УДК 338.23

МЕТОДОЛОГИЯ ПРОТИВОДЕЙСТВИЯ КИБЕРМОШЕННИЧЕСТВУ ДЛЯ ЦЕЛЕЙ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Гречкин Д.Д.

Студент

Сибирский институт управления – филиал РАНХиГС

Российская Федерация, г. Новосибирск

Черепкова Т.Н.

Заведующий кафедры Налогообложения, учета и экономической безопасности, канд. экон. наук, доцент

Сибирский институт управления – филиал РАНХиГС

Российская Федерация, г. Новосибирск

Аннотация: На фоне глубокой рецессии мировой экономики наблюдается стремительное развитие информационно-коммуникационных технологий, что сопровождается повышением угроз безопасности граждан, общества и государства со стороны киберпреступников. Нынешний инструментарий не позволяет в полной мере обеспечить защиту финансов и персональных данных граждан. В результате исследования был предложен комплексный метод борьбы с мошенничеством в сети Интернет, основанный на совместной работе IT-специалистов, экономистов, юристов и общественных молодежных движений.

Ключевые слова: экономическая безопасность, национальная безопасность, угрозы экономической безопасности, Интернет-мошенничество, кибермошенничество, информационная безопасность.

METHODOLOGY OF COUNTERING CYBER FRAUD FOR THE PURPOSES OF ENSURING ECONOMIC SECURITY

Grechkin D.D.
Student
Siberian Institute of Management – branch of RANEPA
Russian Federation, Novosibirsk

Cherepkova T.N.
Head of the Department of Taxation, Accounting and Economic Security, Candidate of Economic Sciences, Associate Professor
Siberian Institute of Management – branch of RANEPA
Russian Federation, Novosibirsk

Annotation: Against the background of a deep recession of the world economy, there is a rapid development of information and communication technologies, which is accompanied by an increase in threats to the security of citizens, society and the state from cybercriminals. The current tools do not allow to fully protect the finances and personal data of citizens. As a result of the study, a comprehensive method of combating fraud on the Internet was proposed, based on the joint work of IT specialists, economists, lawyers and public youth movements.

Keywords: economic security, national security, threats to economic security, Internet fraud, cyber fraud, information security.

В стремлении упростить жизнь и улучшить её качество человечество создаёт для этого различные инструменты, одним из таких инструментов являются информационные технологии. Однако процесс перехода от

традиционного к инновационному зачастую является тернистым, а иногда болезненным.

Это показал 2020, пандемийный, год, когда все развитые страны были переведены на дистанционный режим не только работы, но и жизни. Традиционные покупки еды, одежды и иных экономических благ, оплата коммунальных услуг и прочие товарно-денежные отношения перешли в глобальную сеть Интернет. И если технологии, позволяющие осуществить такой переход, показали свою эффективность, то подготовленность государственного аппарата и простых людей, не являющихся профессионалами в сфере информационных технологий, осталась на уровне ниже среднего.

Этим в свою очередь и воспользовались мошенники. Официальная статистика Министерства внутренних дел Российской Федерации [5] показывает резкий скачок сведений о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации по статье 159 УК РФ (таблица 1).

Таблица 1 – Количество сведений о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий

Отчетный период	**Количество сведений о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий**	**Прирост, % (+/-)**
Январь-Декабрь 2019	119 903	–
Январь-Декабрь 2020	210 493	75,6
Январь-Декабрь 2021	238 560	13,3

Прирост составил колоссальные 75%, а самое печальное, что даже после выхода населения из самоизоляции, тенденция роста преступлений сохранилась. Причиной тому послужила, как было упомянуто ранее, неподготовленность государственного аппарата к пресечению подобного рода преступлений. Об этом говорит и статистика раскрытых преступлений

прошлых лет за 2021 г. – по статьям 159-159.6 УК РФ было раскрыто всего 7 806 преступлений, т.е. 3,7%. Снижения темпов роста преступлений не стоит ожидать и по причине того, что число пользователей сети Интернет с низким уровнем информационной грамотности неуклонно растёт: в глобальную сеть вовлекаются даже самые отдаленные регионы Российской Федерации, население которых на данный момент является слабозащищённым.

