УДК 336.11:004.056
DOI: 10.34020/1993-4386-2024-4-38-47

АНОНИМНОСТЬ В ДАРКНЕТЕ: КЛЮЧ К БЕЗОПАСНОСТИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ ИЛИ УГРОЗА ДЛЯ ОБЩЕСТВА

К. Е. Следнева, Т. Б. Кувалдина
Омский государственный университет путей сообщения (ОмГУПС),
Омск, Россия

В условиях прогрессивного развития цифровых технологий безопасность и анонимность в интернете становятся важными условиями в виртуальном мире, что находит отражение в феномене даркнета. Киберпреступность, являясь основной угрозой в даркнете, охватывает широкий спектр незаконной деятельности, включая распространение украденных данных. Мотивы цифровых преступников различны, начиная от денежной выгоды, заканчивая подрывом доверия к финансовым организациям, государственным структурам. Россия занимает лидирующую позицию по объявлениям о продаже украденных баз данных, а частота утечек информации только возрастает. Отмечается, что темная сеть становится не только площадкой для совершения нелегальных действий, но и местом привлечения новых специалистов в хакерские группировки. Финансовые организации для них представляют огромный интерес, так как именно через них проходят крупные денежные потоки. Этот факт создает благоприятные условия для получения значительных выкупов за украденную информацию, а также делает финансовый сектор вторым по величине лидером по убыткам от утечек данных. Несмотря на растущее внимание к безопасности отечественного финансового сектора, он остается недофинансированным по сравнению с мировыми стандартами. Даркнет представляет собой сложный феномен, где анонимность может служить как защитой прав человека, так и угрозой общественной безопасности. Пользователи действуют без страха быть пойманными, наказанными, что приводит к злоупотреблениям. Регулирование даркнета является серьезной задачей для властей и международных организаций из-за постоянного совершенствования технологий цифровых преступников, значительных отличий в законодательстве. В статье рассмотрены сущность даркнета, его плюсы и минусы, сделан вывод, что анонимность в даркнете играет ключевую роль. С одной стороны, она является инструментом защиты прав человека и личной свободы, с другой, – угрозой общественной безопасности. Поэтому вопросы приватности и киберпреступности в даркнете еще долго останутся актуальными в силу прямо пропорциональной связи экономической стабильности стран и уровня жизни их граждан.

Ключевые слова: даркнет, безопасность, экономические потери, защита данных, социальные последствия, анонимные сети.

В современном цифровом мире, где информация и коммуникации стали неотъемлемой частью жизни, вопросы безопасности и анонимности в интернете приобретают все большую актуальность. Особое внимание в этой связи привлекает феномен даркнета – скрытой части сети Интернет, недоступной для обычного поиска, известной своей связью с незаконной деятельностью.

Вплоть до XXI века о существовании даркнета знали лишь немногие. Изначально, первой сетью, которая осуществила связь между несколькими компьютерами и считается прародительницей современного Интернета стала ARPANET, разработанная в конце 1960-х годов. ARPANET продемонстрировала, как можно передавать данные между разными компьютерными системами, что положило начало новому этапу в области связи, коммуникаций [1, с. 12]. В 1970-х годах уже появился термин «даркнет», или же «темная сеть», используемый для обозначения изолированных от ARPANET сетей. Они были не доступны для общего пользования и имели специфические, зачастую неформальные, критерии доступа. С их помощью осуществлялся обмен информацией в закрытых кругах, что стало основой для дальнейшего развития более сложных, скрытых сетевых структур. Существенным шагом в обеспечении анонимности в интернете стало создание TOR (The Onion

Router) в 1990-х годах. Проект был нацелен на защиту конфиденциальности пользователей, предоставление безопасного, анонимного доступа к ресурсам сети. TOR использует многоуровневое шифрование, что делает почти невозможным отслеживание действий и открывает новые горизонты для общения, работы в интернете. Кроме того, в 2002 году специалистами Microsoft был опубликован документ под названием «Даркнет и будущее распространения информации», который стал ключевым для общественного понимания, популяризации концепции даркнета.

По наблюдениям О. А. Дворянкина, после того как информация о даркнете начала активно распространяться, как в интернете, так и вне его пределов, наблюдался резкий, заметный рост числа пользователей этих платформ [2, с. 15]. Социальные сети, блоги, специализированные форумы, новостные статьи стали местами обсуждения тем, связанных с темной сетью, привлекая внимание рядовых, а также опытных пользователей интернета, стремящихся получить доступ к информации, которая ранее оставалась недоступной.

Повышенный интерес к даркнету способствовал формированию разнообразных мифов и слухов о его структуре, функциональности. Существуют разные мнения: некоторые пользователи считают, что даркнет подразделяется на уровни из-за применения различных методов и технологий, один из которых может быть сложнее другого. Другие же утверждают, что даркнет не делится на отдельные ступени доступа, а является единой сетью, функционирующей по принципу взаимосвязанности всех компонентов. На практике, даркнет является сложной, неоднородной сетью, чем предполагается в популярных нарративах. Мифологизация даркнета, основанная на непонимании, недостатке достоверной информации, создает ложные ожидания у интернет-пользователей и усугубляет ситуацию, поскольку новички в поисках приключений или знаний, часто сталкиваются с обманом, небезопасными ситуациями. Тем не менее, большинство согласно с тем, что сеть, используемая обществом ежедневно (поверхностный интернет), составляет лишь небольшую часть всего содержимого Интернета, которая предполагает еще два раздела – глубокая и теневая сеть[1].

