Трибуна молодого ученого

УДК: 338.342.44
JEL: D85, D89, Y80

КАРИТИЧ Никита Игоревич
Финансовый университет при Правительстве Российской Федерации, Ленинградский проспект, д. 49, Москва, 125993, Россия.
https://orcid.org/0000-0002-9441-505X
Каритич Никита Игоревич, студент Финансового университета, Факультет Экономики и Бизнеса, Экономическая безопасность, 2 курс, Москва, Россия. E-mail: boredbro228@gmail.com

Научный руководитель: Куприянова Людмила Михайловна, кандидат экономических наук, доцент, заместитель заведующего кафедрой «Экономика интеллектуальной собственности», доцент Департамента экономики и бизнеса. E–mail: kuprianovalm@yandex.ru
https://orcid.org/0000-0002-9453-6425

АНАЛИЗ И ОЦЕНКА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ

Аннотация

Предмет: Проведение анализа и оценка экономической безопасности в сети «Интернет».

Цель: Целью работы является сбор информации, сводный анализ и первичная оценка уровня экономической безопасности в сети «Интернет», предоставление данных об объекте изучения и связанных с ним проблемах с различных сторон и точек зрения, а также введение авторских комментариев и оценки.

Методология: В данной работе использовались методы теоретического исследования: анализ, синтез, абстрагирование.

Результаты: Проведено исследование специфики экономической деятельности в сети «Интернет», различных угроз и рисков для данного вида деятельности, а также изучена связь между информационной и экономической безопасностью.

Выводы: Для экономической безопасности в сети «Интернет» существует множество различных угроз и рисков, несмотря на огромное количество мер предосторожности, и систем безопасности, поэтому производить такого рода деятельность во Всемирной Паутине необходимо грамотно, с особой осторожностью, используя все возможные средства для обеспечения её безопасности.

Ключевые слова: *экономическая безопасность, экономическая безопасность в Интернете, цифровая безопасность, информационная безопасность, оценка безопасности экономической деятельности, экономическая деятельность, киберпреступность, преступность в Интернете, мошенничество в сети.*

Young scientist tribune

Nikita I. Karitich, student, Financial University under the Government of the Russian Federation, Faculty of Economics and Business Moscow, Economic Security, undergraduate, Moscow, Russia. E-mail: boredbro228@gmail.com
https://orcid.org/0000-0002-9441-505X

Scientific advisor: Lyudmila M. Kupriyanova, PhD in Economics, Associate Professor, Faculty of Economics and Business. E-mail: LKuprianova@fa.ru
https://orcid.org/0000-0002-9453-6425
Financial University under the Government of the Russian Federation, Moscow.

ANALYSIS AND ASSESSMENT OF ECONOMIC SECURITY ON THE INTERNET

Abstract

Topic Analysis and assessment of economic security on the Internet.
Objectives The purpose of the work is to collect information, a summary analysis and a primary assessment of the level of economic security on the Internet, to provide data on the object of study and related problems from various sides and points of view, as well as to introduce author's comments and assessments.
Methodology In this study, the methods of theoretical research were used: analysis, synthesis, abstraction.
Results The study of the specifics of economic activity on the Internet, various threats and risks for this type of activity, and also studied the relationship between information and economic security.
Conclusions There are many different threats and risks for economic security on the Internet, despite the huge number of precautions and security systems, therefore, it is necessary to carry out this kind of activity on the World Wide Web competently, with extreme caution, using all possible means to ensure its security
Keywords: *economic security, economic security on the Internet, digital security, information security, security assessment of economic activities, economic activities, cybercrime, Internet crime, online fraud.*

Введение

Безопасность экономической деятельности является основополагающим элементом ведения предпринимательства и государственного управления, в рамках финансово-экономической стратегии развития бизнеса.

Сегодня экономическая деятельность как неотъемлемая часть жизни любого человека, связана с ее появлением неотъемлемой составляющей – Интернет-средой. Современные социальные институты общества с каждым годом укрепляют взаимное сотрудничество, в том числе – экономическая деятельность в Интернет-среде, и новые сферы функционирования Интернета, как и новые сферы экономической деятельности.

