КЛЮЧЕВЫЕ ПОКАЗАТЕЛИ И ТЕНДЕНЦИИ РОСТА КИБЕРПРЕСТУПНОСТИ В ПЕРИОД ПАНДЕМИИ COVID-19 В РОССИИ И ЗА РУБЕЖОМ

Айнутдинова К.А., *канд. юрид. наук, магистр психологии, доцент, Университет управления «ТИСБИ»;*

Айнутдинова И.Н., *д-р пед. наук, профессор, ИМО, Казанский (Приволжский) федеральный университет*

Аннотация. Цель статьи - определить ключевые показатели и тенденции роста киберпреступности в период пандемии COVID-19. Выявлены детерминанты и основные виды киберпреступности; описан механизм совершения и сокрытия ряда преступлений; сделан вывод о необходимости усиления мер киберзащиты.

Ключевые слова: пандемия COVID-19, киберпреступность, фишинг, инфодемия, социальная инженерия.

Обращение к теме исследования обусловлено тем, что пандемия COVID-19 стала благодатной почвой для разнообразных видов киберпреступности, а ее взрывной рост зафиксирован во всем мире, включая Российскую Федерацию. В частности, данные, ежемесячно публикуемые Генеральной прокуратурой РФ на портале правовой статистики, указывают на рост (+29,4%) преступлений в сфере IT-технологий (ИКТ) или компьютерной информации, при этом на такие деяния (81,5 тыс.) сегодня приходится каждое из четырех регистрируемых преступлений. Наиболее распространены мошенничества (68%), совершенные с использованием сети Интернет (50,4 тыс.) или при помощи средств мобильной связи (32,8 тыс.), а также на 24,5% выросло число краж с банковских счетов или в отношении электронных денежных средств граждан и организаций (25 тыс.) [6]. Столь же неутешительная статистика по росту киберпреступлений (~300%) прослеживается в отчетах правоохранителей за рубежом (Интерпол, Европол, ФБР и др.) [1; 7; 10].

Анализ отечественной и зарубежной литературы по теме изучения вкупе с данными статистики позволяет выделить ключевые показатели и тенденции роста киберпреступлений в период пандемии. Эксперты сходятся во мнении, что драматические изменения, происходящие в повседневной жизни людей, включая вынужденный переход многих сфер общественной жизни в киберпространство для сдерживания распространения COVID-19 и минимизации экономического ущерба, общее ухудшение эмоционально-психологического состояния населения на фоне волнообразных скачков заражений вирусом и неготовность, как крупных организаций, так и отдельных граждан, противостоять нарастающим угрозам их информационной безопасности (ИБ) стали сегодня основными детерминантами, определяющими состояние и тренды киберпреступности во всем мире [2; 7; 10].

Ежегодный отчет «Hi-Tech Crime Trends 2020/2021» (Тенденции высокотехнологичной преступности), недавно представленный Международной компанией Group-IB (Россия), специализирующейся на расследовании и предотвращении кибератак, содержит исчерпывающие сведения об обновлении и усложнении киберпреступлений на волне пандемии и на фоне развития IT-технологий, анализ эволюции стратегий, тактики и инструментов современных киберпреступников и необходимых мер противодействия им, включает оценку глобального характера ландшафта киберугроз, прогнозы их развития и др. [8].

Главным трендом 2021 г., по мнению аналитиков Group-IB, является стремительный рост финансовых мошенничеств, а также краж персональных данных и денежных средств с кредиток и банковских счетов с использованием методов социальной инженерии. В контексте ИБ такие методы направлены на психологическое манипулирование людьми с целью принудить их к совершению определенных действий заведомо не в их интересах, например, к разглашению конфиденциальной информации (логинов, паролей, номеров карт и др.), участию в подложных лотереях, аукционах, благотворительных акциях и др. [3; 7; 8]. Установлено, что злоумышленники расширяют традиционные схемы онлайн-мошенничества и нещадно эксплуатируют тему пандемии и психологическое состояние жертв для совершения своих фишинговых и вишинговых атак [1; 7; 8].

В сложных условиях пандемии отмечен и такой негативный тренд, как массовое распространение в социальных сетях и массмедиа дезинформации о COVID-19. Волна фейковых слухов, сплетен и домыслов вкупе с навязчивыми предложениями сомнительных методов лечения и оказания псевдомедицинских услуг получила название «инфодемия». Злоумышленники, помимо финансового интереса, стремятся посеять страх, панику и разобщенность в обществе, породить неверие в возможности систем здравоохранения противостоять вирусу и пр. [10].