Поверхностный интернет индексируется и доступен через стандартные поисковые системы, такие как Google, Yandex, Yahoo. В этом сегменте располагаются публичные сайты, блоги, новостные порталы, другие ресурсы, которые могут быть свободно просмотрены пользователями. По статистике, его часть занимает менее 5 % всего интернет-содержимого. Основная характеристика поверхностного интернета заключается в том, что любой субъект, имеющий выход в интернет, может без труда найти, получить доступ к необходимой информации, представленной на этих платформах.

Глубокий интернет включает в себя контент, занимающий 90 % всех сайтов, который не индексируется стандартными поисковыми системами. Это могут быть такие ресурсы, как приватные базы данных, защищенные паролем страницы, корпоративные сети, медицинские записи, образовательные платформы. Доступ к ним обычно требует авторизации или наличия специальных ссылок. Глубокий интернет не всегда означает недоступность информации, но его ресурсы могут быть неподходящими или неправильными для общего использования без соответствующих прав доступа или авторизации.

Темная сеть (даркнет): представляет собой часть глубокого интернета, доступную только с помощью специальных программ (Tor, I2P, FreeNet), занимающую меньший объем по сравнению с поверхностным интернетом. Страницы этой сети не индексируются поисковыми системами, а доступны только для зарегистрированных субъектов конкретных сайтов, что обеспечивает высокий уровень анонимности. Даркнет использует различные методы для защиты данных, скрытия идентичности пользователей, изменения местоположения. Например, Tor, применяющий архитектуру, где данные передаются через несколько шифрующих узлов, каждый из которых знает лишь о предыдущем и следующем узле, позволяет скрывать настоящий IP-адрес, а I2P дает возможность безопасно обмениваться данными в децентрализованной сети, что особенно важно там, где уязвимости могут привести к раскрытию личной информации.

Как отмечают А. В. Свищёв, А. С. Лаухина, зачастую даркнет сравнивают с айсбергом, так как его видимая часть составляет лишь небольшую долю от всего содержимого. На поверхности интернета доступен только малый процент открытых ресурсов, тогда как под ней скрывается огромный массив данных и информации, к которым просто так не добраться [3, с. 39].

Маловероятно, что обычный пользователь доберется до даркнета случайно, так как для этого необходимо знать о существовании специализированного программного обеспечения, иметь определенную цель. Для тех, кто действительно заинтересован и хочет попасть в туда – это не составит труда, благодаря множеству доступных ресурсов, руководств в открытой сети.

Первостепенным преимуществом даркнета, за которым стремятся пользователи – высокая степень анонимности, привлекающая интерес разнообразных слоев общества. Обмен информа-

[1] Что такое глубокий и теневой интернет? URL: https://www.kaspersky.ru/resource-center/threats/deep-web (дата обращения 15.10.2024).

цией, общение без страха широко ценится, особенно для людей, находящихся в странах с жесткой цензурой или репрессивными режимами, позволяя не опасаться наказания за свои слова. Еще одним положительным аспектом является возможность доступа к информации, которая может быть недоступна, уничтожена в открытом доступе из-за блокировок или коммерческих интересов, имеющей значение для определенных сообществ. Это особенно актуально для журналистов, активистов, исследователей, которым необходимо получать доступ к ограниченным данным. Именно в даркнете такие пользователи могут найти альтернативные источники знаний, поделится опытом в своей сфере интересов. Также темная сеть предоставляет возможность экспериментировать с многими продуктами, решениями, не опасаясь столкнуться с юридическими или иными проблемами. К тому же, компании активно пользуются даркнетом для расчета за услуги, обхода санкций, а также имеют возможность получать более высокие комиссии за свои услуги, что довольно выгодно, особенно в условиях экономических ограничений[2].

Бесспорно, что даркнет используется по во многих странах и каждый его посетитель преследует свою цель. Если рассматривать распределение пользования темной сети по миру, то среднемировые ежедневные показания его использования демонстрируют следующее: на лидирующих позициях находятся Соединенные Штаты Америки с 19,69 % от общего числа пользователей, Германия – с 11,95 %, Индия – с 4,32 %. Далее в порядке снижения по количеству пользователей расположились Индонезия, Франция, Россия, Финляндия, Нидерланды, Великобритания, Египет – с 2,13 %[3] (табл. 1).

По мнению 44 % всех пользователей, даркнет – важная часть современного цифрового мира, но 32,56 % отказываются признавать его значимость. При этом, только 6,82 % субъекта оценивают его положительно, тогда как 45,45 % высказывают негативные мнения.

По мнению Д. В. Жмурова, в России, как в большинстве стран, использование темной сети не является прямым преступлением, и в целом доступ к нему легален. Однако не все используют его для реализации хороших вещей, в большей степени это платформа для осуществления незаконной, наносящей ущерб деятельности [4, с. 90].

