DOI: 10.25586/RNU.V9187.21.02.P.091 УДК 342

С.Б. Вепрев, С.А. Нестерович

МЕТОДЫ ФИШИНГОВЫХ АТАК НА ЭЛЕКТРОННУЮ ПОЧТУ И СПОСОБЫ ЗАЩИТЫ ОТ НИХ

Рассматривается проблема применения злоумышленниками фишинга для получения доступа к необходимой информации или для заражения персонального компьютера пользователя. Описаны различные способы фишинговых атак на электронную почту пользователя. Даны рекомендации во избежание фишинговых атак.
Ключевые слова: персональные данные, фишинг, ответственность, защита, правонарушение, информация, правовое регулирование.

S.B. Veprev, S.A. Nesterovich

METHODS OF PHISHING ATTACKS ON E-MAIL AND METHODS OF PROTECTION AGAINST THEM

The article examines the problem of using phishing by cybercriminals to gain access to necessary information or to infect a user's personal computer. Various methods of phishing attacks on a user's e-mail are described. Recommendations for avoiding phishing attacks are given.
Keywords: personal data, phishing, responsibility, protection, offense, information, legal regulation.

Вводные замечания

Небезопасные действия людей, так называемый человеческий фактор, – одна из главных проблем современной информационной безопасности. Применяя техники социальной инженерии, мошенники успешно атакуют и организации, и обычных людей. Особенно актуальна эта проблема стала в 2020 г., когда множество сотрудников начали работать в непривычных для себя условиях – вне офиса, удаленно.

Можно привести много случаев кибератак на предприятия и организации. Так, группа кибервымогателей атаковала крупные российские компании и банки [2]. У одной из медицинских организаций преступники требовали 50 тыс. долл. США после того, как зашифровали ее корпоративную сеть.

По данным Центрального банка Российской Федерации [8], только за третий квартал 2020 г. в результате цифровых атак мошенники украли у юридических лиц почти 180 млн руб., а у обычных людей – 2 млрд 500 млн руб. Главной техникой в каждом случае стала социальная инженерия: сегодня ее доля оценивается от 34 до 64%.

Фишинг как один из видов мошенничества

Одним из наиболее распространенных видов мошенничества является фишинг (от англ. phishing – преднамеренное искажение слова fishing – ловля на крючок, выуживание) – совокупность действий, направленных на получение данных обманным путем [9]. Фишинг – адресуемая с использованием домена информационная система, применяется для

Вепрев Сергей Борисович
доктор технических наук, старший научный сотрудник, заведующий кафедрой информационных технологий Московской академии Следственного комитета Российской Федерации. Сфера научных интересов: информационные технологии, вычислительные распределенные системы, информационная безопасность. Автор 57 опубликованных научных работ.
E-mail: veprevsb@yandex.ru

Нестерович Сергей Александрович
кандидат технических наук, доцент кафедры информационных технологий Московской академии Следственного комитета Российской Федерации. Сфера научных интересов: информационные технологии, системы, основанные на знаниях, информационная безопасность. Автор 23 опубликованных научных работ.
E-mail: sirial_2005@mail.ru

получения от третьих лиц (пользователей системы) конфиденциальных сведений за счет введения этих лиц в заблуждение относительно ее принадлежности (подлинности) вследствие сходства доменных имен, оформления или содержания информации.

С помощью фишинга осуществляют кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации [11]. При фишинговой атаке злоумышленники стараются обмануть пользователей сети Интернет – они отправляют специальные электронные письма, которые содержат в себе ссылки на фишинговые веб-сайты, которые внешне очень похожи на оригинальные. Как правило, при попытке авторизации все логины и пароли к аккаунту пользователя злоумышленники получают для своих целей [4].

Согласно данным отчета компании «Антифишинг» [1], 37% компаний открывают фишинговые письма, из них 79% совершают небезопасные действия. Так, например, злоумышленники маскировали свои письма под уведомления от РБК, белорусского завода «МТЗ» и других организаций. 24 сентября 2020 г. стало известно [10] о масштабной фишинговой кампании, которая была нацелена на российские предприятия топливно-энергетического комплекса. Первая волна была датирована апрелем 2020 г., последние проявления активности – сентябрем 2020 г.