Примерами фишинга в сети Интернет (англ. phishing) являются массовые и единичные рассылки электронных писем или текстовых сообщений с заманчивыми предложениями от псевдобанков, государственных органов, учреждений здравоохранения, магазинов известных брендов и пр., побуждающие пользователей пройти по ссылке на сайты-иммитаторы с вредоносным программным обеспечением (ПО) [3]. Пользуясь изменениями в поведенческих моделях людей на фоне жестких ограничений и неизвестности, фишеры ловко подстраиваются под новую реальность и направляют свои атаки на социально-значимые цели, а также товарно-денежную и досугово-рекреационную сферы. Не случайно, что наибольшее количество фишинга было зарегистрировано в таких секторах, как онлайн-сервисы (39,6%), почтовые сервисы (15,6%), финансовые учреждения (15%), облачные хранилища (14,5%) и платежные сервисы (6,6%) [8].

Другой вариант применения злонамеренного психологического воздействия (социальной инженерии) на «клиентов» – это уже ставшие массовыми и даже привычными вишинговые схемы (англ. vishing; voice phishing – устный фишинг) [3]. Преступники звонят потенциальным жертвам через программы-анонимайзеры или SIP-протоколы и, играя определенную роль (сотрудника банка, полиции, налоговой инспекции), под разными предлогами просят предоставить паспортные данные, реквизиты банковских карточек, коды, поступающие на телефонный номер клиента банка, и иную конфиденциальную информацию. Часто своими действиями преступники стимулируют жертвы к совершению определенных операций со своим счетом или платежной картой в ущерб их интересам. В том и другом случае цель злоумышленников – получение

идентификационных данных пользователей (логины, пароли к банковским картам и учетным записям), ведущее к извлечению финансовой выгоды [3; 9].

Фишинг часто сопровождается многоходовыми действиями преступников, нацеленными на более крупные жертвы, чем единичный клиент атакованного ими компьютера [7]. Например, компьютер отдельного сотрудника корпорации, временно переведенного в онлайн-режим работы, может быть адресно атакован и заражен вредоносным ПО. Такой сотрудник может в силу доверчивости или легкомыслия открыть вредоносные вложения или ввести свои пароли на фишинговых сайтах. Далее через скомпрометированный ими легитимный аккаунт сотрудника посредством технологии EAC-скам (англ. Email account compromise / компрометация почтового аккаунта пользователя) преступники совершают следующую аферу, так называемую BEC-скам атаку (англ. Business email compromise) – с использованием корпоративной электронной почты. В итоге, хакеры получают доступ в корпоративную сеть для дальнейшей установки банковских троянов (банкеров) типа Metamorfo, вирусов-шифровальщиков семейства Ryuk, DoppelPaymer, REvil или криптолокера поколения ProLock [1; 8]. По данным ФБР, EAC и BEC-аферы «стоили» американцам в 2020 г. порядка 1,8 млрд. долл., что составило около 43% от всех потерянных средств за минувший год, а убытки от активности вымогателей возросли до 29 млн. долл. и более, причем таких преступлений стало больше на ~225-300% [7].

При всей многоярусности механизма фишинговых и вишинговых атак мотив совершения данных деяний остается прежним – это кража денег или конфиденциальной информации, которую можно далее продать, то есть извлечь материальную выгоду. Задачи, однако, при этом кардинально меняются; они усложняются и искусно адаптируются под актуальную повестку дня, связанную с пандемией COVID-19 (например, с появлением вакцины жертв начали склонять предоставить данные для записи на вакцинацию, заплатить деньги за «укол» вне очереди) [7]. Техника и способы исполнения киберпреступлений, напротив, упрощаются и ускоряются за счет использования инновационных IT-технологий (дистанционный формат работы, новые вирусы, трояны и пр.) и готовых решений

(подставные счета, фальшивые инвойсы, вымышленные сделки и пр.) [1; 7]. На смену массовым атакам «на живца» приходят целевые (таргетированные) кибератаки, направленные на крупные предприятия, организации здравоохранения, образовательные учреждения, объекты базовой и критической инфраструктуры с целью получения большей выгоды или вывода из строя «целевых жертв» [8; 10]. Например, недавно канадский производитель устройств для Интернета вещей (IoT) Sierra Wireless вынужден был остановить производство после того, как стал жертвой атаки программы-вымогателя [8].