Киберпреступность, как одна из основных угроз даркнета, охватывает широкий спектр незаконной деятельности, которая осуществляется с использованием компьютеров и интернет-технологий. К числу таких деяний относятся фишинг, мошенничество, кибератаки, распространение вредоносного программного обеспечения, различные формы шантажа и торговля незаконными товарами. Например, в 2023 г. Лаборатория Касперского выявила в темной сети, только за первую половину

Таблица 1

Среднемировые ежедневные пользователи даркнета по миру

Country	Mean daily users
United States	467,982 (19.69 %)
Germany	283,997 (11.95 %)
India	102,554 (4.32 %)
Indonesia	92,715 (3.90 %)
France	91,667 (3.86 %)
Russia	89,891 (3.78 %)
Finland	85,092 (3.58 %)
Netherlands	69,416 (2.92 %)
United Kingdom	61,458 (2,59 %)
Egypt	50,612 (2.13 %)

[2] Сайты даркнета: что это, как туда попасть и зачем это нужно URL: https://www.securitylab.ru/blog/ personal/ SimlpeHacker/353437.php (дата обращения: 15.10.2024).

[3] Dark Web Statistics 2024 – By Country, Categories, Users Opinions, Available Dark Websites, Facts and The Average Price Index. URL: https://www.enterpriseappstoday.com/stats/dark-web-statistics.html#General_Dark_Web_Statistics (дата обращения: 15.10.2024).

года, более 700 рекламных объявлений, касающихся услуг по проведению DDoS-атак с использованием устройств интернета вещей (IoT)[4], которые заметно чаще стали встречаться на форумах. Стоимость конкретного предложения варьировалась от сложности реализации атаки, соответствующей защиты у цели[5]. В отчете «Инновации в тени: как злоумышленники экспериментируют с ИИ» Лаборатория Касперского указала, какими выявленными ею средствами и современными технологиями киберпреступники пользуются для достижения поставленных задач. Из исследования можно отметить, что функционал инструментов, таких как большие языковые модели, усложняется. Как следствие, упрощается выполнение стандартных задач, включая применение Chat GPT[6] и возможностей искусственного интеллекта (ИИ), что способствует их результативной интеграции в массы. Одновременно с этим, в 2023 г. на киберпреступных форумах наблюдались активные обсуждения использования ChatGPT для незаконных, противоправных действий. Некоторые пользователи высказывали идеи о применении этого инструмента для разработки полиморфных вредоносных программ, которые изменяют свою форму, но сохраняют главные функции, что усложняет их выявление. Другие обсуждали варианты использования API[7] OpenAI для создания программного кода с определенными характеристиками, акцентируя внимание на неоднозначности этих технологий[8]. С прогрессом технологий доступ к информации становится проще и многие задачи можно решить всего лишь одним запросом. Однако, распространенность передовых цифровых продуктов среди злоумышленников вызывает тревогу, так как такие тенденции зачастую приводят к увеличению потенциальных угроз.

Кроме того, аналитики Лаборатории Касперского сообщили, что в 2023 г. ежемесячно происходило примерно 476 успешных атак на компании с использованием программ-вымогателей, тогда как в 2022 г. таких случаев было примерно 386[9]. За 2024 г., по результатам изучения специалистами информационной безопасности цифровых угроз в даркнете, обнаружено, что около 85 % фишинговых писем направляются в организации Стран ЕАЭС и СНГ, маскирующихся под официальные, финансовые документы. Основная часть рассылки в 91 % имеет не очень хорошее качество, но она рассчитана на невнимательных получателей[10]. К тому же, большая часть фишинговых рассылок основана на программах, покупаемых мошенниками в даркнете. Цена инструментов разная, но некоторые из них и вовсе предлагаются бесплатно[11].

Последствием успешного применения методов киберпреступности в первую очередь является распространение украденных данных как организаций, так и пользователей. В эту категорию входят взлом аккаунтов, кража личной информации, логинов, паролей, финансовых данных, корпоративных секретов, многое другое, используемых в дальнейшем для перепродажи, получения ценных сведений. Согласно исследованию специалистов компании «Positive Technologies», за первое полугодие 2024 г. Россия заняла лидирующую позицию в рейтинге стран по числу объявлений о продаже полученных баз данных различных организаций в даркнете. Это подтвердил и комплексный сервис для мониторинга внешних цифровых угроз Solar AURA. Если за 2023 г. зарегистрировано 420 случаев утечки актуальной, чувствительной информации, то только за первые три месяца 2024 г. уже

[4] Согласно Перечню понятий, приведенному в приказе Минпромторга России от 23.06.2016 г. № 2091 (ред. от 12.08.2021) «Об утверждении Концепции развития государственной информационной системы промышленности», IoT - Интернет вещей (англ. Internet of Things). Концепция сети передачи данных между физическими объектами ("вещами"), оснащенными встроенными средствами и технологиями для взаимодействия друг с другом или с внешней средой.

[5] DDoS, программы-вымогатели, майнеры / «Лаборатория Касперского» проанализировала ландшафт киберугроз для интернета вещей. URL: https://www.kaspersky.ru/about/press-releases/ddos-programmy-vymogateli-majnery-laboratoriya-kasperskogo-proanalizirovala-landshaft-kiberugroz-dlya-interneta-veshej (дата обращения: 15.10.2024).

