УДК 616.9: 004.56(476)

# ВЛИЯНИЕ COVID-19 НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ РЕСПУБЛИКИ БЕЛАРУСЬ

*Купрейчик А.С., студентка гр. 972302*

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Смирнова Н.А. – магистр техн. наук*

**Аннотация.** Пандемии относятся к числу социальных катастроф, сеющих панику, стрессовые и посттравматические стрессовые психологические травмы, массовую агрессию и прочие нарушения поведенческих реакций общества. Сила данных реакций связана с информационным влиянием на человека в период, когда в его психике оказывается постоянное, не поддающиеся рациональному контролю, воздействие. Хотя угрозы пандемии еще не отступили, уже пришло время анализа реакций, возникавших в социуме в период COVID-19.

**Ключевые слова.** Интернет, фишинг, атака, мошенничество, COVID-19, пандемия, безопасность.

Пандемия превратила Интернет в «золотую жилу» - часто единственный путь выживания, обеспечение продуктами, организации работы и образования. Данная ситуация поспособствовала росту количества новых способов мошенничества с использованием Интернет-технологий. Мошенничество всегда растет в периоды кризиса, и не важно с чем они связаны, так как в такие периоды в обществе начинается паника и уровень внимательности, к получаемой информации, снижается [1].

Фишинг, один из самых распространенных видов мошенничество в сети, – это вид интернет-атаки, цель которой получение доступа к конфиденциальным данным пользователей [2]. Особую тревожность вызывают факты активизации виртуальных мошенников во время пандемии коронавируса, когда мошенники используют тему коронавируса как «приманку» и просят переходить по ссылке в письмах, якобы отправленных из банка. В этих письмах может оказаться «сайт-ловушка». Цель таких рассылок – узнать пароли, логины, данные карты за счет подделки сообщений от доверенного источника. Фишинговые страницы похожи на оригинальные страницы сайта банков, вследствие чего люди становятся жертвами преступников. Другими последствиями киберпреступности в период карантина стала организация большого количества сбоев в работе информационных ресурсов. Финансовые угрозы нарушения целостности данных были связаны с переходом многих предприятий на удаленный режим работы без соблюдения необходимых мер безопасности. Помимо проблем для государственных структур и бизнеса в части нарушения целостности или хищения конфиденциальных данных, внедрение хакеров вызывало, например, сбои в процессе дистанционного образования и научной работы.

Новое исследование Anti-Phishing Working Group (APWG) показало, что уровень фишинговых атак на сайты финансовых учреждений, веб-почты и сайты SaaS. рос до 2020 года, удваиваясь в течение года. Приблизительно 70 % всех доменных имен в мире, зарегистрированных в злонамеренных целях, принадлежат китайскими преступниками для использования против различных брендов и предприятий. Число выявленных и заблокированных в глобальной сети за девять месяцев 2020 года фишинговых сайтов превысило показатель прошлого года [3].

Проблематика киберпреступности в период пандемии освещалась, прежде всего, в СМИ, а также через социальные сети, что, несомненно, в связи с мобильностью доведения информации о возможных угрозах, снизило риски и денежные потери населения. Несмотря на это, ряд информационных ресурсов подвергся DDoS-атакам, с них происходило массовое хищение персональных данных граждан, функционирование ресурсов приостанавливалось из-за создававшихся злоумышленниками сбоев в их работе.

Удавалось мошенничество, как правило, при наличии уязвимостей у информационного ресурса, а также благодаря неосведомленности, доверию и невнимательности граждан в моменты наибольшей психической уязвимости (сужения коридора восприятия, флуктуации внимания в момент паники). Прежде всего, были подвержены мошенничеству граждане, находящиеся в особо сложной жизненной ситуации (многодетные семьи, лишившиеся работы граждане, одинокие престарелые люди и др.), а также сотрудники в режиме удаленной работы, оперирующие данными организаций, не предназначенными для обнародования. Интернет-мошенничество особенную опасность представляло для населения с низкой финансовой, правовой и компьютерной грамотностью. Если речь идет о мошенничестве по отношению к гражданам, то кроме неосведомленности, оно апеллирует к сильным эмоциям и жизненным приоритетам потребителей: к сочувствию, тревоге за жизнь близких, к фобиям и страхам (например, к страху перед болезнью,

страху остаться без средств к существованию, а также страху дефицита продуктов потребления) [4].

Распространение информации о борьбе с мошенниками, помимо указанных выше каналов, шло через печатную прессу, радио, телевидение, видеоэкраны в общественных пространствах, объявления в общественном транспорте.

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.

На мой взгляд, одной из причин подобного уровня мошенничества является недостаточное образовательное сопровождение. Отсутствие необходимых знаний в области Интернет и информационных технологий создает благоприятную почву для злоумышленников. В связи с этим следует сформировать систему образования соответствующим навыкам в информационном пространстве:

1) сегодня навыки пользования информационными технологиями в общих чертах преподаются в рамках информатики, но изучения вопросов информационной безопасности не имеется, в связи с чем следует ввести в школах специальную дисциплину касательно понятия и сущности сети Интернет, данная дисциплина также должна предусматривать обучение навыкам первичного пользования и поведения в виртуальном пространстве;

2) в системе высшего образования подготовка технических кадров в области информационной безопасности осуществляется в Белорусском государственном технологическом университете, Белорусском государственном университете, Белорусском государственном университете информатики и радиоэлектроники, Витебском государственном университете имени П. М. Машерова, Гродненском государственном университете имени Янки Купалы, Полоцком государственном университете, при этом современная тенденция в области кадровой политики требует подготовки специалистов в междисциплинарном русле, то есть кадров, обладающих как правовыми, так и техническими навыками обеспечения информационной безопасности;

3) следует создать программу повышения квалификации и переподготовки кадров, осуществляющих оперативно-розыскные мероприятия, дознание или следствие по преступлениям, связанным с информационной безопасностью, в правоохранительных органах [5].

В целом проблема доверия в сети Интернет является комплексной. В этой части необходимо формировать Интернет-культуру со стороны пользователей виртуального пространства путем проведения курсов и ознакомительных уроков, брошюр и иных материалов.

**Список использованных источников:**

1. Информационная безопасность в условиях пандемии: методы стабилизации состояния социума в электронных СМИ и Интернете / Кузина Н. В. // Бюллетень науки и практики, 2020 – №9. – С. 356-394.
2. Национальный правовой Интернет-портал [Электронный ресурс]. – Режим доступа : https://pravo.by.
3. APWG [Электронный ресурс]. – Режим доступа : https://apwg.org.
4. Onliner [Электронный ресурс]. – Режим доступа : https://www.onliner.by .
5. Информационная безопасность в условиях пандемии коронавируса / Расулев А. // Вестник юридических наук, 2020 – №2. – С. 224-228.

UDC 616.9: 004.56(476)

# THE IMPACT OF COVID-19 ON THE INFORMATION SECURITY OF THE REPUBLIC OF BELARUS

*Kupreijchik A.S., Student of the group 972302*

*Belarusian State University of Informatics and Radioelectronics,*
*Minsk, Republic of Belarus*

*Smirnova N.A. – Master of Science in Engineering*

**Annotation.** Pandemics are among the social catastrophes that sow panic, stress and post-traumatic stress psychological trauma, mass aggression and other violations of the behavioral reactions of society. The strength of these reactions is associated with the informational influence on a person during a period when there is a constant, not amenable to rational control, influence in his psyche. Although the threat of a pandemic has not yet receded, it is time to analyze the reactions that arose in society during the COVID-19 period.

**Keywords.** Internet, phishing, attack, fraud, COVID-19, pandemic, security.