Классификация фишинговых атак и меры противодействия им

Н.С. Афанасьева, Д.А. Елизаров, Т.А. Мызникова

Омский государственный университет путей сообщения

Аннотация: В статье рассмотрено понятие фишинга и его разновидности. Проведен анализ фишинговых атак за 2021 год, в котором выявлен рост их количества, что говорит об актуальности предложенных мер противодействия данному типу угроз, разработано браузерное расширение для обеспечения защиты от массовых и направленных фишинговых атак.
Ключевые слова: фишинг, атака, социальная инженерия, Phishing-as-a-Service, обеспечение информационной безопасности.

В настоящее время термин «фишинг» не определен ни в одном нормативно-правовом акте РФ. Под фишингом понимается вид интернет-мошенничества, цель которого – получить идентификационные данные пользователей [1]. Злоумышленники рассчитывают, что пользователи, попадая на поддельные (имитирующие сайты узнаваемых брендов финансового сектора, социальных сетей, маркетплейсов, стриминговых сервисов и т.д.) не заметят подделки и добровольно введут свои личные данные. В настоящее время в России формируется единая платформа, обеспечивающая взаимодействие всех заинтересованных сторон в целях противодействия мошенничеству с использованием фишинговых атак и повышению приватности для граждан, бизнеса и должностных лиц. Согласно техническому заданию от Минцифры, под фишинговым сайтом понимается «информационный ресурс в сети Интернет, схожий до степени смешения с сайтами известных брендов, часто сайтами банков и других финансовых институтов, специально созданный злоумышленниками с целью введения в заблуждение пользователей для завладения их личными данными и совершения в отношении них мошенничества» [2].

Такие поддельные сайты тяжело отличить от оригиналов, что является главной трудностью борьбы с фишингом: не существует программного обеспечения, защищающего компании и людей полностью. Данная

разновидность мошенничества позволяет сэкономить на усилиях и успешно обходить дорогостоящие средства защиты информации посредством человеческого фактора, ведь общая защита системы не может быть сильнее, чем её самое слабое звено. Именно поэтому всегда важен баланс между затратами на средства технической защиты информации и средства социальной инженерии.

Согласно статистике, при отправлении 10 фишинговых писем злоумышленником один пользователь попадется в ловушку с вероятностью 90%, при этом в 99% случаев стараются украсть у пользователей деньги, данные банковских карт или персональные данные для последующей их перепродажи.

Целью любой реализации фишинговой атаки является получение конфиденциальной информации, поэтому для выполнения своих замыслов злоумышленники используют различные формы фишинга. В настоящее время выделяют следующую классификацию типов фишинговых атак.

Почтовый фишинг является одним из самых известных типов фишинговых атак. Злоумышленники массово отправляет электронные письма по всем имеющимся у них адресам и с помощью методов социальной инженерии побуждают пользователей перейти по подмененным ссылкам. Цель атаки состоит в том, чтобы вызвать необдуманное действие у пользователя своей срочностью или привлекательностью. Зачастую, на оформление таких писем не тратится много времени, и, соблюдая элементарные правила безопасности, можно обезопасить себя от такого рода атак.

Целевой фишинг (*Spear Phishin)* также использует электронную почту, но имеет более персонализированный подход. Для сбора информации злоумышленники используют данные из открытых источников, таких, как социальные сети или официальные сайты компании. Затем они

представляются конкретными лицами в организации, используя настоящие имена, должности, контактные данные, чтобы получатель думал, что электронное письмо отправлено кем-то другим внутри организации. В итоге, считая данное письмо внутренним запросом, получатель выполняет все указания [3].

Whaling/CEO fraud – данный тип фишинга очень похож на целевой, но жертвой злоумышленника становится не любой сотрудник компании, а руководители («крупная рыба», *whaling* в переводе с английского – «китобойный промысел»). Такие атаки становятся все более распространенными, так как «киты», как правило, имеют полный доступ к конфиденциальной или желаемой информации.

