DOI 10.35775/PSI.2025.119.2.017
УДК 32.37

Е.Р. ОЩЕПКОВ
стажер-исследователь научной группы «АСЕАН+, БРИКС+, НАТО+: перспективы азиатской интеграции в новом мировом порядке» Факультета мировой экономики и мировой политики НИУ ВШЭ,
Россия, г. Москва
E-mail: eroshchepkov@edu.hse.ru

ПРОБЛЕМА ЦИФРОВОЙ ПРЕСТУПНОСТИ В ЯПОНИИ: ПОСЛЕДНИЕ ТРЕНДЫ И ПОЛИТИЧЕСКИЕ ПОСЛЕДСТВИЯ[1]

Хотя на протяжении десятилетий Япония позиционирует себя как высокотехнологичную державу, реальная ситуация на поприще информационных достижений в стране оставляет желать лучшего. Число киберпреступлений в Японии ежегодно растет с такой скоростью, что полиция уже не справляется с растущей угрозой. Относительно мелкие инциденты расследуются, но более крупные дела по сей день не раскрыты. В 2024 году японское правительство объявило тревогу на национальном уровне и выразило готовность перенимать американские практики борьбы с хакерами. В рамках данной статьи предпринята попытка проанализировать динамику цифровых преступлений в Японии, разобрать несколько наиболее известных кейсов и составить выводы о влиянии киберугрозы на японское общество. По мере развития научно-технического прогресса во всем мире, негативный эффект от регулярных взломов и утечек данных лишь продолжит расти.

Ключевые слова: *преступность, безопасность, киберпреступность, кибербезопасность, Япония, общество, политика.*

Часть 1. Предыстория. По мере развития информационных технологий и их повсеместного внедрения в жизнь современного общества неизбежно увеличивается и частота совершаемых кибер-преступлений; Япония не является исключением из этого правила. По состоянию на начало-середину 2020-х годов, численность цифровых атак возросла в 35 раз за последние 10 лет (при этом количество DDoS атак увеличивается в 15 раз ежегодно) [10]. Число совершенных хакерами преступлений тоже увеличивается, но в арифметической, а не геометрической прогрессии: 2014 год – 7905, 2015 год – 8096, 2016 год – 8324, 2017 год – 9014, 2018 год – 9040, 2019 год – 9519, 2020 год – 9875, 2021 год – 12209, 2022 год – 12369, 2023 год – 12479 [11]. Факт неспособности японских правоохранителей успевать

[1] Публикация подготовлена в ходе реализации проекта № 25-00-05 («АСЕАН+, БРИКС+, НАТО+: перспективы азиатской интеграции в новом мировом порядке») в рамках Программы «Научный фонд Национального исследовательского университета “Высшая школа экономики” (НИУ ВШЭ)».

за негативными трендами свидетельствует о повышенной угрозе кибер-преступлений для общественной безопасности. По сравнению с общим объемом ежедневно совершаемых взломов сайтов/серверов это – капля в море. Переход львиной доли образовательной и экономической активности на онлайн платформы в период пандемии COVID-19 лишь усугубили ситуацию [3].

Чуть более оптимистичную картину можно обнаружить в направлении консультаций по вопросам кибер-преступлений, проводимых сотрудниками Национального Полицейского Агентства. Если в начале 2010-х годов советы цифровой грамотности получали только 17 тысяч японцев, то к концу декады информационная поддержка была оказана уже для 84 тысяч человек [14].

Стоит отметить, что превентивная борьба с цифровой преступностью в любых видах и формах остается приоритетом японского государства на протяжении всего XXI столетия. Взлом или кража личных данных на онлайн-платформах – грубое нарушение статьи № 21 Конституции Сева («は、これをしてはならない。のは、これをしてはならない», «Не допускается ни цензура, ни нарушение тайны любых средств связи») [15].

Хакеры в цифровом пространстве Японии действуют как в одиночку, так и в составе организованных группировок. По статистике правоохранителей, целью онлайн-взломов в абсолютных величинах гораздо чаще становятся малые предприятия (52% атак), а не крупные (36% атак) [16]. Большая степень ущерба малому бизнесу объясняется их большей численностью. 99.7% предприятий в Японии попадают в категорию SME [17]. При этом в относительных измерениях шансы крупного бизнеса стать мишенью для хакеров выше. Причина – их капитал и влияние на рынке. На рубеже 2010-х и 2020-х годов интенсивность хакерских атак вышла на новый уровень. Количество взломов систем безопасности предприятий увеличилось на 31% с 2020 по 2021 год; численность атак на одну случайную компанию резко возросла с 206 до 270 по сравнению с аналогичным предшествующего года [18].