В Интернет-среде с каждым днём наблюдается ускорение оборота денежных средств. Это обуславливает, актуальность обеспечения

безопасности и защиты от мошенничества, возможных рисков и угроз экономической деятельности в Интернет-пространстве.

Уровень экономической безопасности в Интернет-среде напрямую зависит от уровня информационной безопасности. Безопасность финансово-экономической деятельности в Интернет-пространстве обеспечивается программистами, IT-инженерами и веб-разработчиками. В этой связи необходимо отметить значение и требование соответствующего уровня квалификации и ответственности, участвующих в процессе обеспечения безопасности функционирования бизнеса.

Исследования проблем экономической безопасности функционирования бизнеса в интернет-пространстве, позволяют выделить следующие проблемы:

Первая проблема: плохо выстроенная, с точки зрения цифровой архитектуры. Система может столкнуться проблемой отслеживания потока денежных средств и потерей прибыли компании.

Вторая проблема: не соответствующая современным требованиям работа служб безопасности и государственных органов, уполномоченных обеспечивать безопасность в интернет-среде, в том числе: экономическую безопасность для физических и юридических лиц, ведущих предпринимательскую деятельность, использующих современные средства коммуникации и сети Интернет, а также для их клиентов / пользователей услуг в цифровом формате.

Экономические преступления в цифровом пространстве

Проблема обеспечения экономической безопасности и защиты от мошенничества особенно актуальна на протяжении последних десятилетий. С появлением сети Интернет появилось множество новых инструментов для ведения профессиональной деятельности в сфере индивидуального предпринимательства. Появились и активно расширяют свое воздействие на влияние индивидуальных пользователей и захват компьютерных систем крупных компаний, – различные способы, веб-страницы и вирусы. Например, – сайты-клоны, в точности копируют страницу какой-либо организации, с отличием на один незаметный элемент в веб-адресе. Эти инструменты имеют разную степень эффективности, однако, по данным специалистов компании McAfee и Центра стратегических и международных исследований, общий ущерб мировой экономике от кибер-преступлений различных видов и форм за 2020 год составил примерно 1.1 триллион долларов.

По данным статистики информационного портала Positive Technologies, статистика кибератак на различные ресурсы и сервисы за первый квартал

2021 года значительно превышает показатели в сравнении с 2020 годом[1] (рис. 1).

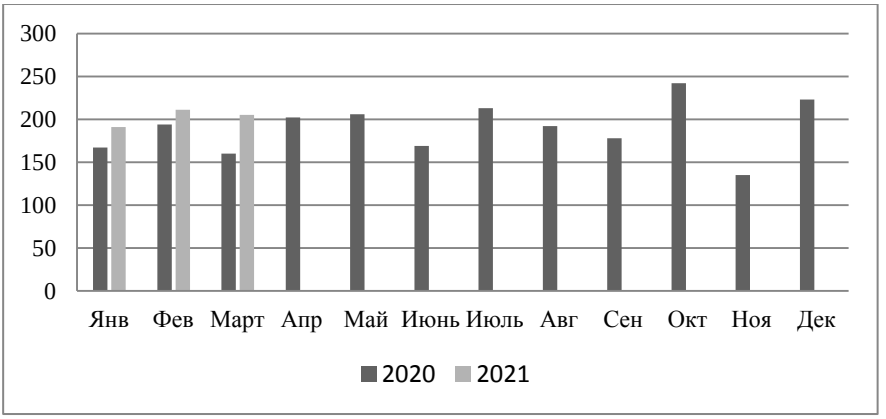

Рисунок 1 – Количество инцидентов в 2020 и 2021 годах / Number of incidents in 2020 and 2021г. Источник: www.ptsecurity.com

Данные статистики показывает, что основной интерес злоумышленников, ориентирован на получение каких-либо личных данных частных лиц или клиентов организаций, очевидно, для использования их для получения в дальнейшем каких-либо финансовых выгод путём их продажи новым владельцам информации. При этом приоритетом является прямое получение финансовой выгоды, когда могут быть использованы атаки на частных лиц, и атаки на организации. При этом атаки на организации показывают больший процент воздействия – 43%. (рис. 2)

