Научная статья
УДК 343.85:[343.34:004](74)

Анастасия Викторовна Пейзак
Уфимский юридический институт МВД России, Уфа, Россия, a.peyzak@gmail.com

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ В США

Аннотация. Статья подготовлена в качестве доклада участника межведомственного семинара «Актуальные вопросы противодействия преступлениям, совершаемым с использованием IT-технологий», проведенного 13 октября 2022 г. в Уфимском юридическом институте МВД России. Говоря о противодействии киберпреступности в США в данной статье, автор исходит из содержания социально-политического смысла предупреждения преступности, при этом отдавая себе отчет в том, что предупреждение преступности в целом, а не конкретного преступления является целью, к достижению которой должны стремиться как специальные правоохранительные органы, так и институты общества в целом, включая коммерческие организации. В работе описывается модель взаимодействия государственных органов и коммерческих структур США, направленная на противодействие преступным проявлениям в информационно-телекоммуникационной сфере.

Ключевые слова: мошенничество, зарубежные страны, США, ФБР, IC3, профилактика, IT, киберпреступление, киберпреступность, фишинг

Для цитирования: Пейзак А. В. Противодействие киберпреступности в США // Общество, право, государственность: ретроспектива и перспектива. 2022. № 4 (12). С. 54–59.

Original Article

Anastasia V. Peyzak
Ufa Law Institute of the Ministry of Internal Affairs of Russia, Ufa, Russia, a.peyzak@gmail.com

COUNTERING CYBERCRIME IN THE USA

Abstract. The article has been prepared as a report of the participant of the interdepartmental seminar «Topical issues of counteracting crimes committed using IT-technologies», held on October 13, 2022 at the Ufa Law Institute of the Ministry of Internal Affairs of Russia. Speaking about countering cybercrime in the USA in this article, the author proceeds from the content of the socio-political sense of crime prevention, while being aware of the fact that crime prevention in general, and not prevention of a specific crime is the goal that should be achieved both by specialized law enforcement agencies and by the institutions of society as a whole, including commercial organizations should strive to achieve. The article describes a model of interaction between state bodies and commercial structures of the USA, aimed at counteracting criminal manifestations in the information and telecommunication sphere.

Keywords: fraud, foreign countries, USA, FBI, IC3, prevention, IT, cybercrime, cybercrime, phishing

For citation: Peyzak A. V. Countering cybercrime in the USA // Society, law, statehood: retrospective and perspective. 2022. No. 4 (12). P. 54−59.

Преступность в сфере информационно-телекоммуникационных технологий в XXI веке стала глобальным вызовом, значение противодействия которой признают в странах СНГ, ШОС, Лиге арабских государств, Совете Европы и ООН. За 5 лет, с 2015 г., количество пользователей, получивших доступ к сети Интернет, увеличилось более чем на 1 млрд человек, а число пользователей различных социальных сетей неуклонно стремится к отметке в 4,5 млрд [1].

Из-за преступлений в сфере информационно-телекоммуникационных технологий человечество теряет около 1,25 %

ВВП ежегодно, что отражается на торговых отношениях, развитии добросовестной конкуренции, прогрессе инноваций и росте экономики вышеуказанных стран. Для сравнения, это лишь на десятую долю процента меньше ущерба, который наносит международный терроризм и организованная преступность, почти на треть процента больше ущерба от подделки товаров и на почти четверть процента больше ущерба от незаконного оборота наркотических средств и психотропных веществ. При этом, по прогнозу аналитиков, в денежном выражении 2022 г. принесет убытков мировой экономике более чем на 2 трлн американских долларов [2].

Неиллюзорность вреда, который несет в себе киберпреступность, для общества, частного сектора экономики и государственных структур США осознается Правительством, толкая его на организацию и координирование борьбы с современными глобальными киберугрозами. О реализации некоторых из таких шагов и пойдет речь ниже.

