УДК 004.624

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИНТЕРНЕТ-МОШЕННИЧЕСТВО: ИМЕЮЩИЕСЯ УГРОЗЫ И ГРАЖДАНСКО-ПРАВОВАЯ КОМПЕТЕНТНОСТЬ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Кузина Наталья Владимировна

кандидат филологических наук, доцент, ведущий научный сотрудник
ФГБУН Центр исследования проблем безопасности Российской Академии наук,
г. Москва, Россия

Аннотация. Обсуждаются вопросы методологического обеспечения кибербезопасности за рубежом и в Российской Федерации, механизмы интернет-мошенничества, его классификация и ответственность за него, примеры информационной уязвимости в период пандемии как для граждан, так и для организаций с удаленным режимом работы сотрудников.

Ключевые слова. Информационная безопасность, кибербезопасность, фишинг, мошенничество с применением информационных технологий, информационная уязвимость, безопасность предприятий, охрана труда.

INFORMATION SECURITY AND INTERNET FRAUD PROBLEMS: EXISTING THREATS AND LEGAL COMPETENCE OF INTERNET USERS IN THE RUSSIAN FEDERATION

Kuzina Natalia Vladimirovna

candidate of philological sciences, associate professor, leading researcher of the
Security Problems Research Center of the Russian Academy of Sciences,
Moscow, Russia

Abstract. The issues of cybersecurity methodological support abroad and in the Russian Federation, internet fraud mechanisms, its classification and responsibility for it, examples of information vulnerability during a pandemic both for citizens and organizations are discussed, with remote work mode for employees.

Keywords. Information security, cybersecurity, phishing, information technology fraud, information vulnerability, enterprise security, labor protection.

Режим самоизоляции и карантина превратил сеть Интернет в технологию, обеспечивающую продуктами первой необходимости, организующую профессиональную и образовательную деятельность в удаленном (дистанционном) формате, реализующую финансовую активность. Данная ситуация привела к росту количества случаев и к выработке новых приемов мошенничества с использованием Интернет-технологий.

В Уголовном кодексе Российской Федерации данные преступления относятся к разделу VIII «Преступления в сфере экономики», глава 21 «Преступления против собственности» (статья 159.1. Мошенничество в сфере кредитования; статья 159.2. Мошенничество при получении выплат; статья 159.3. Мошенничество с использованием электронных средств платежа; статья 159.6. Мошенничество в сфере компьютерной информации), и к разделу IX «Преступления против общественной безопасности и общественного порядка», глава 28 «Преступления в сфере компьютерной информации» (статья 272. Неправомерный доступ к компьютерной информации; статья 273. Создание, использование и распространение вредоносных компьютерных программ; статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации) [11].

Помимо индивидуальной безопасности граждан, сохранности их личных данных и финансовых ресурсов, интернет-мошенничество и в целом проблемы информационной безопасности в период COVID-19 затронули, помимо объектов критической информационной инфраструктуры, интересы всех тех компаний и организаций, которые перевели сотрудников на дистанционный режим работы (обучения).

В связи с переводом большого количества персонала на удаленный режим работы на длительный срок изменилась структура хранения данных в сети, при этом барьеры для их несанкционированного получения, уровни защиты были своевременно не разработаны. Большая сложность состояла прежде всего в изменении привычек поведения сотрудников организаций, находящихся на удаленной работе, в сети, с учетом передачи конфиденциальных сведений организации, в том числе составляющих коммерческую тайну. Сотрудникам, не

специализирующимся на защите информации и информационной безопасности, было свойственно поведение, присущее обычному потребителю, без учета ответственности за сохранность дистанционно обрабатываемых и передаваемых данных. между физическим и информационным миром имеется все меньше барьеров: почти любое производство компьютеризировано, управление часто осуществляется через микроконтроллеры, что создает уязвимости для таких объектов, как опасные производства, коммунальная сфера, системы обеспечения городов, энергосистемы. Главной целью кибератак могут быть данные микроконтроллеры, сеть передачи данных, стандартизированные протоколы, по которым передаются данные. Возникает новый вид угроз киберфизической безопасности IT систем.