Способы сокрытия следов киберпреступлений тоже становятся все более изощренными и технологичными. Сегодня злоумышленники редко отправляют нелегально добытые деньги на собственные банковские счета; они все чаще параллельно совершают другое преступление – «кражу личности» (англ. Identity theft). Они незаконно используют персональные данные жертвы для создания фейковых банковских счетов и получения средств, которые далее быстро выводят и конвертируют в криптовалюты. Латентность в этом секторе киберпреступности крайне высока из-за отсутствия видимых следов и анонимности источников [6].

Действия преступников, однако, сегодня зачастую не ограничиваются лишь шифрованием файлов и требованием значительного выкупа за их разблокирование. Эксперты в области кибербезопасности отмечают, что все чаще злоумышленники начали продвигать программы-шифровальщики как услугу RaaS (англ. Ransomware-as-a-Service) и сдавать вымогателей «в аренду» в обмен на часть выкупа [7; 9; 10]. Более того, по данным отчета специалистов Интерпола [10], можно сделать вывод, что кибермошенники и хакеры все реже работают поодиночке и на региональном уровне. Напротив, они группируются в транснациональные сообщества, действуют организованно и под управлением высококлассных профессионалов, активно и практически открыто проводят рекрутинг новых членов банд, всячески стимулируют молодых и талантливых людей вступать в их ряды [2]. Например, преступная группа, стоящая за атакой вирусом-вымогателем REvil на компанию Acer (Тайвань) в марте 2021 г. и потребовавшая выкуп в $50 млн. за «откат» своих действий, практически в то же

время разместила на русскоязычном хакерском сайте в даркнете / теневой сети (англ. DarkNet) биткойн на сумму $1 млн. для привлечения новых членов. В объявлении говорилось, что группировка ищет новых «аффилированных лиц», которые бы отвечали за взлом организаций с помощью программ-вымогателей Ransomware, а публично предложенные на форуме деньги должны были только подчеркнуть реальные финансовые возможности для найма новых сотрудников.

Становится очевидным смещение вектора киберпреступности в сторону организованной и транснациональной преступности [2; 10; 11]. По данным ФБР, Интерпола и др. организаций [7; 10], сегодня ~80% преступлений в сети Интернет совершается организованными группировками с неустановленной численностью и действующими вне географических границ, при этом рост ущерба в мире от таких преступлений увеличивается экспоненциально. Прогнозируется, что в ближайшее время общий урон от киберпреступлений может составить $6 трлн. [4; 12]. Также максимальный социальный и экономический ущерб может быть нанесен путем компрометации критических инфраструктурных объектов, отключения людей и бизнеса от связи. Ситуация усугубляется и тем, что киберпреступность демонстрирует тенденцию к неуправляемому глобальному распространению, а IT-технологии, попадая в руки радикалов, экстремистов и хактивистов, могут нести угрозы открытых военных операций с использованием кибероружия [4; 5; 9; 12].

На фоне происходящих изменений в киберсреде и нарастания исходящих от нее угроз отмечается трансформация социально-криминологического портрета киберпреступников и их жертв [5]. Для осуществления преступной деятельности в сфере IT-технологий в условиях динамично развивающейся экономики хакеру уже недостаточно быть просто молодым дипломированным программистом, пусть и обладающим незаурядными навыками работы с сетевыми ресурсами. Сегодня для описания хакера понадобится много иных навыков, качеств, свойств и личностных черт, характеризующих его криминальный профессионализм [2; 5]. Перечисление некоторых из них может сформировать псевдоположительный портрет хакера в глазах общественности. Действительно, реализация, например, технически сложных преступных деяний с интеграцией социальной инженерии невозможна

без глубоких знаний психологии, экономики и иных смежных наук. Сокрытие следов преступления и уход от ответственности могут потребовать знаний в сфере юриспруденции, в том числе уголовного права, основ криминологии, криминалистики и пр. Коллаборация в преступных сообществах для успешного достижения общих преступных целей требует умений коммуникации, сотрудничества и работы в команде; совершение кибератак на правительственные и инфраструктурные объекты может ложно восприниматься некоторыми как проявление смелости и решительности [2; 5; 9]. Однако тот факт, что жертвами преступников сегодня могут стать люди из любой сферы занятости, любого возраста (включая детей), достатка, воспитания, а моральный и финансовый ущерб, наносимый киберпреступностью, сопоставим по масштабам с самим коронакризисом, лишает хакера романтического флера.