Электронная почта как основной способ распространения фишинговых атак

Одним из основных способов распространения фишинговых веб-ссылок является электронная почта. Так как фишинг развивается, злоумышленники будут использовать все новые способы для распространения и сокрытия фишинговых сайтов. Усложнение фишинговых атак приводит к определенным затруднениям при обеспечении должного уровня защищенности пользователей [5]. Сейчас все меньше остается людей, которые не пользуются электронной почтой. Электронная почта может быть зарегистрирована на различных почтовых серверах. На нее могут поступать как личные сообщения, так и письма, связанные с работой, учебой или другой деятельностью человека.

Следует отметить, что для взлома электронной почты с помощью фишинга совершенно не важно, на каких серверах она располагается. Существует достаточно случаев взлома электронной почты, при которых пользователи не могут вспомнить время, действия, которые они совершали, в результате чего произошел факт неправомерного завладения их электронным аккаунтом, хотя в процессе проведения компьютерной технической экспертизы можно обнаружить следы фишинговой атаки на электронную почту пользователя. Почта пользователей, которые вводят логин и пароль для аутентификации своей электронной почты на уровне условного рефлекса, как бы в автоматическом режиме, не уделяя достаточного внимания каждому совершаемому действию, подвергается опасности.

Пример фишинговой атаки

Рассмотрим типичную фишинговую атаку.

Допустим, на электронную почту приходит обычное письмо. На рисунке 1 в списке входящих писем содержится письмо от PUY.M.RU с темой «Квитанция об оплате за Счет», и имеется во вложении файл.

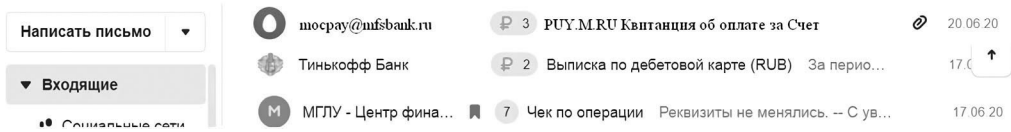

Рис. 1. Входящее письмо от PUY.M.RU с темой «Квитанция об оплате за Счет»

Если владелец электронного адреса откроет данное письмо, то оно будет выглядеть в браузере, как показано на рисунке 2.

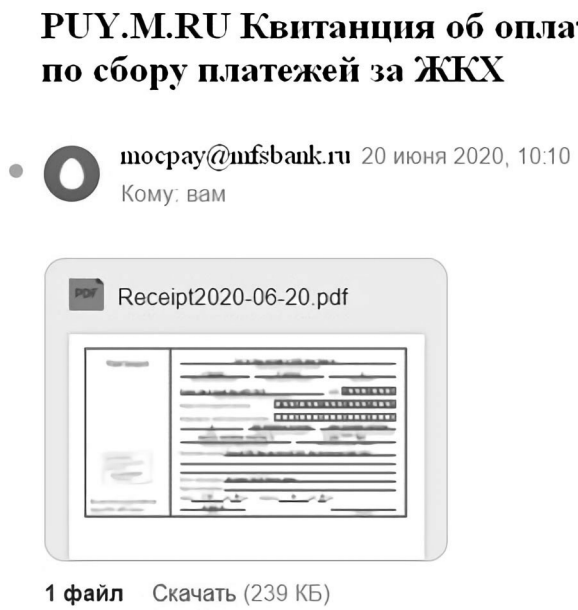

Рис. 2. Вид электронного письма

Письмо содержит pdf-файл во вложении, который пользователь может посмотреть или скачать.

Пользователь скачивает файл. После этого действия открывается следующая страница (рис. 3), на которой указаны логин пользователя, дополнительная информация о файле, который находится во вложении, и дальнейшие возможные варианты действий: скачать, посмотреть.