Методологическая работа по предотвращению данных угроз активно ведется на Западе, в частности, сформирован компанией MITRE (https://www.mitre.org/) перечень возможных угроз и сценариев поведения злоумышленников Atta&ck (Adversarial Tactics, Techniques & Common Knowledge: Тактики, техники и общеизвестные знания о злоумышленниках, https://attack.mitre.org/), позволяющий определить, с какого типа угрозами сталкивается пользователь или компания и как именно их предотвратить (описаны тактики их предотвращения). Например, перед вторжением злоумышленники могут выполнять активное сканирование сведений о жертве для сбора информации, которая в дальнейшем может быть использована. В этом случае предполагается для защиты использование техник работы с сетевым трафиков, указывающим на шпионаж, в частности – техник выявления больших объемов трафика из одного источника (особенно если известно, что этот источник связан с ботнетом). Анализ веб-метаданных также позволяет выявить артефакты, которые могут быть отнесены к потенциально вредоносной активности [3]. Сканирование «жертвы» злоумышленниками ведется прежде всего на предмет наличия уязвимостей, а именно – это сбор информации о хосте, об имеющемся и запущенном программном обеспечении и т.п. В этом случае для предотвращения угроз применяется комплекс мер, перечисленных в источнике [8]. Кража данных производится через эксфильтрацию в различных ее видах, например: с использованием сжатия и шифрования, а также передачи данных как

по каналу управления, так и по альтернативному каналу (в том числе только в определенное время дня или через определенные интервалы времени), с помощью зеркалирования трафика, фрагментирования контента, через физический носитель (например, съемный диск или любое устройство, подключенное к USB), через облачное хранение и т.п. [4]. Данные методы используются в том числе для изъятия информации из ресурсов государственной власти [10]. Представителями MITRE Atta&ck предлагаются прогнозы и пути профилактики киберпреступности в будущем [7]. Однако в период пандемии регулярно возникают новые типы угроз, которые еще не попали в данную матрицу MITRE Atta&ck (https://attack.mitre.org/).

В Российской Федерации, где действует Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ данной проблематикой активно занимаются специалисты ФСТЭК России, где разрабатываются стандарты информбезопасности в различных сферах. Экстренное реагирование на экономические киберугрозы производят специалисты Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT) Банка России. Существуют созданные приказами ФСБ России Национальный координационный центр по компьютерным инцидентам в критической инфраструктуре Российской Федерации (Приказ от 24 июля 2018 г. № 366), а также Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (Приказ от 24 июля 2018 г. № 367), ведущая учет данных угроз. Центры изучения киберугроз и противодействия им имеются при многих региональных органах власти в субъектах Российской Федерации, при Федеральных органах исполнительной власти, в высших учебных заведениях инженерного профиля. Для Российской Федерации особенно важна методологическая работа, позволяющая классифицировать присущие отечественным реалиям киберугрозы и своевременно предотвращать их.

Помимо обеспечения национальной безопасности в сфере критических технологий, речь идет о продуктовой безопасности – о технологиях выявления атак, направленных на физический мир, в том числе на IT–интернет вещей. В

данном аспекте возникают не только инциденты в области информационной безопасности – при передаче данных, но инциденты в области охраны труда: на безопасность существенно влияют не только действия злоумышленников, но и поведение сотрудников внутри компании (или пользователей продукта). Данные технологии важны и в условиях развития современных прикладных проектов, например «Умный город» (ПАО «Ростелеком»).

Более высокая степень связанности процессов реального и виртуального мира в производстве, сфере услуг, бизнесе влияет на возникновение сетевого эффекта: малые воздействия приводят к сильному эффекту. Однако растет и стабильность системы – в силу формирования большего количества механизмов обратной связи. В связи с этим необходимы изменения в поведении бизнеса, коммунального хозяйства, производства, сферы услуг, и прежде всего - в критической инфраструктуре. Таким образом, необходимо не только защищать промышленные предприятия и производство, сферу услуг в целом от вторжения, но и обеспечить надлежащую организацию труда и технику безопасности при работе сотрудников в условиях высокой компьютеризации – то есть предугадывать возможные угрозы не только в передаче данных, но и в физическом поведении людей.