Часть 2. Современность. Основной интерес для современных хакеров в Японии представляют ценности нематериальные. Прежде всего, речь идет о личных сведениях и уникальной информации. При этом финансовые убытки (поддающиеся подсчету) относительно невелики: в 2022 году они составили 37 миллиардов йен для всех случаев онлайн атак и компьютерного мошенничества [6]. В переводе на курс рубля это приблизительно 24 миллиардов, что эквивалентно, например, бюджетным доходам городского округа Мытищи за 2024 год.

При этом риск потери засекреченных документов или персональных данных относительно высок. По статистике того же 2022 года, порядка 50% всех японских фирм и организаций пострадали от программ-вымогателей, из них 20% предприятий заплатили выкуп в том же году [4]. Проблема не в том, что сумма денег была велика (см.: первый абзац); основная трудность – в том, что материалы все равно были выгружены в сеть, то есть стали публичными. Еще одним отягощающим фактором стала невозможность восстановить цифровую инфраструктуру после кибер-атак. По оценке специалистов, 26% технического оборудования подлежало

ремонту в течении 1 недели, 25% – в промежутке от 1 недели до 1 месяца, 16% – в диапазоне от 1 до 2 месяцев, 11% – в срок больше 2 месяцев и еще 22% систем было нельзя починить вообще [5. P. 7].

Кража IP адресов и вирусы-вымогатели – не единственная проблема, с которой сталкиваются в цифровом пространстве японские граждане. Известны случаи создания онлайн-сервисов по сбору чаевых, которые неожиданно повышают порог пожертвований до 100 тысяч йен (40 тысяч рублей) [19]. И все же, в приоритете злоумышленников – доступ к учетным записям. В этом контексте необходимо упомянуть вредоносную программу Emotet, вспышка которой пришлась на 2020-2021 и особенно 2022 годы [20]. Как правило, червь проникал на устройство по спам-ссылке или через зараженный файл. В марте 2022 года число зараженных Emotet адресов увеличилось в 5 раз по сравнению с показателями 2020 года (речь идет об адресах электронной почты с доменом «JP») [21. С. 4]. Основная идея сводилась к шантажу: либо жертва выполняет условия, либо информация утекает в сеть. Обеспокоенность японского общества нарастающими проблемами цифровой уязвимости невозможно отрицать. По данным полиции, кибер-преступность в качестве важнейшей угрозы назвали 54.1% японцев – это четвертая по значимости проблема после «страха резни» (63.5%), «телефонных афер» (62.4%) и «детских изнасилований» (55.5%) [6. P. 30].

Примечательно, что значительная доля японцев оказалась не готова к «хакерскому буму» начала 2020-х годов. Только 57.6% жителей знакомы с понятием шпионских ПО (следовательно, 42.4% никогда о них не слышали); 62.7% граждан ни разу не сталкивались с фишингом (соответственно, лишь 37.3% имели о нем представление); не более 3.7% респондентов обладали сведениями о ботнетах (иными словами, остальные 96.3% были не готовы к данной угрозе) [14]. Между тем, только за 2022 год сотрудниками полиции было зафиксировано не меньше 968 тысяч попыток взлома аккаунтов путем онлайн-рассылок по электронной почте (+84% по сравнению с 2021 годом) [5. P. 2]. Частым атакам подвергались и электронные биржи. В подавляющем большинстве случаев объектом интереса со стороны мошенников были крипто-валюты – на них пришлось 93% цифровых взломов (для сравнения, доля доллара – оставшиеся 7% и доля йен – в пределах статистической погрешности) [5. P. 5].

Если рассуждать в более общих категориях, то по сферам национального хозяйства Японии данные распределены следующим образом: 33% цифровых атак пришлись на производство, 21% – на услуги, 9% – на здравоохранение, 7% – на ритейл, 7% – на строительство, 7% – на ИКТ, 6% – на образование и еще 11% – на оставшиеся отрасли [5. P. 5]. В 2023 году статистика немного поменялась. На сектор производства пришлись 34% кибер-атак, на ритейл – 17%, на услуги – 14%, на ИКТ – 8%, на строительство – 6%, на здравоохранение – 5%. Вместо образования новой целью хакеров стали финансы – их доля составила 4%. Оставшиеся категории – 13% [7. P. 1]. Данные примечательны тем, что в Японии (как, впрочем, и любой другой постиндустриальной стране) вклад сектора услуг в формирование ВВП превышает долю промышленности почти в 3 раза [22].

