy profilak-tiki kiberekstremizma sredi molodezhi*, Materialy vnutrivuzovskoj konferencii, Magnito-gorsk, Magnitogorskij gosudarstvennyj tekhnicheskij universitet, 09-12 October, 2015, pp. 443-453.

Anastasia B. Arkhipova

Cand. of Sci. (Engineering), Associate Professor of the Department of Information Security of Novosibirsk State Technical University (20 Karl Marx Ave., Novosibirsk, 630073), e-mail: arhipova@corp.nstu.ru, ORCHID: 0000-0003-0791-8087, Scopus Author ID: 57223676445, Author ID (RSCI): 593263, SPIN code (RSCI): 3885-1932.

The main direction of scientific research is mathematical modeling in information security.

Dmitry A. Nechaev

Student of the Department of Information Security specialty 10.05.03 "Information security of automated systems", Novosibirsk State Technical University, e-mail: dimanechaev9@gmail.com, ORCHID: 0000-0001-8861-9147, Author ID (RSCI): 593263.