Интернет-мошенничество традиционного типа обозначается через термин «фишинг» – интернет-атака, где используются стратегии получения персональных или корпоративных конфиденциальных данных, финансового мошенничества, а также приемы, убеждающие пользователя установить вредоносное программное обеспечение. согласно исследованиям, обучение пользователей методам защиты считается низкорезультативным из-за не выработанной у них мотивации и отсутствия потребности изучать информационные материалы [5; 6].

В работе «Seven Deadliest Social Network Attacks», описывая технологии фишинга, авторы рассказывают об одном из изощренных методов получения персональных данных пользователей в сетях MySpace, Facebook, Twitter методом перенаправления на фишинговую страницу входа в социальную сеть с целью повторного введения конфиденциальных данных, пароля [9].

В США в начале 2000-х годов сложилось открытое межотраслевое научное сообщество, изучающее проблемы киберпреступности (прежде всего фишинга), регулярно публикующее годовые отчеты по активности фишинга в соотнесении с реестром доменных имена, используемых в различных странах мира. Согласно данным сообщества на 2017 г., Россия замыкала топ–10 стран, доменные имена которых наиболее активно используются при создании временных мошеннических фишинговых ресурсов (показатели: «Количество фишинговых доменов на 10000» и «Фишинговые атаки на 10000 доменов») [1, с. 13]. Около половины регистраций доменных имен с целью фишинга производятся с территории Китая. 75 % доменных имен, с которых ведется мошенническая деятельность, имеют расширение .com, .cc, .pw и .tk. Более половины (56%) из мошеннических ресурсов были организованы в 2016 году (взломаны или созданы) в реестрах .com и .net. [1, с. 10-11]. В условиях пандемии ассоциация организовала онлайн-совещание по теме «Cybercrime trends due to COVID-19», где впервые публично в научном сообществе обсудила данную проблематику по отношению к периоду пандемии [2].

В Российской Федерации в период пандемии мошенничество направлено было прежде всего на получение персональных данных, финансовых данных с целью обогащения, а также на создание атмосферы нестабильности, недоверия к органам власти, в частности, через выведение из строя официальных информационных ресурсов. IP адреса мошенников, как правило, были связаны со странами Европы, США, Китаем, Украиной. Проблематика киберпреступности в период пандемии освещалась в средствах массовой информации (приоритет оказался за наиболее мобильными электронными СМИ, связанными с органами власти – федерального центра или регионов), а также через самооповещение пользователями в социальных сетях, что в связи с мобильностью доведения информации о возможных угрозах, снизило риски и финансовые потери населения. Одной из популярных форм доведения информации стали интервью с первыми лицами отделов обеспечения финансовой безопасности банковских структур в электронных СМИ и специализированный информационный видеоконтент (например, в метро) для населения, посвященный профилактике финансового мошенничества. Несмотря на это, ряд государственных

информационных ресурсов подвергся DDoS-атакам, с них происходило массовое хищение персональных данных граждан, функционирование ресурсов приостанавливалось. Удавалось мошенничество, как правило, при наличии уязвимостей у информационного ресурса, а также благодаря неосведомленности, доверию и невнимательности граждан (в том числе и работников предприятий и организаций, работающих в дистанционном режиме).

Выделим цели мошенничества по отношению к гражданам, характерные для периода пандемии, выявленные в ходе наблюдения над информационной повесткой, прецедентами (по данным чатов и социальных сетей пользователей):

1) завладеть персональными данными (паспортные данные, СНИЛС и др.) как через взлом устройств пользователей, так и через хакерство по отношению к официальным государственным ресурсам (например, порталы госуслуги.ру, mos.ru),

2) завладеть данными счетов и электронных карт (во многих случаях, даже не имея полных данных о банковской карте, можно осуществлять платежи),

3) внедрить вредоносные программы (в личную компьютерную технику, на мобильное устройство, на сервер), похищающие персональные, финансовые данные, конфиденциальную информацию для служебного пользования,

4) путем создания фишингового ресурса получить денежные средства населения (при заказах и оплате приобретения товаров и услуг онлайн),

5) получить доступ к конфиденциальным данных бизнес-структур и государственных организаций через доступ в системы, использующиеся сотрудниками в период удаленной работы.