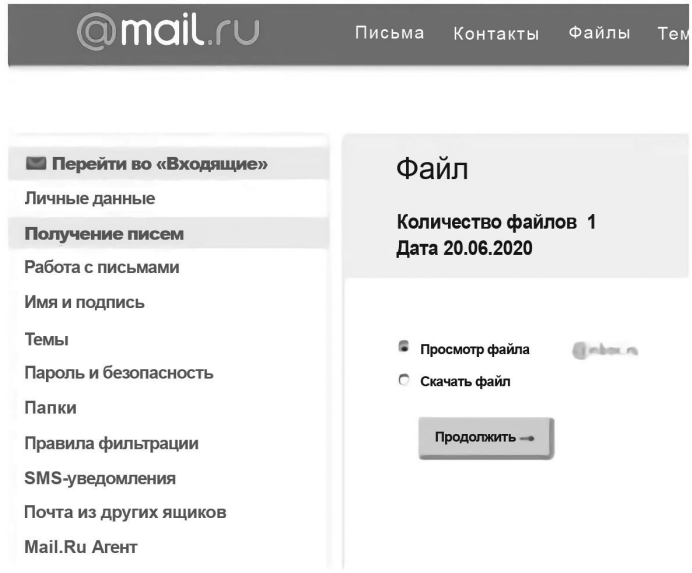

Рис. 3. Страница, отображаемая при переходе по ссылке в письме

После нажатия кнопки «Продолжить» запускается процесс авторизации и подключения к почтовому серверу, как показано на рисунке 4.

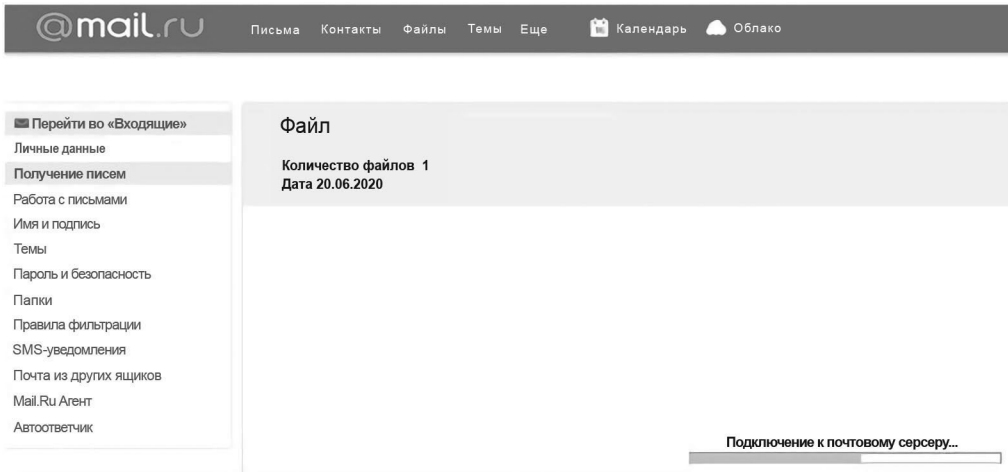

Рис. 4. Процесс авторизации

Далее почтовая система просит пользователя повторить авторизацию. Окно авторизации (рис. 5) уже содержит логин пользователя, требуется только ввести пароль.

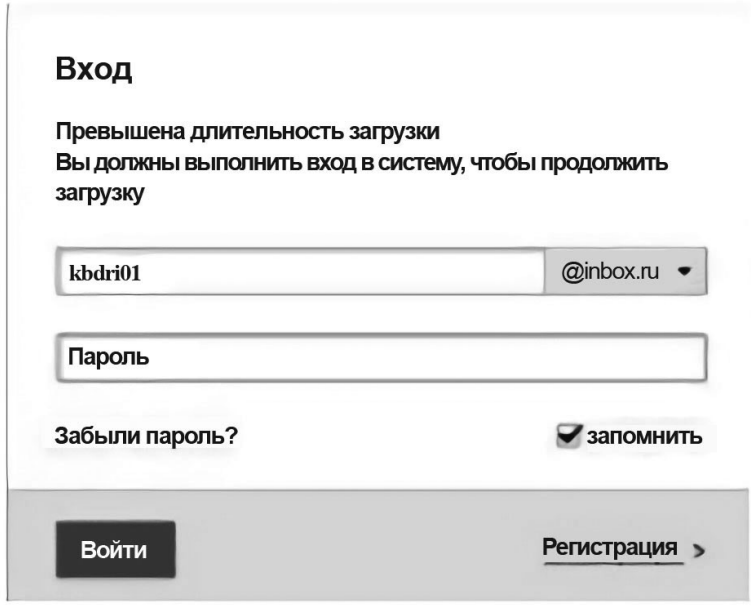

Рис. 5. Окно повторной авторизации

После этого пользователь вводит пароль и получает файл для скачивания. Он возвращается к входящим сообщениям своего электронного ящика и продолжает работу в штатном режиме. При этом антивирус не сработал.