В числе первых двадцати государств Соединенные Штаты Америки ратифицировали Будапештскую конвенцию по борьбе с киберпреступностью Совета Европы для того, чтобы объединить усилия по предупреждению преступлений, использующих возможности современных торговых отношений между ведущими странами (свобода перемещения услуг и товаров, капитала и данных посредством информационно-телекоммуникационной сети Интернет).

Будапештская конвенция вступила в силу в 2007 г. В рамках Конвенции США оказывали поддержку процессам международной гармонизации существенных и процессуальных законодательств в области борьбы с киберпреступностью посредством создания неформального канала сбора и обмена информацией среди стран Большой семерки, круглосуточных контактных узлов и координации усилий стран-доноров в оказании содействия развивающимся странам. Кроме того, правоохранительные органы США регулярно сотрудничают с большим количеством стран-партнеров в области ареста и экстрадиции преступников для их судебного преследования в США или других странах [3].

После того, как стало неоспоримым фактом то, что огромное количество аспектов жизни современного человека с немыслимой скоростью переносится в Интернет, который таит в себе немало угроз и опасностей, Правительство Соединенных Штатов Америки объединило усилия государственного аппарата и частного сектора в противодействии проявлениям киберпреступности.

На протяжении вот уже нескольких лет в США октябрь объявляется месяцем осведомленности о кибербезопасности, что стало хорошей традицией [4]. Не стал исключением и октябрь 2022 г. Во главе с Федеральным бюро расследований США (далее – ФБР) партнерские агентства призывают граждан защищать свои цифровые устройства и информацию, хранящуюся онлайн, от преступников, давая при этом соответствующие рекомендации по соблюдению «кибергигиены», и не забывать сообщать о случаях компрометации данных или попытках завладеть ими через специальную форму на сайте Центра жалоб на интернет-преступления (далее – IC3) ФБР.

IC3 ФБР опубликовал свой ежегодный отчет. Статистика о преступлениях в Интернете за 2020 г. включает информацию о 791 790 жалобах о подозрении в совершении интернет-преступлений (на 300 000 жалоб больше по сравнению с 2019 г.) и сообщает о понесенных убытках, превышающих 4,2 млрд долларов. В тройку основных преступлений, о которых сообщали жертвы в 2020 г., вошли мошенничество с фишингом, мошенничество с невыплатой/недоставкой товаров и вымогательство. Жертвы потеряли больше всего денег из-за мошенничества с компрометацией деловой электронной почты, использования преступниками романтических схем и схем, основанных на личном доверии, а также мошенничества, связанного с инвестициями. Примечательно, что в 2020 г. появились мошеннические схемы, использующие пандемию COVID-19.

IC3 получил более 28 500 жалоб, связанных с COVID-19, при этом мошенники были нацелены как на компании, так и на частных лиц [5].

В дополнение к статистике отчет IC3 об интернет-преступлениях за 2020 г. содержит информацию о наиболее распространенных интернет-мошенничествах, затрагивающих общественность, и предлагает рекомендации по предотвращению и защите. В нем также освещается работа ФБР по борьбе с интернет-преступностью, включая недавние примеры. Наконец, в Отчете об интернет-преступлениях за 2020 г. объясняется миссия и функции IC3.

IC3 предоставляет общественности надежный и удобный механизм для сообщения ФБР о предполагаемых интернет-преступлениях. Бюро анализирует и обменивается информацией из поданных жалоб в следственных и разведывательных целях, для правоохранительных органов и для информирования общественности.

С выпуском Отчета о преступлениях в Интернете за 2020 г. ФБР напоминает общественности о необходимости немедленно сообщать о подозрениях в преступной деятельности в Интернете через форму на сайте IC3. Таким образом, сообщая о преступлениях в Интернете, жертвы не только предупреждают правоохранительные органы о выявлении фактов преступной деятельности, но и помогают в общей борьбе с киберпреступностью.