Vishing и Smishing – данные типы фишинга включают в себя использование телефона. При *vishing*-атаке пользователю поступает звонок от злоумышленников, которые манипуляцией получают конфиденциальную информацию пользователя. Данная атака также основана на создании у пользователя ощущения срочности и опасности, чтобы у него не было другого выбора, кроме как передать информацию. При *Smishing* вместо голосового вызова используются текстовые сообщения (*SMS*), чтобы обмануть пользователя. На телефон в таких случаях приходит сообщение с номером телефона или ссылкой на контролируемый злоумышленниками сайт. Жертвы склонны доверять таким текстовым сообщениям, полученным на телефон, больше, чем подозрительному электронному письму.

Фишинг в социальных сетях подразумевает использование push-уведомлений и функцию прямого обмена сообщениями в приложениях, чтобы побудить пользователя к действиям.

Pharming – данная разновидность фишинга наиболее технична и такие атаки затруднительно обнаружить – происходит скрытое перенаправление на вредоносные ресурсы, то есть злоумышленник портит навигационную

инфраструктуру. Один из вариантов реализации – злоумышленники захватывают *DNS*-сервер, который в последствии перенаправляет легитимные запросы пользователей на зараженные веб-сайты.

Clone Phishing (клон-фишинг) – данный метод фишинга также использует электронную почту, но отличается от классического подхода тем, что злоумышленники создают копию уже доставленного легитимного письма. И в данной копии подменяют оригинальные ссылки или вложения на вредоносные. Затем поддельная копия повторно отправляется от якобы того же отправителя под предлогом некоторой ошибки в оригинальном сообщении.

Pop-up фишинг – злоумышленниками вредоносный код размещается во всплывающих окнах уведомлений. Более новые версии атак позволяют использовать функцию «уведомлений» браузеров – когда пользователь нажимает «Разрешить» всплывающее окно устанавливает вредоносный код.

Фишинг в поисковых системах – злоумышленники научились обходить фильтры поисковых систем и размещают зараженные веб-сайты в первых строках поисковой выдачи. Зачастую такие объявления выглядят очень заманчиво для пользователей и они доверчиво вводят информацию о себе и своих банковских продуктах для завершения покупки.

Evil Twin (злой двойник) – при данной атаке злоумышленник фальсифицирует точку доступа, которая позволяет перехватывать данные во время их передачи. При использовании фальшивой точки доступа реализуются атака «человек посередине» и подслушивание.

Аналитики Positive Technologies выделили десять самых популярных и интересных тем фишинговых атак в 2021 году: вопросы вакцинации, сервисы доставки, онлайн-знакомства, сервисы по подписке, компенсация жертвам мошенничества. По данным компании, доля атак на частных лиц с использованием методов социальной инженерии в третьем квартале 2021 года выросла до 83% по сравнению с 67% в том же квартале 2020-го [4].

Согласно отчетам Group-IB за 2021 год рост фишинга составил 18%, такая тенденция роста сохраняется с 2018 года. В 2021 замечено существенное увеличение фишинга на онлайн-сервисы в противовес значительному спаду, отмеченному в 2020. Также, по сравнению с предыдущим периодом, за текущий отчетный период специалисты Group-IB зафиксировали существенный рост фишинга на сайты знакомств, социальные сети и финансовые учреждения. Важно отметить, что основные схемы фишинга мало изменяются, при этом постоянно используются новые актуальные инфоповоды [5]. «Лаборатория Касперского» в отчете «Спам и фишинг в 2021 году» подтвердили выявленные аналитиками Positive Technologies тенденции фишинговых атак [6] и представили рейтинг атакованных фишерами организаций, под которыми мошенники маскировали свои страницы (рис. 1).