В это время выполняется несанкционированное копирование всех файлов почты пользователя (документов, изображений и др.). Проверяется доступ к имеющимся за аккаунтом сервисам, происходит поиск информации в почте, по ключевым словам, с целью обнаружения компромата, реквизитов, данных авторизации к платежным системам и корпоративным сервисам и др., что может заинтересовать злоумышленников.

Это происходит потому, что пароль пользователя от электронной почты украден.

Нужно вернуться к началу и посмотреть поступившее от PUY.M.RU письмо с темой «Квитанция об оплате за Счет», которое как бы имеется во вложении файла.

На самом деле никаких pdf-файлов в «Квитанции об оплате за Счет» во вложении нет, а есть интегрированное в письмо изображение pdf-файла, которое имитирует наличие вложения.

Изображение практически полностью соответствует стилистике интерфейса электронной почты почтового сервиса и ничем себя не выдает. Обнаружить подмену достаточно сложно, тем более что система почтового сервера такова, что при наведении на данные изображения пользователь может увидеть ссылку вида

https://proxy.imgsmail.ru/?email=**0inbox.ru&e=1498379070&h=9-c-pc-Us7zjiMuCsJ7qKQ&urll71=cnUtbXguZWlhaWwvaWlnL21tZzEucG5n&is_https=0

Информационная безопасность

Страница https://proxy.imgsmail.ru/ является официальным ресурсом почтового сервера.

Реальное расположение страницы, на которой указан логин пользователя, информация о файле-вложении и возможность скачать или просмотреть его, находится по адресу

http://e.mail.ru-cgibix.ru/files/?Login=&Domain=:.ru&id=12433644800000023780&msg=bWFpbC5ydQIIZWxlbmFfcGFy

Или http://e.mail.ru-cgi-bix.ru/files/

Данный адрес – e.mail.ru-cgi-bix.ru – принадлежит фишинговому злодею, а не официальному почтовому сервису, хотя внешне очень похож на него.

В нашем случае авторизации при вводе пароля не происходит, созданная в виде почтового сервиса страница «пробегает» и для достоверности процесса соединения выдает вполне обычное окно авторизации, которое также является частью фишинговой страницы.

После «авторизации» пользователь попадает на официальный сервер своей электронной почты. При этом все необходимые данные – пароль с учетной записью и доменным именем – вскрываются, а программа, которая входит в состав фишинговой страницы, записывается в нужный файл или отсылается на адрес электронной почты или сервер злоумышленника. Перемещения с официального почтового сервиса на фишинговый адрес злоумышленника пользователь не заметит, даже если будет знать о возможной фишинговой атаке.

Специалисты в области информационной безопасности, которые встречались с фишинговыми атаками, утверждают: чтобы не попасться, нужно удостовериться, что перед вами страница фишингового сайта. Для этого достаточно обратить внимание на адресную строку в браузере сайта, и если она отличается от оригинального названия сайта, то перед вами фишинговый сайт.

Однако часто пользователи не обращают внимания на доменное имя в строке браузера. Доменное имя – обозначение символами, предназначенное для адресации сайтов в сети Интернет в целях обеспечения доступа к информации, размещенной в Сети [6]. Строка браузера для многих пользователей содержит набор непонятных букв, цифр и символов, и этим пользуются злоумышленники. Количество сервисов и привязанных к ним почтовых аккаунтов довольно велико и постоянно растет, и каждый сервис содержит какое-либо отличное доменное или субдоменное имя. Например, обычный пользователь, не разбирающийся в тонкостях адресации, не обратил внимание, что строка сервиса электронного ящика

https://proxy.imgsmail.ru/?email=**&e=1498379070&h=9- c- pc- Us7zjiMuCsJ7qKQ&url17l=cnUtbXguZWlhaWwvaWlnL21tZzEucG5n&is_https=0

будет заменена на строку

http://e.mail.ru- cgi- blx.ru/files/?Login=&Doraain=.ru&id=12433644800000023780&msg=bWFpbC5ydQIIZWxlbmFfcGFy=0

В результате пользователь перейдет на фишинговую страницу сайта, которая внешне не отличается от оригинального сайта, и содержит небольшую программу действий для незаметного получения пароля пользователя.