В рамках информирования потенциальных жертв Правительство США призывает с подозрением относиться к сообщениям в социальных сетях или онлайн-просьбам от людей, утверждающих, что они пострадали от недавней трагедии или стихийного бедствия. Гражданам рекомендуется не отправлять деньги неизвестным физическим лицам или компаниям, не проверив их добропорядочность и законность деятельности по сбору средств.

Кроме того, советом для сотрудников компаний, служащих государственных органов и корпораций, а также обычных граждан является просьба не открывать никакие вложения электронной почты и не нажимать ссылки, если не ожидается получения файла, документа или счета от коллеги/знакомого и если не подтвержден адрес электронной почты отправителя. Одним из распространенных способов введения жертвы в заблуждение является способ, при котором мошенники имитируют известный сайт или адрес электронной почты, используя небольшое изменение в написании, например, специальные символы или цифры вместо букв, заменяя, переставляя, удаляя или удваивая похожие буквы.

Отдельно упоминается об угрозе использования бесплатных зарядных станций в аэропортах или торговых центрах, которые могут заразить устройство потенциальной жертвы вредоносными программами или программами слежения. Чтобы избежать подобных неблагоприятных последствий гражданам рекомендуют использовать собственную вилку и зарядное устройство, вставлять которые можно лишь непосредственно в розетки.

Наиболее распространенными средствами и способами, которыми пользуются киберпреступники в США, являются: мошенничество с компрометацией деловой электронной почты, кража личных данных, использование программ-вымогателей, спуфинг и фишинг. Все большую угрозу для молодежи несет разрушительная деятельность так называемых Интернет-хищников. Со всеми этими угрозами потенциальным жертвам предоставляется возможность ознакомиться детально, перейдя по соответствующей ссылке на официальном сайте ФБР, то есть пользователю не приходится самостоятельно искать информацию в поисковых системах, на что, как правило, может не хватать ни времени, ни желания у потенциальной жертвы.

К профилактическим мерам предупреждения киберпреступности в США можно отнести следующие рекомендации потенциальным жертвам, следование которым существенно снизит их индивидуальную виктимность:

– осведомленность и бдительность каждого пользователя подключенного к Интер-

нету устройства об основных способах совершения киберпреступлений;

− поддержание системы и программного обеспечения в актуальном состоянии;

− установка надежной антивирусной программы, имеющей хорошую репутацию;

− соблюдение осторожности при подключении к общедоступным сетям Wi-Fi, включая запрет на совершение конфиденциальных операций (например, покупки, авторизации в банк-клиентах, сделки на онлайн-бирже и т. п.);

− создание надежной и уникальной парольной фразы для каждой учетной записи, которую регулярно необходимо менять. Чтобы не запутаться в паролях, можно использовать какое-либо общее предложение, в тексте которого буквы заменяются специальными символами, а регулярно сменяемая часть пусть включает в себя название сервиса, приложения или сайта и месяц установки;

− настройка многофакторной аутентификации для всех учетных записей, в которых она разрешена. Вероятность того, что злоумышленник помимо доступа к данным учетной записи получит физическую возможность прочитать код на телефоне или компьютере жертвы значительно ниже;

− изучение адреса электронной почты всей входящей и исходящей корреспонденции, URL-адреса веб-сайтов прежде чем отвечать на сообщение или посещать сайт. Также пользователям рекомендовано не нажимать на ссылки, картинки или кнопки в нежелательных электронных письмах или текстовых сообщениях;

− осторожность с указанием информации, которая доступна неопределенному кругу лиц в онлайн-профилях и учетных записях в социальных сетях. Злоумышленники, зная имена домашних животных, членов семьи и название школы, могут получить подсказки, необходимые им для угадывания паролей или ответов на секретные вопросы учетной записи;

− не отправлять платежи неизвестным людям или организациям, которые ищут денежную поддержку и призывают к немедленным действиям. Мошенники почти всегда пытаются создать паническое настроение у жертвы, не давая времени на обдумывание действий или возможности посоветоваться с кем-то, вынуждая совершить платеж или передать данные банковской карты незамедлительно (во время общения по телефону или в переписке в социальной сети).