Если сравнить статистику по объектам кибер-атак за 2022 и 2023 годы, то динамика получается следующая: производство – было 33%, стало 34% (+1%). Ритейл – было 7%, стало 17% (+10%). Услуги – было 21%, стало 14% (-7%). ИКТ – было 7%, стало 8% (+1%). Строительство – было 7%, стало 6% (-1%). Здравоохранение – было 9%, стало 5% (-4%). Дополнительная статья: в 2022 году это образование, а в 2023 году это финансы – было 6%, стало 4% (-2%). Все остальное – было 11%, стало 13% (+2%). Итого: самые крупные перемены пришлись на сектор ритейла, где всего за год доля цифровых атак увеличилась на 10%. Ничего подобного в других областях не зафиксировано. В том, что ритейл – наиболее «лакомый кусок» для хакеров, сходятся многие эксперты и из западных государств [1], и непосредственно из самой Японии [2].

Со временем проблема кибер-преступности в Японии только набирает обороты. Ситуация столь серьезна что в 2024 году правительство объявило тревогу на национальном уровне. 10 сентября состоялась конференция по защите от цифровых угроз с участием премьер-министра Фумио Кисида и министра обороны Ицунори Онодера. В качестве выхода они видят не развитие суверенных систем противодействия кибер-атакам, а сближение с американскими коллегами. Члены ЛДП озвучили следующие тезисы: 1) нужно назначить представителя Японии в Офис национального директора США по кибер-безопасности; 2) создать в японском правительстве ведомство, копирующее Агентство национальной безопасности США; 3) добиться реорганизации японского NISC («Национальный центр информационной безопасности») для последующего внедрения инициативы ЦРУ под названием JCDC («Совместное сотрудничество в области кибер-защиты») [8].

Часть 3: Известные кейсы. Абсолютное большинство информации о японских хакерах засекречено. Либо данные скрыты самими взломщиками, либо уже вычислившими их представителями японских спецслужб. Обнародованы некоторые личные дела, но почти все они приходятся на конец 2010-х годов. Впрочем, даже они дают представление о том, как действуют японские правонарушители в онлайн-среде. Примеры: 1) «двое безработных 36 лет создали фиктивный интернет-аукцион, ущерб от платформы составил 15 миллионов йен (10 миллионов рублей)»; 2) «безработный мужчина 34 лет использовал механизм фишинга для кражи логинов и паролей у посетителей онлайн-торгов»; 3) «27-летний студент внедрил SQL-код в сервер фирмы и украл данные 160 тысяч человек»; 4) «безработный мужчина 34 лет отправлял разным компаниям под предлогом деловых жалоб электронные письма с шпионским ПО, в результате чего похитил 210 тысяч йен (что эквивалентно 138 тысячам рублей)»; 5) «офисный работник 42 лет разработал поддельный вебсайт, полностью копирующий популярное приложение – точное число жертв остается неизвестным» [14].

На основании полицейских сводок можно составить приблизительный портрет японского хакера. Возраст: около 35 лет, социальный класс: прекариат (то есть лицо потенциально уязвимое – не обладающее большим заработком или вовсе лишенное его). Впрочем, встречаются и исключения. Например,

в Осаке зафиксирован случай ареста 14-летнего распространителя вредоносных ПО (имя засекречено) [12]. Точная информация имеется лишь о тех, кто прямо сотрудничает с японским государством. Яркий пример – Асука Накадзима (27 лет), обучающая хакерским техникам юное поколение женщин-инженеров [13]. Вероятно, спустя несколько лет – по прошествии срока давности – публике откроются имена новых японских хакеров. В свое время именно это случилось с Цутому Симомура, вошедшего в историю после поимки Кевина Митника [9].