[6] ChatGPT – это чат-бот с искусственным интеллектом, который появился в 2022 году и тут же завоевал огромную популярность. Разработчики ChatGPT – компания OpenAI, которую основал Илон Маск. ChatGPT до сих пор обучается, когда обрабатывает запросы пользователей. URL: https://blog.skillfactory.ru/glossary/chatgpt/ (дата обращения: 15.10.2024).

[7] API - программный интерфейс приложения (англ. Application Programming Interface). Описание способов (набор классов, процедур, функций, структур или констант), которыми одна компьютерная программа может взаимодействовать с другой программой (см. также приказ Минпромторга России от 23.06.2016 г. № 2091 (ред. от 12.08.2021) «Об утверждении Концепции развития государственной информационной системы промышленности»).

[8] Инновации в тени: как злоумышленники экспериментируют с ИИ. URL: https://dfi.kaspersky.ru/blog/ai-in-darknet-ru (дата обращения: 15.10.2024).

[9] Даркнет (теневой интернет, DarkNet) (публикация от 25.03.2024). URL:https://www.tadviser.ru/index.php /Статья:Даркнет_(теневой_интернет,_DarkNet) (дата обращения: 18.10.2024).

[10] Улов из даркнета: как защитить банковскую карту и пароли от хакеров // https://iz.ru/: сайт. URL: https://iz.ru/1731641/dmitrii-alekseev/ulov-iz-darkneta-kak-zashchitit-bankovskuiu-kartu-i-paroli-ot-khakerov (дата обращения: 15.10.2024).

[11] Даркнет (теневой интернет, DarkNet) (публикация от 25.03.2024). URL:https://www.tadviser.ru/index.php /Статья:Даркнет_(теневой_интернет,_DarkNet) (дата обращения: 18.10.2024).

произошло 170 таких инцидентов[12]. При этом, одна и та же информация нередко продается повторно или под видом украденной базы данных предлагаются подделки, состыковки информации из разных источников[13].

В темной сети каждый день совершается множество сделок, в которых цифровые преступники выступают в качестве продавцов и покупателей информации, предоставляют нелегальные услуги. Эти операции сопряжены с рисками для всех вовлеченных сторон: клиенты могут не произвести оплату, а продавцы – исчезнуть с полученными средствами, не оставив никаких следов. Однако, несмотря на эти опасности, наблюдается спрос на наем сотрудников в хакерские группировки для совершения противоправных деяний. В отчете Лаборатории Касперского «Как хантят IT-специалистов в даркнете» за 2022 год на основании анализа 155 сайтов темной сети, связанных с продолжительной и постоянной работой, составлен рейтинг востребованности тех или иных специалистов[14] (рис. 1).

В числе самых высокооплачиваемых специалистов, согласно рейтингу, находятся разработчики (программисты), доход которых может достигать 20 тыс. долл. США в месяц. Основными работодателями таких специалистов являются хакерские группировки и APT (Advanced Persistent Threat), которые активно ищут людей, способных заниматься созданием вредоносного программного обеспечения, поддержкой информационных систем, другими подобными задачами[15].

Получается, что темная сеть применяется не только для осуществления нелегальных операций, распространения запрещенных материалов, но и для привлечения новых участников в разнообразные хакерские сообщества, спрос на которые довольно высок. Методы поиска IT-специалистов в даркнете во многом схожи с теми, которые используются в легальных компаниях. Как и в традиционном бизнесе, работодатели стремятся найти квалифицированных специалистов, выбирают наиболее подходящих кандидатов. Анализ опубликованных объявлений показывает, что многие люди готовы заниматься нелегальной или полулегальной деятельностью, несмотря на связанные с этим риски.

Стоит отметить, что в России увеличивается и количество организаций, которые продаются в даркнете[16]. Одни приобретают их с целью ложного партнерства, ведь компания, существующая небольшой промежуток времени и пытающаяся стать контрагентом, привлекает к себе больше внимания, подозрений, чем скрытно приобретенная организация с долгой историей. В других случаях, покупка обоснована отмыванием денег, выводом доходов. Использование биткойнов, криптовалют значительно затрудняет отслеживание транзакций, способствует анонимности преступников. К тому же, санкции, введенные против некоторых российских банков, и остановка работоспособности международных платежных инструментов также оказали влияние на предпринимателей, которые чаще стали обращаться за помощью к посредникам в темной сети[17].

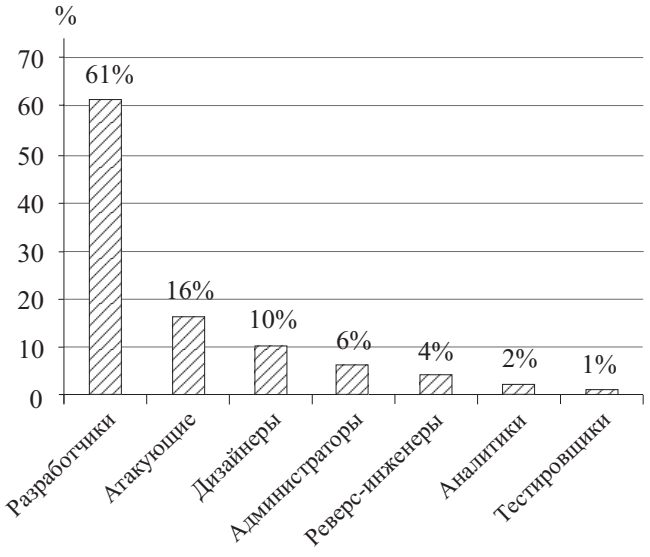

Рис. 1. Рейтинг востребованных специалистов даркнета

[12] Россия стала лидером по количеству слитых в даркнет баз данных. URL: https://cybmir.ru/rossiia-stala-mirovym-liderom-po-kolichestvy-slityh-v-darknet-baz-dannyh/ (дата обращения: 18.10.2024).