В этом случае пользователю можно дать совет – ввести любой придуманный адрес электронной почты и пароль, и если сайт фишинговый, то он примет введенные данные как верные и произведет переадресацию на настоящий сайт.

Современные тенденции фишинга

Следует отметить, что сейчас некоторые разработчики фишинговых сайтов могут использовать проверку вводимых пользователем данных – логина и пароля, осуществлять проверку на корректность. Например, в скриптовом языке PHP для установления соединения можно использовать сетевую функцию **fsockopen**() для возвращения некоторых файловых указателей, и если вызов завершится неудачей, то функция вернет значение ***FALSE***.

Есть утверждения, что антивирусы блокируют фишинговые атаки, и официальные сайты сервисов блокируют переход по фишинговым ссылкам. В почтовых сервисах антиспам-фильтры распознают фишинговые письма, а многие современные версии браузеров и почтовых клиентов – массовые фишинговые атаки; однако при персональном фишинге они не дают нужных результатов, и антифишинговые технологии стандартных средств защиты браузеров и почтовых клиентов малоэффективны.

На рисунке 6 показан классический пример фишингового сайта «Сбербанк-Онлайн».

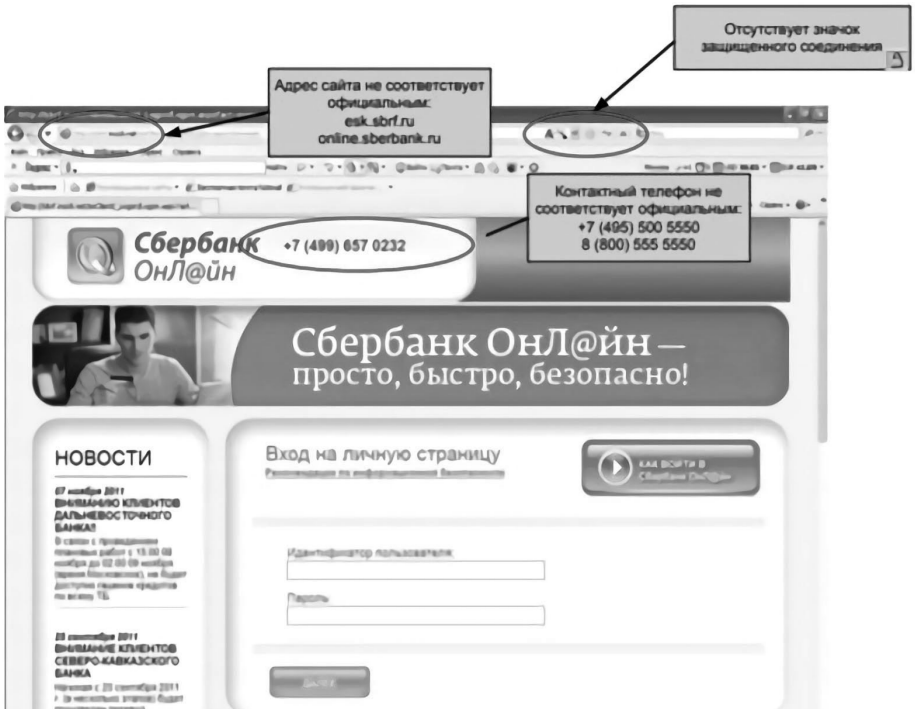

Рис. 6. Пример фишингового сайта «Сбербанк-Онлайн»

На рисунке 7 показана страница фишингового сайта с пользовательским интерфейсом настроек учетной записи.