На протяжении 2020-х годов японские спецслужбы продолжают охоту за организаторами крупных кибер-нападений, но конкретные имена по сей день не названы. Специалисты предполагают, что основной виновник – КНР. Ниже приведены наиболее известные случаи цифровых атак в новейшей истории Японии: 1) «в 2021 году вследствие взлома системы японской компании Soft Bank Z Holdings в открытом доступе оказались личные данные 86 миллионов аккаунтов, зарегистрированных в приложении Line»; 2) «в том же 2021 году были украдены данные 621 клиента японского провайдера Nippon Telegraph & Telephone (NTT) – аналога МТС, Билайна или Мегафона. Не так много, но случай достаточно вопиющий»; 3) «тогда же, в 2021 году, хакеры взломали свыше 76 тысяч адресов, оставленных на платформе Fujitsu, которую использовали министерства земли, инфраструктуры, транспорта и туризма Японии»; 4) «в середине 2021 года в сети были обнародованы коды 100 тысяч платежных карт, вбитых в систему сайта Acro, обеспечивающего продажу косметики»; 5) «в начале 2022 года злоумышленники проникли в систему сразу 14 заводов Тойота и одновременно парализовали их работу – на конвейере остановились 13 тысяч автомобилей»; 6) «весной 2022 года хакеры взломали сайт кондитерской фирмы Morinaga и украли данные 1.6 миллионов клиентов». По состоянию на январь 2025 года, ни одно дело не раскрыто.

Заключение. Подводя итоги, необходимо еще раз подчеркнуть: проблема хакерских атак в Японии с годами лишь нарастает, что естественным образом сказывается на общественной и национальной безопасности. Никто не чувствует себя в полной мере защищенным. От периодических взломов страдают малые, средние и крупные предприятия, частные домохозяйства, а также государственные ведомства. Некоторые случаи действительно успешно расследуются японской полицией, однако это – лишь малая капля по сравнению с надвигающимся цунами. Киберпреступления усугубляют экономическую обстановку и порождают страх внутри и без того атомизированного общества. С последствиями перечисленных проблем либерально-демократическое правительство будет иметь дело еще долго.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Castro C.** Retail and tech firms are hackers' most wanted targets – here's what you can do about it // Tech Radar. 2024 (11) // https://www.techradar.com/pro/vpn/retail-and-tech-firms-are-hackers-most-wanted-targets-heres-what-you-can-do-about-it.

2. **Iwasawa A.** Cyberattacks on Japan soar as hackers target vulnerabilities: number doubles in three years as intruders exploit weak defenses // Nikkei Asia. 2023 (1) // https://asia.nikkei.com/Spotlight/Datawatch/Cyberattacks-on-Japan-soar-as-hackers-target-vulnerabilities.
3. **Jolly J.** Huge rise in hacking attacks on home workers during lockdown: cybercriminals are exploiting fears and chaos caused by coronavirus, says security firm // The Guardian. 2020 (5) // https://www.theguardian.com/technology/2020/may/24/hacking-attacks-on-home-workers-see-huge-rise-during-lockdown.
4. **Matsubara M.** Why Japan and the US need cyber and data security cooperation for their economic security // Sasakawa Peace Foundation. 2022 (11) // https://spfusa.org/publications/why-japan-and-the-us-need-cyber-and-data-security-cooperation-for-their-economic-security/.
5. National Police Agency (NPA). Threats in Cyberspace. 2022 // https://www.npa.go.jp/english/bureau/cyber/document/threatsincyberspace2022.pdf.
6. National Police Agency (NPA). Crime situation in 2022. 2023 // https://www.npa.go.jp/english/crime_situation_in_2022_en.pdf.
7. National Police Agency (NPA). Leaflet threats in cyberspace in 2023. 2024 // https://www.npa.go.jp/english/bureau/cyber/document/Leaflet_threats_in_cyberspace_in_2023.pdf.
8. NSBT Japan. Japan's «Active Cyber Defense» System: Now Set to Become Reality? // Asian Military Review. 2024 (10) // https://www.asianmilitaryreview.com/2024/10/japans-active-cyber-defense-system-now-set-to-become-reality/.
9. Right Code. 史上最強ハッカー対決！下村努　VS　ケビン・ミトニック (Сильнейшее хакерское противостояние в истории! Цутому Симомура против Кевина Митника). 2022 // https://rightcode.co.jp/blogs/34189.
10. **Siripala T.** Japan's Rush to Play Cyber Defense Catchup: The Japanese government plans to introduce «preemptive» cyber defense as Japanese companies face successive cyber-attacks // The Diplomat. 2024 (6) // https://thediplomat.com/2024/06/japans-rush-to-play-cyber-defense-catchup/.
11. Statista. Number of cleared cybercrime cases in Japan from 2014 to 2023. 2024 // https://www.statista.com/statistics/746963/japan-number-of-cyber-crime-arrests/.
12. **Wang W.** 14-Year-Old Japanese Boy Arrested for Creating Ransomware // The Hacker News. 2017 (6) // https://thehackernews.com/2017/06/japanese-ransomware-malware.html.
13. **Yasuda S.** Meet the Japanese hacker training a generation of female cyber-warriors // Asia News Network. 018 (7) // https://www.nationthailand.com/perspective/30350281.
14. 警察庁. 安全・安心なインターネット社会を目指して. 2018. [Национальное полицейское агентство Японии. На пути к безопасному и надежному интернет-сообществу. 2018] // https://www.npa.go.jp/hakusyo/h18/honbun/hakusho/h18/html/i1130000.html.