[13] Бизнес в Даркнете. Сделки и их регуляция. URL: https://docs.yandex.ru/docs/view?tm=1729171475&tld=ru&lang=ru&name=Biznes-v-darknete-sdelki-i-regulyatsia.pdf.

[14] Как хантят IT-специалистов в даркнете // https://www.kaspersky.ru/: сайт.– URL: https://docs.yandex.ru/ docs/ view?tm=1729172193&tld=ru&lang=ru&name=Kak-hantyat-IT-spetsialistov-v-darknete.pdf.

[15] Там же.

[16] Эксперты выявили рост числа продаваемых в даркнете российских компаний. URL: https://www. rbc.ru/business/22/03/2024/65fce7889a79470adac11cc2 (дата обращения: 20.10.2024).

[17] Международные платежи российского бизнеса ушли в даркнет. Это дорого и опасно, но риск того стоит. URL: https://360.ru/tekst/dengi/ushli-v-darknet/ (дата обращения: 20.10.2024).

Специалисты Группы компаний (ГК) «Солар» в «Отчете об атаках на финансовый сектор в 2023 году», подготовленном по результатам анализа запросов на даркнет-ресурсах, указали, что предложения на нелегальные услуги в финансовой сфере, продолжая занимать значительную долю среди всех исследованных публикаций, составляют 40 %; причем, количество таких запросов остается практически неизменным[18] (рис. 2).

Высокий уровень активности на даркнете *в области финансовых услуг* можно считать индикатором проблем в безопасности. Несмотря на применяемые технологии и способы защиты, в информационных системах финансовых организаций находятся слабые места. О том, что субъекты финансового сектора остаются одними из самых заманчивых мишеней для киберпреступников, войдя в пятерку по числу зарегистрированных инцидентов, в начале 2024 г. объявила российская компания «Positive Technologies», специализирующаяся на разработке решений в сфере информационной безопасности[19] (рис. 3).

Компания «Positive Technologies» отметила также и то, что большая доля цифровых угроз может быть недоступна обществу, а появляться только в темной сети – теневых форумах. Потому специалисты в области информационной безопасности все чаще прибегают к ловким стратегиям маскировки, внедряясь в даркнет под видом обычных пользователей, покупателей, продавцов. Приняв облик «своих», повышают уровень доверия к себе, открывают доступ к более ценным и подробным данным. Именно эта практика, позволяющая исследовать теневые рынки, собирая информацию о том, как функционируют схемы атак, помогает выявлять ключевых игроков, новейшие угрозы. Благодаря чему, специалистам удалось зафиксировать в пять раз больше случаев, в отличие от открыто сообщаемых инцидентов.