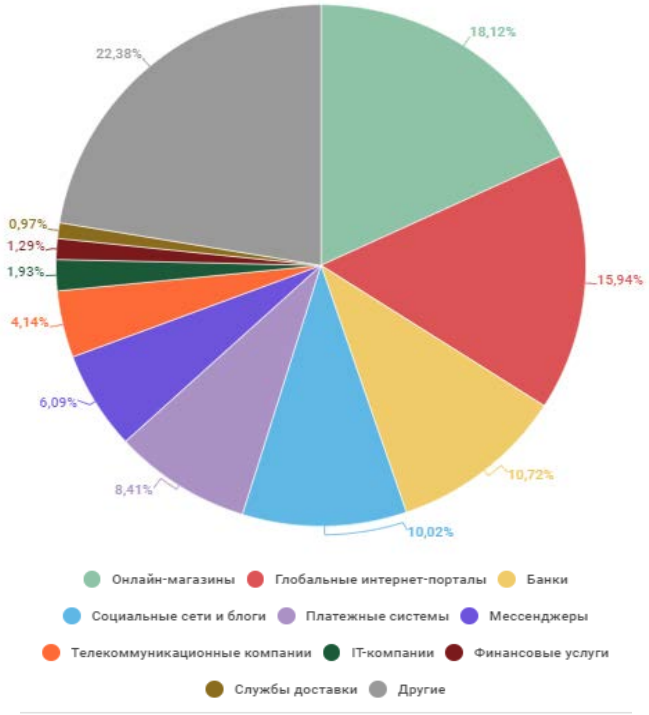

Рис. 1 – Рейтинг атакованных фишерами организаций

Большому росту фишинга способствует популяризация нового подхода – Phishing-as-a-Service (PhaaS, «фишинг как услуга»). Суть PhaaS состоит в

том, что злоумышленникам предлагается на выгодных (а иногда и бесплатных) условиях аренда или покупка готовых решений фишинговых сайтов, скриптов и схем монетизации украденных средств, то есть создание фишинговых ресурсов происходит автоматически – остается лишь вовлечь жертву в эту схему. Соответственно порог входа для мошенников, не обладающих специальными навыками, снижается, что приводит к глобальному масштабированию.

Угрозы фишинга связаны с социальной инженерией, поэтому от них нельзя полностью избавиться, так как достаточно лишь одной жертвы для компрометации всей сети. Также привлекательность таких атак обусловлена их универсальностью – они применимы для проникновений в любые системы [7].

Для построения комплексной системы защиты предприятия от фишинговых атак можно выделить три основных направления:

- программные средства защиты для недопущения реализации атаки с использованием базовых средств защиты электронной почты, использование средства контроля доступа в Интернет, которые позволяют отслеживать переходы по ссылкам, полученным по почте или SMS, а также использование возможности мониторинга в различных сервисах для проверки доменов/отправителей;

- проведение обучения сотрудников (пользователей) своими силами – локально (напомнить базовые правила: обязательный анализ строки адреса в браузере; проверка написания домена, наличия HTTPS; запрет на введение излишних данных банковских карт; подключение к неучтенным открытым точкам доступа); привлечение готовых решений систем обучения и повышения осведомленности в области информационной безопасности. Для систематизации требований необходимо разработать политику пользования электронной почтой в организации, регламент работ с обращениями о

выявлении фишинговых атак, регламент мониторинга таких атак и реагирования на них [8];

- защита данных, находящихся на компьютерах пользователя, позволяющая исключить возможность перехвата данных даже в случае, если фишинговая атака оказалась успешной (Internet Security Products).

Согласно прогнозам, количество фишинговых ресурсов в ближайшем будущем продолжит расти, а мошеннические схемы станут более масштабными. Поэтому необходимость реализации всех защитных механизмов остается обоснованной, в особенности, предупредительные разъяснительные беседы с персоналом. Стоит отметить, что антивирусные программы обеспечивают защиту от фишинга в режиме реального времени, основанную лишь на анализе публичных черных списков сайтов (список фишинговых сайтов). Предлагается разработать решение в виде браузерного расширения, которое бы реагировало на открывающиеся ссылки пользователя, что позволит свести человеческий фактор к минимуму. Особенностью решения является применение двухэтапной проверки. На первом этапе осуществляется проверка домена веб-сайта по списку фишинговых сайтов. При обнаружении домена в списке доступ к веб-сайту блокируется. Для выявления фишинговой атаки на втором этапе осуществляется разбор содержимого страниц веб-сайта. В ходе работы были изучены особенности метаданных веб-страницы, а также выделены критерии, на основе которых осуществляется анализ содержимого веб-страницы. В случае если расширение обнаруживает большое количество подозрительных элементов, то оно блокирует доступ к ресурсу и выводит краткую информацию о найденных вредоносных элементов. На рис. 2 представлена подробная интеллектуальная карта проверки признаков фишинговой атаки при анализе содержимого веб-страницы.