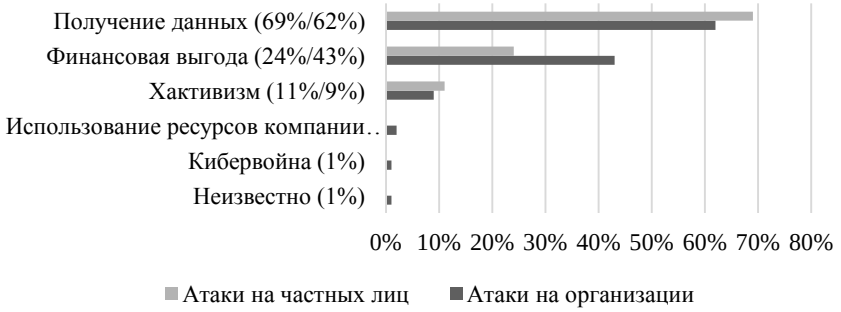

Рисунок 2 – Мотивы злоумышленников / Attackers' motives[2] Источник: www.ptsecurity.com

[1] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q1/ (www.ptsecurity.com, date of the application 01.11.2021)

[2] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q1/ (www.ptsecurity.com, 01.11.2021)

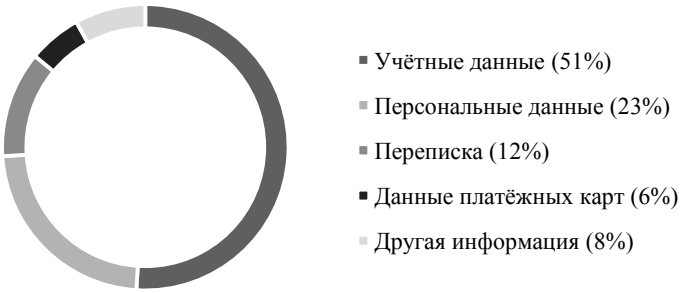

Рисунок 3 – Типы украденных данных (в атаках на частных лиц) / Types of stolen data (in attacks on individuals)

Источник: www.ptsecurity.com

Целенаправленный характер – 77% атак (от общего числа) связаны с хищением информации. Более половины атак направлены на получение учётных данных, четверть атак заинтересованы в получении персональных данных пользователей интернет-сервисов[1], например хищение данных банковских карт составляют 6%. Атаки на частных лиц составляет около 12%, остальное – на различные организации – 88%, при которых 31% от объёма украденных данных составляют персональные данные сотрудников и клиентов. 24% от общего объёма данных – хищение коммерческой тайны, что наиболее серьёзно влияет на экономическую безопасность пострадавших организаций. В равных долях злоумышленников заинтересовали медицинская информация, базы данных клиентов и данные платёжных карт – 6%.

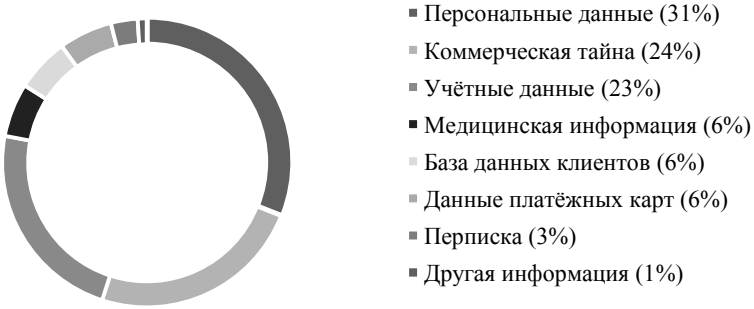

Рисунок 4 - Типы украденных данных (в атаках на организации) / Types of stolen data (in attacks on companies)

Источник: www.ptsecurity.com

[1] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q1/ (www.ptsecurity.com, date of the application 01.11.2021)

Представленная статистика подтверждает актуальность обеспечения экономической безопасности в интернет среде и зависимость от защиты безопасного хранения и передачи информации. Необходимость безопасности функционирования организации в работе с различными системами, связанными с сетью Интернет пространства. Особое внимание следует обратить на «облачные» формы и серверы компании в своей деятельности, предоставляющей услуги облачного хранения данных, либо непосредственно в виртуальном пространстве[1].