Экономическая безопасность является неотъемлемой частью в обеспечении национальной безопасности страны, наравне с обороной, экологией и научно-техническим развитием [2]. И здесь нужно понимать, что мошенничество нужно рассматривать не только как угрозу экономической безопасности отдельно взятого гражданина, но и как угрозу для развития человеческого потенциала и общественной безопасности. Общественная опасность рассматриваемого преступления обуславливается тем, что в результате его совершения незаконно перераспределяются ресурсы в процессе экономической деятельности [4, 61]. Ведь в «лучшем» случае похищенное имущество направится мошенниками на улучшение качество своей жизни за счёт простых граждан, а в худшем случае – отправятся на финансирование терроризма и иностранных агентов.

В ст. 159 УК РФ дано точное определение мошенничества – это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием [1]. В этом и кроется, пожалуй, самая главная причина успеха мошенников – жертва добровольно, сама этого не осознавая, позволяет злоумышленнику посредством социальной инженерии завладеть чужим имуществом. Если в случае с обычной кражей факт преступления можно точно доказать, путём отточенных оперативно-розыскных мероприятий, то в случае с мошенничеством факт обмана пострадавшего доказать проблематично, особенно в сети Интернет.

На сегодняшний день можно выделить 2 категории наиболее обобщённых и распространённых мошеннических схем в Интернете:

1. Невыполнение договорных отношений – устаревший, но не потерявший своей актуальности благодаря технической модернизации, способ кражи денежных средств. Суть заключатся в фиктивной покупке или продаже несуществующего товара. Первый вариант можно разобрать на простом примере: на торговых интернет-площадках мошенник пишет продавцу о желании приобрести товар через «безопасный платёж» и отправляет ему ссылку на одностраничный сайт, который полностью копирует внешний вид оригинального сайта с очень похожим доменным адресом. Продавец вводит данные своей банковской карты для получения денежных средств, но происходит обратное.

Во втором случае злоумышленник выкладывает объявление о продаже дорогой вещи по цене ниже рыночной, получает за неё предоплату или полную стоимость, после чего удаляет свой профиль и блокирует все каналы связи с жертвой. Другой пример: молодой человек знакомится с девушкой на популярном сайте знакомств, она предлагает ему встретиться, предварительно забронировав столик в кафе, которое она хорошо знает. Она даёт жертве ссылку на страницу в социальной сети, где указаны контактные данные, адрес и поддельные положительные отзывы. В этом «заведении» бронирование столика является платным – жертва переводит деньги, приходит в назначенное время по адресу, но никого там не находит, а страницы девушки и заведения уже удалены.

2. Фишинг (от англ. «fishing» – рыболовство) – самый опасный и технически подкованный способ, заключающийся в «вылавливании» персональных данных граждан, отсюда и название. Опасность заключается в том, что при получении данных банковской карточки жертвы, можно украсть

все имеющиеся там денежные средства, а при получении личных данных – злоумышленник может систематически шантажировать свою жертву.

Основой этой категории мошенничества является создание фишинговых сайтов-зеркал популярных интернет-магазинов и государственных сайтов, а также ботов в мессенджерах для сбора и систематизации данных. Данный способ хорошо комбинируется с предыдущим, и пример такой комбинации с «безопасным платежом» был упомянут ранее.

Противодействие кибермошенничеству должно быть комплексным и осуществляться с двух направлений – со стороны общественности и государственного аппарата. Во-первых, как когда-то старшее поколение научило нас, молодое поколение, читать и писать, так и мы обязаны научить слабо осведомлённую в области информационной безопасности часть населения страны обезопасить себя в сети Интернет. Обязаны распространять информацию о действующих мошеннических уловках, указывать на часто совершаемые ошибки пользователями сети Интернет, обучать безопасному пользованию всеми доступными информационно-телекоммуникационными технологиями.