В США продвигается командный подход к борьбе с киберпреступностью через уникальные центры, где правительство, промышленность и академические круги формируют долгосрочные доверительные отношения. Одним из таких центров является Национальная совместная группа по расследованию киберугроз (далее − NCIJTF). ФБР возглавляет эту целевую группу из более чем 30 совмещенных агентств разведывательного сообщества и правоохранительных органов. NCIJTF организован вокруг специализированных центров, обоснованных в ключевых областях сферы информационно-телекоммуникационных технологий США, и возглавляется высшим руководством партнерских агентств. Через эти специализированные центры правоохранители и разведка объединяются для максимального воздействия на киберпреступность, угрожающей США.

Отдельного внимания заслуживает предоставление возможности в максимально короткий срок и наиболее простым способом для Интернет-пользователя передать сообщение в единый для всей страны IC3. Соответствующие заявления о преступлениях используются как в следственных, так и разведывательных целях, а также могут помочь в восстановлении потерянных средств. Посетители сайта IC3 могут получить дополнительную информацию, включая советы и данные о текущих тенденциях киберпреступности. К сожалению, жертвы телефонных или интернет-мошенничеств в России зачастую теряют время в раздумьях, куда им обратиться (в кредитную организацию, Центральный банк, полицию, Федеральную службу по финансовому мониторингу или к оператору сотовой связи). Информация о наличии единого центра обработки подобных сообщений жертв киберпреступлений в Рос-

сии до граждан не доводится. Дополнительно гражданам или организациям в случае, если они стали жертвой вторжения в сеть, утечки учетных данных или атаки программы-вымогателя, предлагается обратиться непосредственно в ближайший местный офис ФБР или сообщить об этом на сайте.

Бюро является ведущим федеральным агентством по расследованию кибератак и вторжений. ФБР собирает и передает разведывательные данные и взаимодействует с жертвами, работая над разоблачением тех, кто совершает злонамеренные действия в киберпространстве, в какой бы стране они ни находились. У ФБР есть специально обученные кибер-отряды в каждом из 56 территориальных офисов, которые работают вместе с партнерами по межведомственным оперативным группам. Группа быстрого реагирования (Cyber Action Team) может быть развернута по всей стране в течение нескольких часов для реагирования на крупные инциденты.

Имея помощников по юридическим вопросам в посольствах по всему миру, ФБР тесно сотрудничает с международными партнерами, добиваясь справедливости для жертв международной киберпреступности. IC3 собирает сообщения об интернет-преступлениях от общественности. Используя такие жалобы, команда IC3 по восстановлению активов за период с 2016 по 2020 гг. помогла заморозить и в последующем вернуть более 2,2 млрд долларов США жертвам киберпреступлений [5]. CyWatch − это круглосуточный оперативный центр ФБР и дежурная служба, обеспечивающая поддержку для отслеживания инцидентов и связи с местными офисами по всей стране.

Стратегия ФБР в предупреждении киберпреступности заключается в том, чтобы подвергать киберпреступников риску и последствиям, а цель — в изменении поведения преступников, угрожающих сетям, финансовой и интеллектуальной собственности, критически важной инфраструктуре США, которые считают, что сами они ничем не рискуют. Для достижения этих целей Правительство Соединенных Штатов использует сочетание полномочий как на национальном уровне, так и на уровне международных организаций, имеющихся технических возможностей и наличия партнерских отношений по всему миру, чтобы киберпреступники несли ответственность за свои деяния против граждан, компаний и государственных структур США по всему миру.