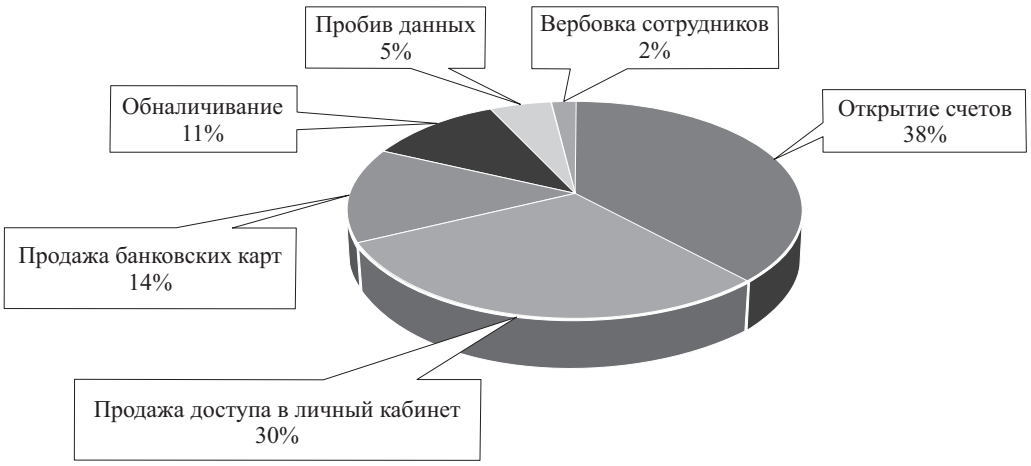

Рис. 2. Распределение нелегальных услуг в финансовой сфере по категориям

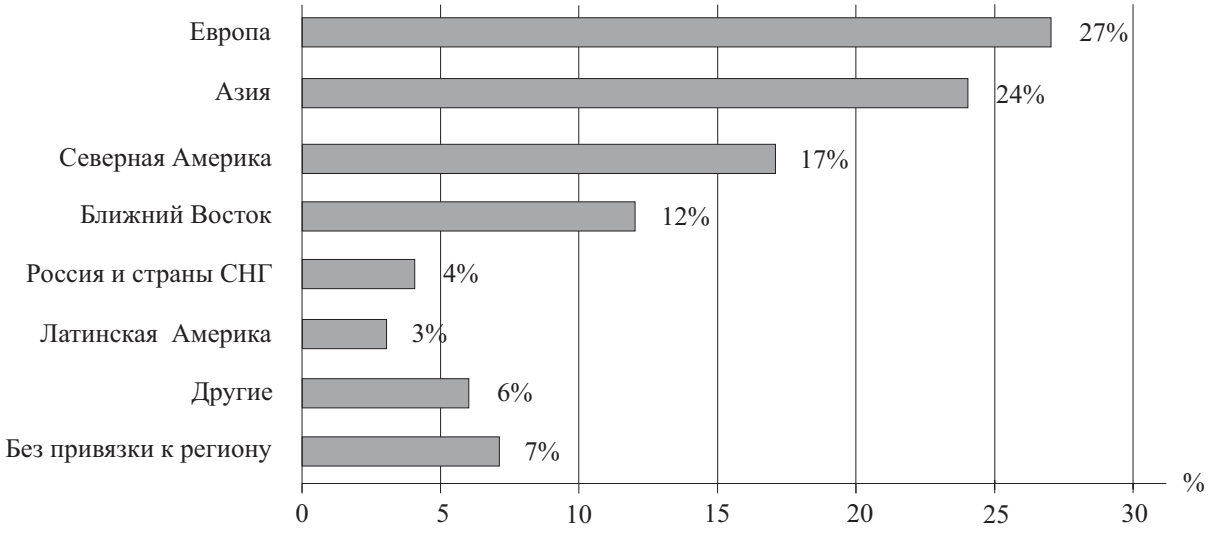

Рис. 3. Распределение сообщений на теневых площадках по географии скомпрометированных организаций

[18] Отчет об атаках на финансовый сектор в 2023 году (с. 20). URL: https://rt-solar.ru/upload/iblock/a63/ 5b5veyxliulzjrd2eq5zo1kizwk6750f/Otchet-finsektor-2023_final.pdf (дата обращения 20.10.2024).

[19] Киберугрозы финансовой отрасли: 2023-2024. URL: https://www.ptsecurity.com/ru-ru/research/analytics /financial-industry-security-h2-2023-h1-2024/ (дата обращения: 21.10.2024).

Множество финансовых организаций активно сотрудничает с государственными структурами и вовлечено в решение значительных экономических, социальных проблем, что делает их специфической целью для мошеннических группировок. Киберугрозы, предназначенные для данных целей, обладают высоким уровнем организации, отличаются целенаправленным подходом к реализации атак, выделяются детальным планированием каждого элемента своих действий. В период с начала 2023 г. (на рис. 4 первая половина года помечена H1 2023, вторая половина года – H2 2023) и до середины 2024 г. (первая половина года помечена H1 2024) можно проследить значительные перемены в применяемых методах компрометации финансовых организаций. Эти изменения отражают адаптацию мошенников к новым технологиям, мерам безопасности, а также меняющиеся правила, регуляции в сфере финансов[20] (рис. 4).

Основной мотивацией киберпреступников является финансовая выгода, которая достигается через кражу данных, вымогательство, мошеннические транзакции. Многие из них стремятся получить доступ к конфиденциальной информации, что позволяет им впоследствии проводить более сложные атаки, а некоторые группы действуют с политическими или идеологическими целями, стараясь подорвать доверие к финансовым институтам, государственным структурам, приводя к нарушению основной деятельности финансовой организации[21] (рис. 5).