Ошибки при формировании систем

Проблема обеспечения экономической безопасности имеет свою специфику, которая заключается в том, что ошибки совершаются на фазе формирования архитектуры системы, то есть – в самом начале ее создания. Например, автомобиль, построенный на слабой защите безопасности, невозможно исправить, даже в условиях завода-производителя. Возможна только разработка нового поколения модели – на основе новой спроектированной архитектуре. Если здание, построенное с архитектурными и инженерными ошибками, невозможно перестроить, – возможен только снос и строительство с нуля. Объективно это связано с огромными экономическими потерями, а также срывом исполнения всех сроков сдачи объекта. Именно поэтому многие компании, даже если замечают какие-либо критические недочёты, оставляют их без изменений, «закрывая глаза», и также после очередного хищения информации о данных пользователей их системы или другого подобного события, приносят публичные извинения, обещают исправить выявленные проблемы, при этом создают другие ошибки. Компании, как правило, не признают собственные ошибки и стараются не показывать какие-либо уязвимости в собственных системах.

Один из самых стабильных источников подобной системы является компания Facebook, ныне Meta. На протяжении долгих лет, стабильно, раз в несколько месяцев происходили утечки личных данных пользователей продуктов корпорации, в том числе и информация финансового характера, данные банковских карт и счетов. Это позволяет относить эти случаи к крахам систем экономической безопасности, так как страдали не только пользователи, чьи данные были похищены, но и инвесторы и держатели акций и прочих активов корпорации Facebook, которые теряли свои доходы. При этом, рейтинг компания падал.

Некомпетентность контролирующих органов

Сегодня государственные органы на протяжении последних двух лет, активно проводят мероприятия и очные встречи с менеджерами, и

[1] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q1/ (www.ptsecurity.com, date of the application 01.11.2021)

специалистами, разъясняя цели их деятельности, выявляя признаки финансовой пирамиды, контроль наличия лицензий для ведения деятельности. Однако, уполномоченные органы не активно участвуют в контроле и не принимают меры выявления опасности. Например, по действующим компаниям в области Блок-чейн и криптовалюты, правоохранительные органы не активно воздействуют, учитывая отсутствие у них алгоритмов и навыков выявления нарушений, а также, не имеют отработанных процедур по противостоянию и расследованию преступной деятельности в этой сфере. С такими проблемами сталкиваются в разных странах, не только Россия, по всему миру ситуация в данной сфере примерно одинакова. Например, в Египте, Непале, Северной Македонии, Алжире и Бангладеш запрещено взаимодействовать с криптовалютами любым способом как юридическим, так и физическим лицам, однако самыми первыми такой запрет ввели власти Боливии в 2014 году, тем самым создав прецедент. Катар и Бахрейн запрещают своим гражданам инвестировать в криптовалюту на своей территории. Власти Вьетнама запрещают использовать конкретную криптовалюту - Bitcoin, в качестве платёжного средства, за нарушение данного закона предусмотрены крупные штрафы, однако нет запрета на покупку и продажу его в виде актива. В Китае частные лица имеют право владеть цифровой валютой, но с 2013 года действует запрет на операции с ней для финансовых организаций. В 2017 году в Китае закрыли все криптобиржи и ограничили проведение ICO. В апреле 2021 года в Турции начал действовать закон, запрещающий использование криптовалют в качестве платежного средства для расчетов за товары и услуги. В России криптовалюта легализована, но как виртуальный актив или товар, но не как платежное средство[1].

В настоящее время в России начинается оптимизация экспертной деятельности, в поддержку правоохранительных органов в борьбе с простыми телефонными мошенниками. Сегодня разработаны современные технологии, способные практически мгновенно пресекать незаконные действия мошенников.