Подводя итоги проведенному исследованию, резюмируем, что пандемия COVID-19 оказала беспрецедентное влияние на различные области жизни людей, включая современный технологический уклад и информационную безопасность. Статистика всплеска кибератак во всем мире [1; 6-8; 10-11] свидетельствует об активном использовании злоумышленниками темы пандемии для осуществления своей преступной деятельности, в том числе с применением методов социальной инженерии. Перечень киберугроз при этом постоянно пополняется, а жертвами становятся как крупные организации, так и простые обыватели. География, цена и сложившийся ландшафт киберпреступности растут и расширяются [8]; появляются все новые транснациональные преступные группы и сообщества, отличающиеся слаженностью и высокой организацией при планировании атак, выборе преступных целей и их осуществлении [2; 9]. Отмечается, что пандемия COVID-19 обнажила все риски и уязвимости сети Интернет при коммуникации, транзакциях, передаче данных и пр., а уровень борьбы с киберпреступностью пока не соответствует ее масштабам. Сегодня, как никогда ранее, остро стоит задача усиления мер по противодействию киберугрозам [12]. На глобальном уровне – это может быть сотрудничество между государствами и организациями в рамках ООН, Интерпол, Европол и др.; на региональном – усиление работы

правоохранителей, пересмотр законодательства в сторону ужесточения мер ответственности, взаимодействие между государственным и бизнес-секторами; на индивидуальном (пользовательском) уровне – повышение осведомленности о кибератаках, базовых мерах безопасности, основных правилах кибергигиены и пр.

Список источников:

1. Боль К. Поймать вирус киберпреступности, дезинформации и пандемии COVID-19: Отчет (на рус. яз.) / Кэтрин де Боль / Исполнит. директор, Европол. - 3 апр. 2020 г. - 12 с.

2. Бондарь М.М., Жукова С.С. COVID-19 как детерминанта развития организованной преступности // Общество: политика, экономика, право. - 2020. - № 12 (89). - С. 119-123.

3. Касперский Е.В. Что такое вишинг? / Vishing / Угрозы. [Электронный ресурс]. - URL: https://www.kaspersky.ru/resource-center/definitions/vishing (дата обращения: 09.04.2021).

4. Путин В.В. Видеообращение на пленарном заседании юбилейной 75-й сессии Генеральной Ассамблеи Организации Объединенных Наций (22.09.2020). [Электронный ресурс]. - URL: http://kremlin.ru/events/president/news/64074 (дата обращения: 12.04.2021).

5. Пучков О.А. Социально-криминологический портрет хакера: концептуальный образ // Вопросы российского и международного права. - 2020. - № 3А. - Т. 10. - С. 60-71.

6. Состояние преступности в России за январь-декабрь 2020 г.: Ежемесячный сб. о состоянии преступности в России за январь-февраль 2021 г. / Отчет Генпрокуратуры РФ / Портал правовой статистики. [Электронный ресурс]. - URL: http://crimestat.ru/analytics (дата обращения: 10.04.2021).

7. Abbate P. (2021). The FBI’s Internet Crime Complaint Center / IC3’s 2020 Internet Crime Report / Paul Abbate / Deputy Director of Federal Bureau of Investigation, USA (March 2021). - P. 30.

8. Paganini P. (2020). Group-IB, a global threat hunting and intelligence company, has presented its annual Hi-Tech Crime Trends 2020/2021 report / Pierluigi Paganini // Security Affairs (November 2020). [Electronic resource]. - URL: https://securityaffairs.co/wordpress/111434/cyber-crime/hi-tech-crime-trends.html (Retrieved on 14.04.2021).

9. Radoni A. (2020). Cyber-crime during the COVID-19 pandemic / Adil Radoini. Freedom from Fear (f3magazine, UNICRI). - Iss. 16. - P. 6-10.

10. Stock J. (2020). Cybercrime: COVID-19 Impact. INTERPOL Cybercrime Analysis Report / Jürgen Stock / INTERPOL General Secretariat, Lyon, France (August 2020). - P. 20.

11. The Global Risks Report 2020 / Insight Report 15th Ed. / World Economic Forum (WEF) in partnership with Marsh & McLennan and Zurich Insurance Group, Switzerland. - 102 p.

12. The Global Risks Report 2021 / Insight Report 16th Ed. / World Economic Forum (WEF) in partnership with Marsh McLennan, SK Group and Zurich Insurance Group, Switzerland. - 97 p.