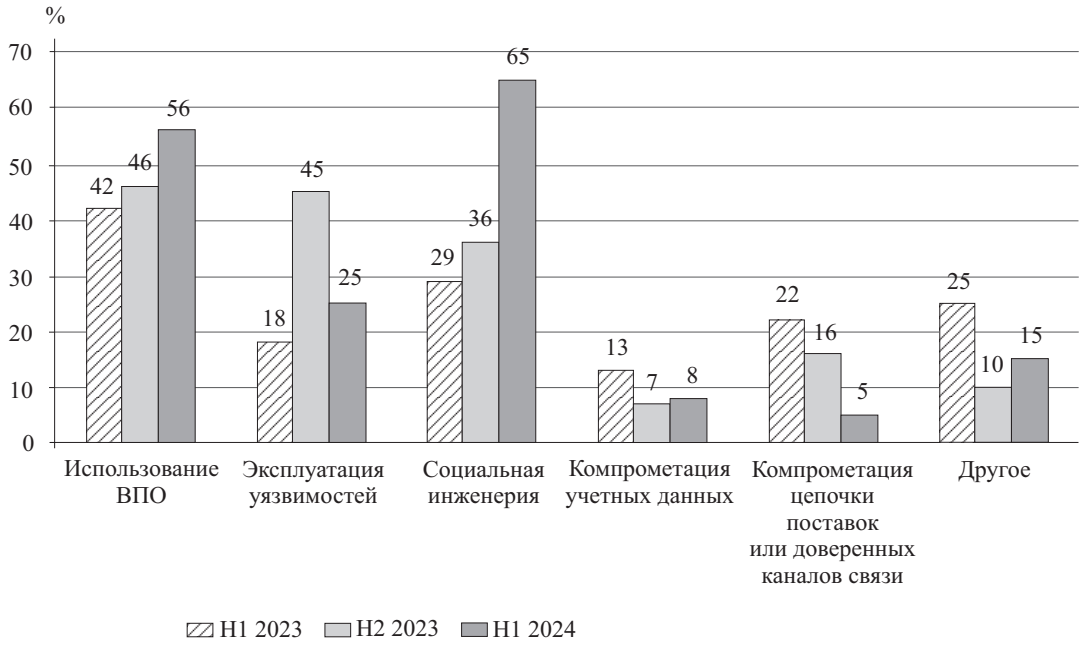

Рис. 4. Методы компрометации информационной инфраструктуры финансовых организаций

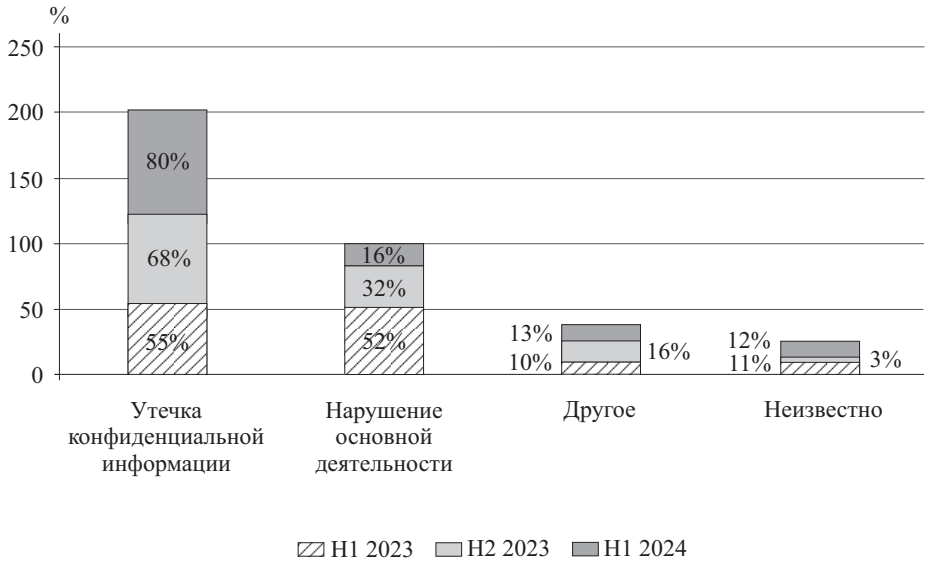

Рис. 5. Динамика последствий успешных кибератак на финансовые организации

[20] Там же.
[21] Там же.

В «Отчете о ключевых внешних цифровых угрозах для российских компаний» за январь-апрель 2023 г., подготовленном ГК «Солар» и представленном в открытом доступе, было обнародовано данных в отношении 123 российских финансовых организаций. Основная часть утечек представлена их базами данных (76 %), а оставшаяся часть – документами, похищенными с серверов[22] (рис. 6).

Сообщения о совершенных похищениях информации появляются каждый день, но не все они являются последствием действительно совершенных атак. Если говорить о малом бизнесе, то примерно 80 % случаев могут считаться действительными и отражают реальные угрозы. Ситуация значительно меняется, когда речь идет о финансовых организациях и крупных компаниях, а также государственных структурах; в отношении их мошенники часто действуют по иным принципам, причем, даже при недостатке реальных результатов желание повысить свой статус среди «коллег», создать напряженную обстановку вокруг конкретного объекта, увеличить ценность информации сподвигают их на мошеннические действия.

Финансовый сектор занимает вторую позицию по величине денежного ущерба, вызванного утечками информации. Ситуация обусловлена тем, что финансовым организациям необходимо тратить крупные суммы на обеспечение, поддержание безопасности данных, расследование, отслеживание потенциальных кибератак. В результате успешно совершенного инцидента, организации могут подвергаться штрафам, судебным искам за недостаточную защиту, что, в свою очередь, приводит к длительному процессу восстановления информации, снижению прибыльности, нанесению ущерба репутации в виде потери доверия клиентов и партнеров. Стоит отметить, что финансовые организации являются одними из тех, у кого цифровые преступники запрашивают наивысшие суммы выкупов за неразглашение полученных сведений: в 58 % случаев они превышают 1 млн долл. США, а в 38 % – составляют более пяти млн долл. США[23].

Через финансовые организации проходят значительные потоки капитала, что делает их привлекательной целью для киберпреступников, стремящихся к незаконному завладению денежными средствами, хранящимися как на счетах самих организаций, так и на счетах клиентов. Согласно данным Банка России, по итогам второго квартала 2024 г. в Российской Федерации с банковских счетов клиентов и организаций было похищено примерно 4,8 миллиарда рублей, что превышает средний уровень за четыре предыдущих квартала[24]. С 25 июля 2024 г. финансовые организации должны замедлять переводы на два дня, если сведения о получателе находятся в базе данных Банка России о мошенничестве. Если этого не сделать, банк будет должен вернуть клиенту средства в течение 30 календарных дней[25]. Эти новые требования могут повлечь определенные недовольства и сложности.