15. 日本国憲法 // 昭和二十一年憲法 (The Constitution of Japan // Constitution 1946) // https://www.japaneselawtranslation.go.jp/en/laws/view/174/tb.
16. 那須慎二. サイバー犯罪者を紐解く. どんな人が攻撃しているのか、攻撃されたらどうなるのか // Tokyo Cyber Port. 2024 (9). [Насу Синдзи. Разгадка кибер-преступников: что за люди атакуют Вас и что произойдет, если Вы подвергнетесь нападению // Tokyo Cyber Port. 2024 (9)] // https://tokiocyberport.tokiomarine-nichido.co.jp/cybersecurity/s/column-detail121.
17. 新井, 民夫. 世界にはばたく日本の中小企業. オンリーワン企業の優れた新技術と、そのポテンシャル // The Government of Japan, Public Relations Office 2024 (6) (Arai T. Japanese Small and Medium Enterprises Leading the World // The Government of Japan, Public Relations Office). 2024 (6) // https://www.gov-online.go.jp/hlj/ja/july_2024/july_2024-00.html.
18. カスペルスキー. サイバー犯罪とは？サイバー犯罪の種類や身を守る方法を紹介 // セキュリティ情報. 2025. [АО «Лаборатория Касперского». Что такое кибер-преступность? Узнайте о различных видах кибер-преступлений и о том, как защитить себя // Информация по безопасности. 2025] // https://www.kaspersky.co.jp/resource-center/threats/what-is-cybercrime.
19. 総務省. 実際に起きていることでネットの使い方を考えよう！ インターネットトラブル事例集 (Министерство внутренних дел и коммуникаций Японии. Подумайте о том, как Вы используете интернет, и что происходит на самом деле! Примеры проблем с Интернетом). 2022 // https://www.soumu.go.jp/main_content/000707803.pdf.
20. 須藤龍也, 藤野隆晃. 最恐コンピューターウイルスが再び 一気に感染爆発、スピードも脅威 // 朝日新聞. (Судо Т., Фудзино Т. Самый страшный компьютерный вирус снова в деле: внезапный взрыв заражений и угроза скорости // Asahi Shimbun). 2022 (3) // https://www.asahi.com/articles/ASQ3501ZRQ34ULZU00Z.html?iref=pc_ss_date_article.
21. 内閣サイバーセキュリティセンター. 我が国のサイバーセキュリティ戦略について (Центр кибер-безопасности кабинета министров. Стратегия кибер-безопасности Японии). 2022 // https://www.soumu.go.jp/main_content/000853311.pdf.
22. 経済産業省. 我が国は GDP の 7 割、就業者数の 7 割をサービス産業が占める経済社会である // サービス生産性レポート – 経済産業省 (Министерство экономики, торговли и промышленности . Япония – это экономика и общество, где на сектор услуг приходится 70% ВВП и 70% численности работников // Отчет о производительности труда в сфере услуг). 2022 // https://www.meti.go.jp/press/2021/03/20220328005/20220328006-1.pdf.

E.R. OSHCHEPKOV
Research Assistant of the Research and
Study Group «ASEAN+, BRICS+, NATO+: Prospects for Asian
Integration in the New World Order», Faculty of World Economy
& International Affairs, HSE University, Moscow, Russia

THE PROBLEM OF DIGITAL CRIME IN JAPAN: LATEST TRENDS AND POLITICAL IMPLICATIONS

Although Japan has positioned itself as a high-tech power for decades, the real situation in the field of information achievements leaves much to be desired. The number of cybercrimes in Japan is increasing annually at such a rate that the police can no longer cope with the growing threat. Relatively minor incidents are investigated, but larger cases remain unsolved. In 2024, the Japanese government issued a national alert and expressed its willingness to adopt American practices to combat hackers. This article attempts to analyze the dynamics of digital crime in Japan, study a few of the most prominent cases, and draw conclusions about the impact of the cyber threat on Japanese society. As scientific and technological progress develops around the world, the negative effects of regular hacking and data breaches will only continue to grow dramatically.

Key words: *Crime, security, cybercrime, cybersecurity, Japan, society, politics.*