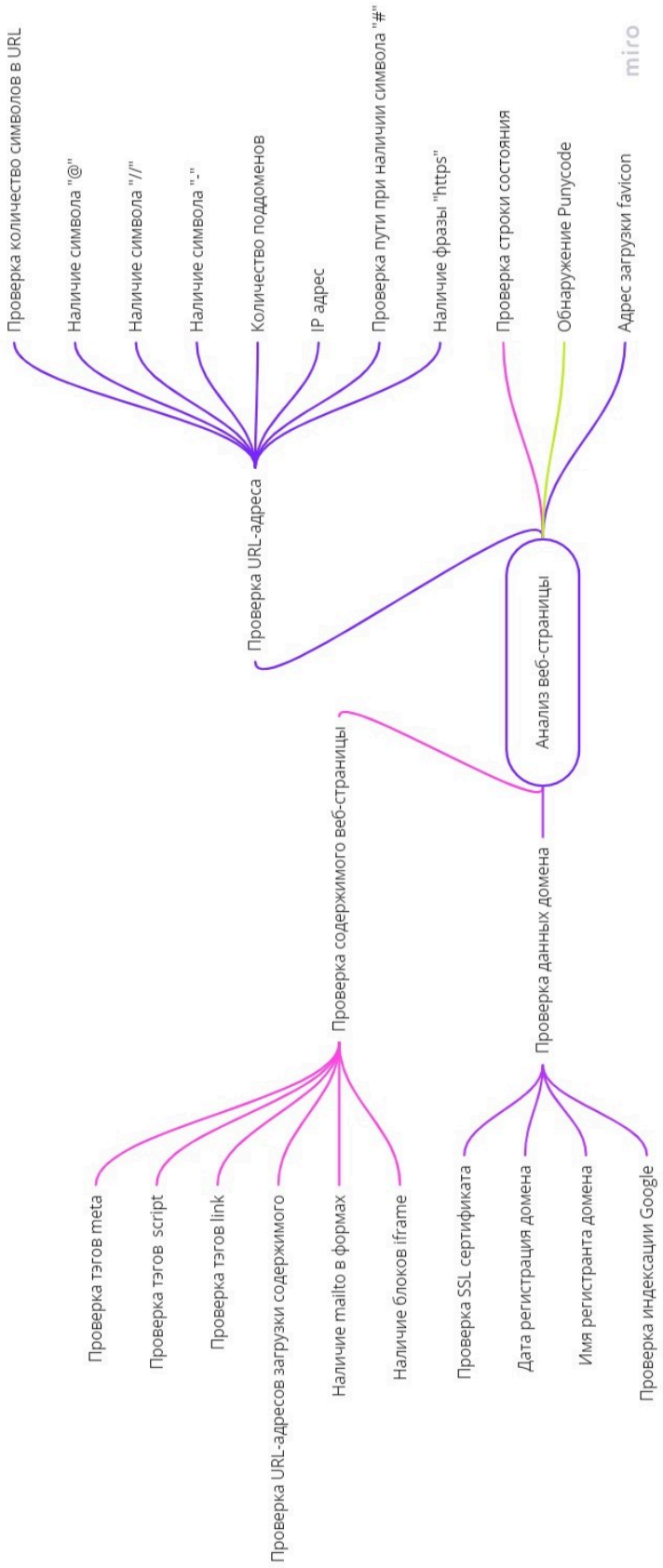

Рис. 2. – Интеллектуальная карта анализа веб-страницы

Для проведения разбора содержимого страниц веб-сайта расширение формирует из URL адреса веб-сайта и html-кода веб-страницы элементы для дальнейшей проверки. Правила проверок составлены на основе функций фишинговых веб-сайтов.

Анализ начинается с проверки URL адреса на длину, количество поддоменов, наличие прямого IP-адреса вместо домена, использование символа «@», наличие «//» (осуществляет перенаправление пользователя на другой веб-сайт), наличие символа «-», наличие фразы «https». При наличии символа «# следует обращать внимание на параметр «href» тега <a> и URL адреса (разные доменные имена сигнализируют о фишинговой атаке).

Легитимность сайта может показать наличие действующего SSL сертификата, однако следует проверить поставщика и сам сертификат. Информация о домене является показателем, следует обращать внимание на недавно созданные домены и на домены, у которых скрыто имя регистранта.