Способы мошенничества, применявшиеся в период пандемии (по нашим наблюдениям над прецедентами и информационной повесткой в период пандемии в чатах и социальных сетях пользователей):

1) просьбы о переводах в гуманитарные фонды или на счета пострадавших от пандемии граждан и государств,

2) требования предоплаты на фишинговых ресурсах комиссий за реальные назначенные социальные компенсационные выплаты, в том числе на несовершеннолетних детей (суммы комиссий назывались невысокие, чтобы у

граждан не возникало сомнение в необходимости или критичности для них данной оплаты, однако охват пользователей был настолько широким, что данный вид мошенничества позволил злоумышленникам получить высокий доход),

3) требования предоплаты через фишинговые ресурсы за займы/ льготные кредиты известных банков экономически пострадавшим гражданам (использовалась ложная информация о возможностях получить льготный займ с необходимостью внесения предоплаты),

4) создания фишинговых ресурсов несуществующих компаний или имитирующих известные бренды, информационные ресурсы крупных интернет-магазинов, ритейлеров для сбора предоплаты за продукцию с доставкой на дом в период самоизоляции (например, за санитарно-гигиенические средства, продукты неотложного спроса, промышленные товары),

5) реальное или фиктивное распространение с внесением предоплаты онлайн средств, предохраняющих или излечивающих от коронавируса (ладанки, талисманы, медальоны и др.),

6) рассылка фишинговых (фальсифицированных) сообщений на сайты государственных и банковских услуг с целью получения компенсаций от лица населения,

7) создание групп в социальных сетях и мессенджерах с искаженными данными по пандемии с целью поддержания паники и создания путей получения личных, финансовых данных и денежных средств населения,

8) распространение фишинга в мессенджерах и присоединение к его распространению больших массивов пользователей,

9) распространение фиктивной информации о возможности выполнения лабораторных исследований по COVID-19 на коммерческой основе или о возможностях амбулаторного обследования/ страховки/ лечения от коронавируса при условии предоплаты онлайн через фишинговый ресурс,

10) распространение информации о платных услугах по обеззараживанию и антивирусной обработке против COVID–19 (оплаченная онлайн услуга могла осуществляться, однако была не сертифицирована или ее стоимость оказывалась многократно завышена),

11) предоставление в помощь самоизолированным или находящимся на карантине гражданам лже-волонтеров, связывающиеся с жертвой посредством Интернет и телекоммуникационных технологий,

12) фишинговые рассылка от имени органов здравоохранения и ВОЗ с требованием онлайн оплаты не предоставляемых услуг,

13) рассылки сведений о ложных штрафах от ФСИН и МВД, иных органов, за нарушение самоизоляции и передвижение без пропусков с требованием о переводе средств на подставные счета,

14) DDoS-атаки с целью перегрузки линий связи и ликвидации доступа граждан к важнейшим информационным ресурсам и к официальным государственным сайтам в Интернет для создания социальной нестабильности и усиления паники,

15) фишинговые предложения о списании долга по кредитам и ипотеке (мошенники – «раздолжнители») и др.

Помимо учреждений Научно-технической службы и созданных подразделений ФСБ России, ФСТЭК России, компьютерных и экономических отделов МВД, контроль ситуации осуществляли подразделения отечественных банков, прежде всего Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT) Банка России, специалисты по защите критической инфраструктуры, а также лаборатория Касперского, лаборатория ESET и другие разработчики антивирусов и софта, частные компании или их подразделения (например – Уральский центр систем безопасности, https://www.ussc.ru/), специализирующиеся на предотвращении кибер-атак.