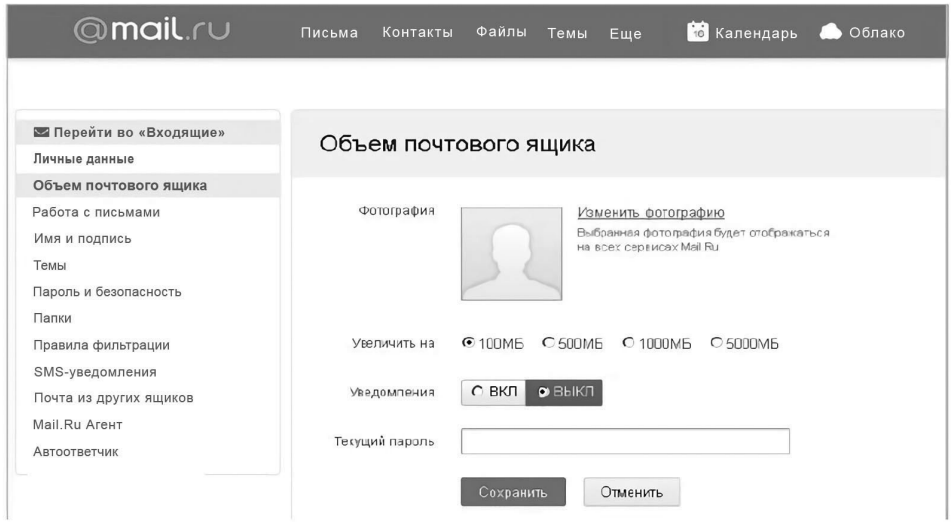

Рис. 7. Страница фишингового сайта с интерфейсом пользовательских настроек учетной записи

На рисунке видно, что внешний вид страницы практически копирует одну из настроек официальной страницы почты mail.ru, незаконно используя стиль и дизайн этого ресурса. Пользователю предлагается изменить настройки электронного ящика, тем самым производится кража его пароля.

Можно дать некоторые простые рекомендации, чтобы противостоять фишингу:

– не открывать и не читать письма от неизвестных отправителей;

– не переходить по ссылкам из писем;

– проверять сайты, на которые предлагают перейти;

– вводить в поисковую систему часть текста – возможно, многие пользователи сталкивались с этой проблемой и о ней уже давно известно;

– пользоваться антивирусным приложением с актуальной базой данных.

– обязательно устанавливать обновления для программного обеспечения, прежде всего операционной системы Windows и офисного программного обеспечения Microsoft Office;

– руководителям компаний периодически организовывать тренировки по кибербезопасности.

Выводы

Современный фишинг постоянно видоизменяется и совершенствуется. Антивирусная система может заблокировать доменное имя или сервер и внести его в базу данных, но создателям фишинга ничто не помешает зарегистрировать еще несколько десяток доменных имен и разместить их на несколько десятков других виртуальных хостингов [3]. Таким образом, фишинг существует и остается одним из самых эффективных способов хищения пароля и другой информации.

Литература

1. Антифишинг. Годовой отчет о защищенности сотрудников 2020 г. / Блог компании Антифишинг [Электронный ресурс]. – URL: https://blog.antiphish.ru/files/Antiphish_Employee_Safety_Report-2020.pdf (дата обращения: 04.03.2021).
2. Большая охота OldGremlin: операторы шифровальщика атакуют крупные компании и банки России / Group-IB [Электронный ресурс]. – URL: https://www.group-ib.ru/media/oldgremlin/ (дата обращения: 04.03.2021).
3. *Кудрявцев А.В.* Использование интернет-хостингов для хранения учебной информации в целях реализации принципов открытого образования // Педагогическое образование в России. 2016. № 7. С. 32–36.
4. *Митюков Е.А.* Жизненный цикл фишинговых атак и техники их реализации // Решение. 2019. Т. 1. С. 140–142.
5. *Митюков Е.А.* Уязвимости MS SQL SERVER, или использование хранимых процедур в своих целях // Защита информации. Инсайд. 2017. № 6. С. 44–47.
6. О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации: Федеральный закон от 28 июля 2012 г. № 139-ФЗ / Российская газета [Электронный ресурс]. – URL: https://rg.ru/2012/07/30/zakon-dok.html (дата обращения: 04.03.2021).
7. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ / Российская газета [Электронный ресурс]. – URL: https://rg.ru/2006/07/29/informacia-dok.html (дата обращения: 04.03.2021).
8. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств: III квартал 2019/2020 года / Центральный Банк Российской Федерации – официальный сайт [Электронный ресурс]. – URL: https://www.cbr.ru/analytics/ib/review_3q_2020/ (дата обращения: 04.03.2021).
9. *Сазонова М.* Мошенничество в сети: как обезопасить свою компанию в Интернете? / Гарант.ру [Электронный ресурс]. – URL: https://www.garant.ru/article/1417573/ (дата обращения: 04.03.2021).
10. Фишинг в России / TAdviser [Электронный ресурс]. – URL: https://www.tadviser.ru/index.php/Статья:Фишинг_в_России (дата обращения: 04.03.2021).
11. Что такое «фишинг» / Энциклопедия «Касперского» [Электронный ресурс]. – URL: https://encyclopedia.kaspersky.ru/knowledge/what-is-phishing/ (дата обращения: 04.03.2021).