Проверка содержимого страницы веб-сайта начинается с meta-тэгов, адреса загрузки favicon, тэгов подключения скриптов и css-файлов. Отсутствие отличных от доменного имени ссылок свидетельствует о легитимности сайта. На веб-странице могут находиться внешние мультимедийные объекты (фото, видео), большинство которых не должны загружаться из другого домена. Наличие перенаправления на почту в веб-формах также свидетельствует о фишинге. Отображения другой веб-страницы при помощи тега <iframe> без использования границ свидетельствует о возможной фишинговой атаке Отсутствие внесения изменений в настройку строки состояния (для отображения поддельного URL адреса) свидетельствует о легитимности ресурса.

Алгоритм позволяет проверить индексацию веб-сайта в Google, отсутствие в индексе свидетельствует о существовании сайта в течение короткого времени, что является подозрительным.

Поскольку символы Unicode могут выглядеть одинаково невооруженным глазом, алгоритм обнаружения Punycode позволяет определить незаконные URL адреса и тем самым защититься от фишинговых атак методом Homograph.

На основе представленных правил осуществляется проверка веб-сайта и выводится результат. Если количество подозрительных элементов превышает пороговое значение, пользователю запрещается доступ. Элементы имеют статус «законный», «подозрительный», «фишинг». Для ресурсов, к которым пользователю разрешен доступ, рассчитывается вероятность фишинговой атаки с указанием подозрительных элементов.

Согласно данных аналитической компании StatCounter браузер Google Chrome продолжает оставаться самым востребованным браузером среди пользователей персональных компьютеров, смартфонов и планшетов [9]. Разрабатываемое расширение было разработано для браузера Google Chrome. Схема архитектуры расширения браузера Google Chrome представлена на рис. 3 [10].

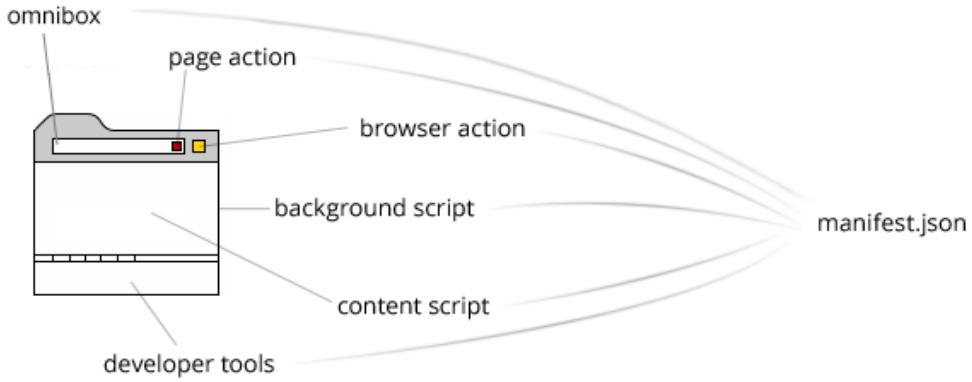

Рис. 3 – Схема архитектуры расширения браузера Google Chrome

Для проверки наличия домена веб-сайта в публичном черном списке расширение обращается к этим спискам, которые предоставляются в формате json для обновления своего локального хранилища. При проверке содержимого веб-страницы для каждого правила написан код, реализующий

алгоритм, описанный на рис. 2. Так, например, при помощи метода regexp.test осуществляется проверка наличия символа «@» (листинг 1).

```
patt=/@/;
if(patt.test(page_url)) {
  result["@ Symbol"]="1";
} else {
  result["@ Symbol"]="-1";
}
```

Листинг 1 – Проверка наличия символа «@» в URL адресе веб-сайта

Проверка наличия блоков iframe осуществляется с помощью метода getElementsByTagName, при котором в html-документе выделяется элемент тегом <iframe> (листинг 2).

```
var iframes = document.getElementsByTagName("iframe");
if(iframes.length == 0) {
  result["iFrames"] = "-1";
} else {
  result["iFrames"] = "1";
}
```

Листинг 2 – Проверка наличия блоков iframe

В результате работы полученное браузерное расширение обеспечивает защиту от массовых фишинговых атак путем сопоставления веб-сайтов с публичными черными списками и направленных атак путем анализа содержимого веб-страниц и информации о домене в реальном времени. Разработанное расширение для браузера может использоваться индивидуальными пользователями, а также в корпоративных информационных системах. Преимуществом расширения является автономная работа при проверке и блокировке веб-сайтов, содержащихся в публичных черных списках, за счет постоянного обновления локального

хранилища, а также обеспечение защиты от фишинговых атак с использованием анализа URL адреса и анализа содержимого страниц веб-сайта. Разработанный алгоритм универсален и может использоваться в других веб-браузерах.