Говоря об экономической безопасности всего общества в целом, основной вектор воздействия на мошенников, остается проблема – безнаказанность, в то время когда похищенные средства выводятся за пределы страны.

[1]https://www.mn.ru/smart/v-velikobritanii-bespreczedentnoe-kolichestvo-kriptovalyutnyh-kompanij-ne-soblyudayut-zakon-po-borbe-s-otmyvaniem-deneg-na-segodnyashnij-den-tolko-pyat-firm-poluchili-sootvetstvuyushhuyu
(date of the application, 03.11.2021)

Важно отметить возможности цифровой экономики, когда почти все подобные преступные операции проводятся либо с использованием, либо вовсе полностью в Интернете. Именно в среде интернет ресурсов выстраиваются системы, позволяющие отследить любые операции и всех пользователей всех страны мира.

Заключение

Несмотря на большое количество мер предосторожности, систем безопасности, правильно работающих законодательных решений и сформированных компетенций специалистов государственных органов и специальных служб, Интернет-среда остается источником угроз экономической безопасности на всех её уровнях и во всех её формах. Оценивая экономическую деятельность в сети Интернет, важно учитывать активный прогресс совершенствования технологий, заинтересованность компаний в защите своей деятельности и обеспечении безопасности в рамках собственных ресурсов, что побуждает компании совершенствовать определённые процедуры и техпроцессы, а также активность в просвещении клиентуры, что крайне актуально и для коммерческих банков. Сегодня экономическая безопасность в интернет среде оценивается относительно на удовлетворительном уровне. Тем не менее, ошибки разработчиков, веб-архитекторов, и требующих повышение компетентности уполномоченных служб в решении проблем обеспечения экономической безопасности, создают высокий уровень угрозы. Решение данных проблем возможно при грамотном использовании сервисов, веб-ресурсов и приложений.

Список источников

1. Демидова, Поляруш (2017) – Демидова А.С., Поляруш А.А. // Мошенничество в сети интернет как угроза экономической безопасности молодежи // Наука и образование сегодня. – 2017. – № 12.

2. Кунявский (2021) – Кунявский, С.С. // ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ТЕНЕВОЙ ЭКОНОМИКИ // Форум молодёжной науки. – 2021. – № 4.

3. Мальцева, Балашова, Ершова, Корнусова (2021) – Мальцева С.М., Балашова Е.С., Ершова Е.А., Корнусова В.М. // Финансовые пирамиды: современное состояние и способы борьбы / // Азимут научных исследований: экономика и управление. – 2021. – № 1.

4. Моденов, Власов (2020) – Моденов, А.К., Власов М.П. // Особенности экономической безопасности в цифровой экономике // Петербургский экономический журнал. – 2020. – № 2.

5. Шулик (2021) – Шулик, И.С. // Теоретические аспекты экономической безопасности // Форум молодёжной науки. – 2021. – № 3.

References

1. Demidova, Polyarush (2017) – Demidova A.S., Polyarush A.A.// Online fraud as a threat to the economic security of youth // Science and education today [Nauka i obrazovaniye segodnya]. – 2017. – № 12.

2. Kunyavsky (2021) – Kunyavsky S.S.// Theoretical aspects of the shadow economy // Forum of Youth Science [Forum molodozhnoy nauki]. – 2021. – № 4.

3. Maltseva, Balashova, Ershova, Kornusova (2021) – Maltseva S.M., Balashova E.S., Ershova E.A., Kornusova V.M. // Financial pyramids: current state and methods of fight / // Research Azimuth: Economics and Management [Azimut nauchnykh issledovaniy: ekonomika i upravleniye]. – 2021. – № 1.

4. Modenov, Vlasov (2020) – Modenov A.K., Vlasov M.P. // Features of economic security in the digital economy // Petersburg economic journal [Peterburgskiy ekonomicheskiy zhurnal]. – 2020. – № 2.

5. Shulik (2021) – Shulik I.S. // Theoretical aspects of economic security // Youth Science Forum [Forum molodozhnoy nauki]. – 2021. – № 3.