Эффективность данной стратегии можно проиллюстрировать на примере телефонного мошенничества, которое поразило граждан Российской Федерации в последние годы. Ни для кого не секрет, что подавляющее большинство соответствующих атак производилось с территории соседнего государства, партнерские отношения с которым не позволяли пресечь данную преступную деятельность. Правительству и правоохранительным органам Украины не было никакого дела до организованной преступности Днепропетровска, которая основным объектом преступных посягательств выбрала граждан России. Когда силы Российской Федерации, задействованные в специальной военной операции, подобрались непосредственно к границам Днепропетровска, объем соответствующих мошеннических атак на граждан России сократился на порядок.

Таким образом, можно однозначно прийти к выводу, что киберпреступность, являясь комплексной глобальной проблемой в силу того, что вести борьбу государствам приходится с преступниками, находящимися за пределами своих территорий, требует ответственной и эффективной взаимной работы с иностранными партнерами и частным сектором, несмотря на существующие политические или экономические противоречия. Организованная киберпреступность, которая сегодня атакует США или Российскую Федерацию, завтра, потеряв такую возможность, будет вынуждена переключиться на другие территории, даже если вчера там на нее закрывали глаза. При этом немаловажно организовать взаимодействие государственных структур и частного сектора экономики, который заинтересован в первую очередь в обеспечении безопасности своих активов. Виктимологическая профилактика ведется и

в России, однако от киберпреступности, на наш взгляд, более эффективными будут не билборды и социальная реклама на остановках, а всплывающие окна и баннеры в социальных сетях, так как современные пользователи с каждым днем проводят все больше и больше времени именно в киберпространстве.

СПИСОК ИСТОЧНИКОВ

1. Global Digital 2022: вышел ежегодный отчет об интернете и социальных сетях – главные цифры (2022). URL: https://www.sostav.ru/publication/we-are-social-i-hootsuite-52472.html (дата обращения: 01.10.2022).

2. Потенциальный ущерб от киберпреступности в 2022 году оценили в ₽165 млрд (2022). URL: https://www.gazeta.ru/business/news/2022/02/17/17304823.shtml (дата обращения: 01.10.2022).

3. Киберготовность США 2.0: Киберпреступность и охрана правопорядка (2022). URL: https://digital.report/kibergotovnost-ssha-2-0-kiberprestupnost-i-ohrana-pravoporyadka/ (дата обращения: 01.10.2022).

4. October Is Cybersecurity Awareness Month. URL: https://www.fbi.gov/investigate/cyber (дата обращения: 01.10.2022).

5. Internet Crime Report 2020. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (дата обращения: 01.10.2022).

REFERENCES

1. Global Digital 2022: The annual report on the Internet and social networks – the main figures (2022) has been released. URL: https://www.sostav.ru/publication/we-are-social-i-hootsuite-52472.html (date of access: 01.10.2022). (In Russ.)

2. The potential damage from cybercrime in 2022 was estimated at ₽165 billion (2022). URL: https://www.gazeta.ru/business/news/2022/02/17/17304823.shtml (date of access: 01.10.2022). (In Russ.)

3. US Cyber Readiness 2.0: Cyber Crime and Law Enforcement (2022). URL: https://digital.report/kibergotovnost-ssha-2-0-kiberprestupnost-i-ohrana-pravoporyadka/ (date of access: 01.10.2022). (In Russ.)

4. October Is Cybersecurity Awareness Month. URL: https://www.fbi.gov/investigate/cyber (дата обращения: 01.10.2022).

5. Internet Crime Report 2020. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (дата обращения: 01.10.2022).

Информация об авторе:
Пейзак А. В. – кандидат юридических наук.

Information about the author:
Peyzak A. V. – Candidate of Law.

Статья поступила в редакцию 16.10.2022; одобрена после рецензирования 28.10.2022; принята к публикации 15.12.2022.

The article was submitted 16.10.2022; approved after reviewing 28.10.2022; accepted for publication 15.12.2022.