Литература

1. Что такое «фишинг». URL: encyclopedia.kaspersky.ru/knowledge/what-is-phishing.

2. В России к 1 июня 2022 года должна быть создана система мониторинга фишинговых сайтов, Минцифры определило подрядчика. URL: d-russia.ru/v-rossii-k-1-ijunja-2022-goda-dolzhna-byt-sozdana-sistema-monitoringa-fishingovyh-sajtov-mincifry-opredelilo-podrjadchika.html (дата обращения: 30.04.2022).

3. Cisco. Целевой фишинг. URL: cisco.com/c/dam/global/ru_ru/downloads/broch/ironport_targeted_phishing.pdf.

4. Топ-10 «фишинговых» тем 2021 года по версии Positive Technologies. URL: d-russia.ru/top-10-fishingovyh-tem-2021-goda-po-versii-positive-technologies.html (дата обращения: 30.04.2022).

5. Hi-Tech Crime Trends Reports 2021/2022. URL: group-ib.com/resources/threat-research/2021-reports.html.

6. Спам и фишинг в 2021 году. URL: cisoclub.ru/spam-i-fishing-v-2021-godu (дата обращения: 30.04.2022).

7. Путято М.М., Евглевский В.Ю., Макарян А.С., Володин И.В. Исследование механизмов социальной инженерии и анализ методов противодействия // Научные труды КубГТУ, 2021, № 2. С. 57-68.

8. Спирфишинг: разбираем методы атак и способы защиты от них. URL: habr.com/ru/company/acribia/blog/472368 (дата обращения: 30.04.2022).

9. Desktop Browser Market Share Worldwide. URL: gs.statcounter.com/browser-market-share#monthly-202001-202101 (дата обращения: 30.03.2022).

10. Разработка расширений Google Chrome. URL: coderlessons.com/articles/veb-razrabotka-articles/razrabotka-rasshirenii-google-chrome (дата обращения: 30.04.2022).

References

1. Chto takoe «fishing». [What is phishing]. URL: encyclopedia.kaspersky.ru/knowledge/what-is-phishing.

2. V Rossii k 1 iyunya 2022 goda dolzhna byt' sozdana sistema monitoringa fishingovyh sajtov, Mincifry opredelilo podryadchika. [In Russia should be created a system for monitoring phishing sites by 01.06.2022, the Ministry of Digital Development has determined the contractor]. URL: d-russia.ru/v-rossii-k-1-ijunja-2022-goda-dolzhna-byt-sozdana-sistema-monitoringa-fishingovyh-sajtov-mincifry-opredelilo-podrjadchika.html.

3. Cisco. Celevoj fishing. [Cisco. Spear phishing]. URL: cisco.com/c/dam/global/ru_ru/downloads/broch/ironport_targeted_phishing.pdf.

4. Top-10 «fishingovyh» tem 2021 goda po versii Positive Technologies. [Top 10 phishing topics of 2021 according to Positive Technologies]. URL: d-russia.ru/top-10-fishingovyh-tem-2021-goda-po-versii-positive-technologies.html.

5. Hi-Tech Crime Trends Reports 2021, 2022. URL: group-ib.com/resources/threat-research/2021-reports.html.

6. Spam i fishing v 2021 godu. [Spam and phishing in 2021]. URL: cisoclub.ru/spam-i-fishing-v-2021-godu.

7. Putyato M.M., Evglevskij V.Yu., Makaryan A.S., Volodin I.V. Nauchnye trudy KubGTU, 2021, № 2. pp. 57-68.

8. Spirfishing: razbiraem metody atak i sposoby zashchity ot nih. [Spearphishing: analyze the methods of attacks and ways to protect against them] URL: habr.com/ru/company/acribia/blog/472368.

9. Desktop Browser Market Share Worldwide. URL: gs.statcounter.com/browser-market-share#monthly-202001-202101.

10. Razrabotka rasshirenij Google Chrome. [Development of Google Chrome extensions]. URL: coderlessons.com/articles/veb-razrabotka-articles/razrabotka-rasshirenii-google-chrome.