Применявшиеся меры профилактики мошенничества были связаны с усилением защиты информационных ресурсов с целью предотвращения их взлома, а также с информированием населения о приемах распознавания и о порядке реагирования на действия мошенников для исключения утечки персональных данных и финансовых потерь. При работе с гражданами многократно повторялась установка быть внимательнее при онлайн-оплате услуг к адресу и виду ресурса, через который производится оплата, к порядку предоставления товаров и услуг, установка не доверять e-mail и СМС–

сообщениям с неизвестных номеров и адресов, а также телефонным звонкам злоумышленников, связываться по факту мошенничества и подозрения в мошенничестве с отвечающими за безопасность государственными структурами и банками. Рекомендовалось заказывать в период самоизоляции дорогостоящую продукцию с предоплатой только на крупных ресурсах с высокой степенью информационной защиты от фишинга («Озон», «Aliexpress», «Tmall», «Юлмарт» и др.), через официальные магазины, имеющие интернет-доставку. Не сообщать личных и банковских данных в сетях открытого доступа и мессенджерах, а также незнакомым лицам, не осуществлять перевод средств неизвестным лицам и организациям, не отвечать на интернет-сообщения и не открывать электронную корреспонденцию с неизвестных адресов, не сохранять пароли доступа к ресурсам и данные банковских карт для автоматических платежей в браузерах и на мобильных устройствах.

Предлагаемая работа проводится в рамках Государственного задания ФГБУН «Центр исследования проблем безопасности РАН» на 2019 г. и на плановый период 2020 и 2021 гг. (НИР № 0006–2020–0001).

ЛИТЕРАТУРА

1.*Aaron G., Rasmussen R., R2 Cyber.* Global Phishing Survey: Trends and Domain Name Use in 2016 // APWG. Unifying the Global Response to Cybercrime. An APWG Industry Advisory. – USA, Lexington, 2017. URL: http://www.antiphishing.org/globalphishingsurvey/

2.Current cybercrime trends due to COVID-19 // APWG. – 2020. URL://apwg.org/members-webinar-cybercrime-trends-due-to-covid-19/

3.*Dainotti A. et al.* Analysis of a «/0» Stealth Scan from a Botnet// MITRE/Atta&ck, 2012, p. 1–13. URL: https://www.caida.org/publications/papers/2012/analysis_slash_zero/analysis_slash_zero.pdf

4.Exfiltration. The adversary is trying to steal data // MITRE/Atta&ck. URL: https://attack.mitre.org/tactics/TA0010/

5.*Hong J.* The state of phishing attacks // Communications of the ACM. – T. 55, V. 1, 2012. https://doi.org/10.1145/2063176.2063197

6.Jagatic T.N., Johnson N.A., Jakobsson M. & Menczer F. (2007). Social phiching // Communications of the ACM. – T. 50 (V.10), 2007. https://doi.org/10.1145/1290958.1290968

7.*O'Brien D.* Symantec 2021 Cyber. Security Predictions – Looking Tovard the Future// Broadcom. Symantec Enterprise Blogs/ Threat Intelligence. URL: https://symantec-enterprise-blogs.security.com/blogs/

8.Pre-compromise. Techniques Addressed by Mitigation // MITRE/Atta&ck. URL: https://attack.mitre.org/mitigations/M1056/

9.*Timm C., Perez R.* Chapter 3. Phishing Attacks // Seven Deadliest Social Network Attacks. – 2010, P. 43-61. https://doi.org/10.1016/B978-1-59749-545-5.00003-3

10.Waterbug: Espionage Group Rolls Out Brand-New Toolset in Attacks Against Governments // Broadcom. Symantec Enterprise Blogs/ Threat Intelligence. 2019. URL: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/waterbug-espionage-governments

11. "Уголовный кодекс Российской Федерации" от 13.06.1996 № 63 – ФЗ (ред. от 31.07.2020). http://www.consultant.ru/document/cons_doc_LAW_10699/