Во-вторых, необходимо привлекать молодежь к сотрудничеству с общественными движениями «МедиаГвардия» и «Лига безопасного интернета», цель которых – искоренение опасного контента путем самоорганизации и объединения усилий профессионального сообщества, участников интернет-рынка и рядовых интернет-пользователей для совместного выявления интернет-сайтов, сообществ и групп в социальных сетях, специализирующихся на распространении противоправного контента. Вся собранная ими информация передается в профильные ведомства для принятия решений по блокированию их работы. При реализации этих проектов используются средства государственной поддержки, выделенные в качестве гранта в соответствии с Распоряжением Президента Российской Федерации №

11-рп от 17.01.2014 г. и на основании Протокола заседания конкурсной комиссии от 18.06.2014 г. Общероссийской общественной организации «Российский союз молодежи».

В-третьих, необходимо на законодательном уровне закрепить взаимодействие таких общественных движений с Советом по обеспечению экономической безопасности. Для реализации данной меры необходимо создание технически оснащенного и наполненного квалифицированными кадрами отделения при Совете безопасности Российской Федерации, к функционалу которого будет относиться формирование базы нелегальных сайтов и ведение координационной работы со специалистами технической поддержки Интернет-провайдеров, хостингов и ведущих мировых социальных сетей с целью максимально оперативного блокирования сайтов и аккаунтов мошеннических организаций. Рабочий состав подобного аппарата должен состоять из взаимодействующих друг с другом специалистов юридической направленности, специалистов технических областей, специалистов экономической безопасности, итогом деятельности которых будет информационно-аналитическое обеспечение предупреждения, выявления, пресечения, раскрытия и расследования экономических и налоговых преступлений, связанных с противоправными действиями в сети Интернет [6, 81].

В-четвертых, созданной группой технических специалистов, юристов и экономистов нужно апробировать инструменты машинного обучения, которые, опираясь на сформированную базу заблокированных Интернет-ресурсов, будут в автоматическом режиме выявлять и блокировать фишинговые сайты, сайты с экстремистским контентом и т.п.

Таким образом, количество преступлений мошеннического характера в сети Интернет растёт, и это продолжится, если уже сейчас не начать принимать меры по комплексному противодействию. Игнорирование такого опасного вида

киберпреступления несет большую угрозу экономической безопасности, а впоследствии подрыву национальной безопасности государства. У нас есть все необходимые инструменты для реализации проекта не только по противодействию кибермошенничеству, но по искоренению его как такового. Для этого требуется совместная усердная работа специалистов информационно-технической сферы, юристов и экономистов, органов охраны правопорядка, задействовано должно быть всё население – от отдельно взятого гражданина до государственного аппарата.

Библиографический список:

1. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 09.03.2022). Доступ из справ.-правовой системы «Консультант Плюс». Источник: http://www.consultant.ru/document/cons_doc_LAW_10699/8012ecdf64b7c9cfd62e90d7f55f9b5b7b72b755/ (дата обращения: 29.03.2022).

2. О Стратегии национальной безопасности Российской Федерации : указ Президента РФ от 02.07.2021 N 400.

3. Организация предупреждения правонарушений в сфере экономики : учебник для бакалавров / В. И. Авдийский, Ю. В. Трунцевский, А. В. Петренко, И. Л. Трунов ; под общей редакцией Ю. В. Трунцевского. — М.: Издательство Юрайт, 2022. — 272 с. — (Бакалавр. Академический курс). — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/508910 (дата обращения: 29.03.2022).

4. Русанов, Г. А. Экономические преступления : учебное пособие для вузов / Г. А. Русанов. — М.: Издательство Юрайт, 2022. — 224 с. — (Высшее образование). — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/488739 (дата обращения: 29.03.2022).

5. Сайт Министерства внутренних дел Российской Федерации. URL: https://xn--b1aew.xn--p1ai/reports/1/ (дата обращения: 29.03.2022);

6. Сергеев Д.Р., Любименко О.А., Савватеева О.В. Мошенничество в сети интернет как угроза экономической безопасности государства // Теоретическая экономика. – 2020. - №3. - С. 76-84.

7. Экономическая безопасность : учебник для вузов / Л. П. Гончаренко [и др.] ; под общей редакцией Л. П. Гончаренко. — 2-е изд., перераб. и доп. — М.: Издательство Юрайт, 2022. — 340 с. — (Высшее образование). — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489082 (дата обращения: 29.03.2022).

Оригинальность 85%