References

1. (2020) Antifishing. Godovoj otchet o zashchishchennosti sotrudnikov 2020 g. [Antiphishing. Annual Employee Security Report 2020]. *Blog of Antiphishing Company*. Available at: https://blog.antiphish.ru/files/Antiphish_Employee_Safety_Report-2020.pdf (date of the application: 04.03.2021) (in Russian).
2. (2020) Big Game Hunting Comes to Big Country: Group-IB Detects Series of Ransomware Attacks by OldGremlin. *Group-IB*. Available at: https://www.group-ib.ru/media/oldgremlin/ (date of the application: 04.03.2021).
3. Kudrjavtsev A.V. (2016) Ispol'zovanie internet-khostingov dlya khraneniya uchebnoj informatsii v tselyakh realizatsii printsipov otkrytogo obrazovaniya [Use of the Internet Hosting to Store Educational Information for the Implementation of the Principles of Open Education]. *Pedagogical Education in Russia*, no. 7, pp. 32–36 (in Russian).

4. Mityukov E.A. (2019) Zhiznennyj tsikl fishingovykh atak i tekhniki ikh realizatsii [The Life Cycle of Phishing Attacks and Techniques for Their Implementation]. *Reshenie*, vol. 1, pp. 140–142 (in Russian).
5. Mityukov E.A. (2017) Uyazvimosti MS SQL SERVER, ili ispol'zovanie khranimykh protsedur v svoikh tselyakh [Vulnerabilities in MS SQL SERVER or the Stored Procedures Using for Different Purposes]. *Zaŝita informacii. Inside*, no. 6, pp. 44-47 (in Russian).
6. (2012) O vnesenii izmenenij v Federal'nyj zakon «O zashchite detej ot informatsii, prichinyayushchej vred ikh zdorov'yu i razvitiyu» i otdel'nye zakonodatel'nye akty Rossijskoj Federatsii: Federal'nyj zakon ot 28 iyulya 2012 g. № 139-FZ [On Amendments to the Federal Law "On the Protection of Children from Information Harmful to Their Health and Development" and Certain Legislative Acts of the Russian Federation]. Federal Law no. 139-FZ of July 28, 2012. *Rossijskaya gazeta*. Available at: https://rg.ru/2012/07/30/zakon-dok.html (date of the application: 04.03.2021) (in Russian).
7. (2006) Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii: Federal'nyj zakon ot 27 iyulya 2006 g. № 149-FZ [On Information, Information Technologies, and Information Protection]. Federal Law no. 149-FZ of July 27, 2006. *Rossijskaya gazeta*. Available at: https://rg.ru/2006/07/29/informacia-dok.html (date of the application: 04.03.2021) (in Russian).
8. (2020) Obzor otchetnosti ob intsidentakh informatsionnoj bezopasnosti pri perevode denezhnykh sredstv: III kvartal 2019/2020 goda [Review of Transactions Not Authorised by Customers for 3rd Quarter of 2019/2020]. *The Central Bank of the Russian Federation – Official Website*. Available at: https://www.cbr.ru/analytics/ib/review_3q_2020/ (date of the application: 04.03.2021) (in Russian).
9. Sazonova M. (2020) Moshennichestvo v seti: kak obezopasit' svoyu kompaniyu v Internete? [Online Fraud: How to Keep Your Company Safe on the Internet?]. *Garant.ru*. Available at: https://www.garant.ru/article/1417573/ (date of the application: 04.03.2021) (in Russian).
10. (2021) Fishing v Rossii [Phishing in Russia]. *TAdviser*. Available at: https://www.tadviser.ru/index.php/Статья:Фишинг_в_России (date of the application: 04.03.2021) (in Russian).
11. Chto takoe fishing [What is Phishing]. *Encyclopedia by Caspersky*. Available at: https://encyclopedia.kaspersky.ru/knowledge/what-is-phishing/ (date of the application: 04.03.2021).