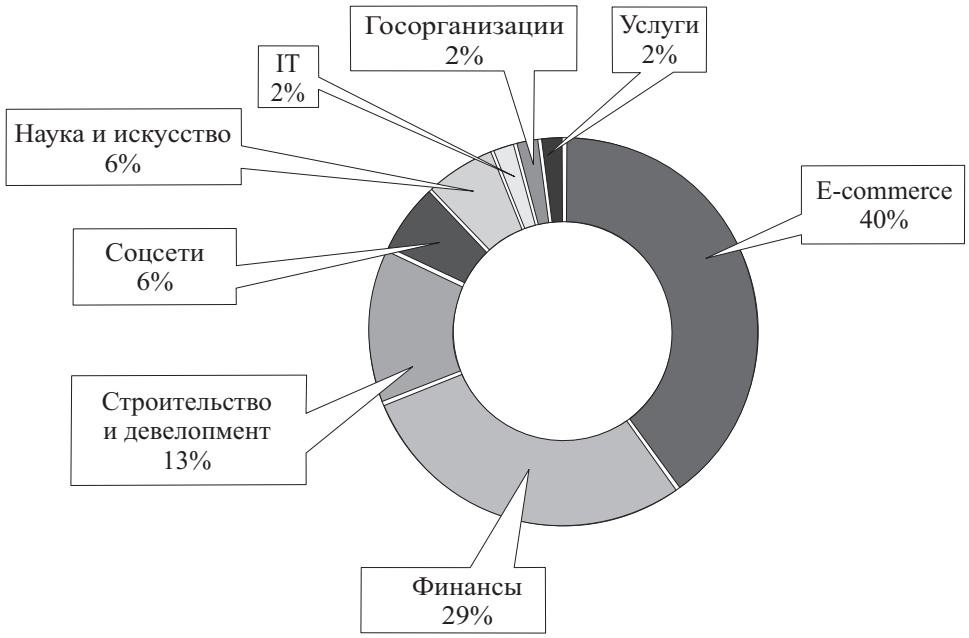

Рис. 6. Распределение утечек по отраслям

[22] Отчет о ключевых внешних цифровых угрозах для российских компаний (январь-апрель 2023) (с. 10). URL: https://rt-solar.ru/upload/iblock/93a/bx4m3tr2s79ubeoeanop5vuu6clm1zi7/Otchet_o_klyuchevykh_vneshnikh_ts ifrovy kh_ugrozakh_dlya_rossiyskikh_kompaniy.pdf.

[23] Киберугрозы финансовой отрасли: 2023-2024. URL: https://www.ptsecurity.com/ru-ru/research/analytics /financial-industry-security-h2-2023-h1-2024/ (дата обращения: 21.10.2024).

[24] Мошенники установили рекорд по похищению у россиян денег с банковских счетов. URL: https://www.cnews.ru/news/top/2024-08-22_moshenniki_pohitili_pochti (дата обращения: 21.10.2024).

[25] Граждан защитят по-новому от мошеннических переводов. URL: https://cbr.ru/press/event/?id=18865 (дата обращения: 22.10.2024).

Учитывая, что мошенники не перестают применять современных передовых достижений, включая технологии искусственного интеллекта – это значительно влияет на появление новых вызовов в области безопасности. Например, по предоставленной информации Сбербанком, с начала 2024 г. увеличился рост числа дипфейков[26] в 30 раз, который говорит о новом тренде в киберпреступности, ставит под удар не только финансовую безопасность в виде убытков, которые могут составить 300 миллиардов рублей за год, но и подрывает доверие к системам и онлайн-платформам[27].

Степень зрелости процессов обеспечения безопасности прямо пропорционально оказывает влияние на своевременное выявление цифровых угроз и минимизацию их последствий. Несмотря на то, что абсолютная защита от всевозможных атак недостижима, правильные, результативные методики способны повысить уровень киберзащиты, помочь снизить потери, даже при осуществлении вторжения преступника.

На сегодняшний день любой значительный инцидент становится известным и негативно сказывается на благополучии той или иной организации в дальнейшем, не говоря уже о тех, которые относятся к финансовым организациям и государственным структурам. Несмотря на то, что организации, деятельность которых связана с предоставлением денежных, инвестиционные услуг, одними из первых обратили внимание на обеспечение безопасности, финансовый сектор остается недофинансированным по сравнению со средними мировыми стандартами. Согласно выводам, к которым пришли специалисты ГК «Солар», в России доля расходов на осуществление информационной безопасности «в ИТ-бюджетах финансовых организаций составляет лишь – 5 %, в то время как в мире она достигает 8-10 %. По оценке аналитиков, к 2030 г. затраты финансовых организаций на обеспечение информационной безопасности (ИБ) могут составить 30 млрд рублей при среднегодовом темпе роста (CAGR) в 8 %, что соответствует росту рынка ИБ в целом»[28].

Существует множество факторов, влияющих на финансовую составляющую, и их негативное воздействие на экономику страны может быть весьма серьезным. К ним относятся: уровень ключевой ставки Банка России по кредиту, колебания курсов валют, инфляция, уровень безработицы, изменение потребительского спроса, другое. Каждый из аспектов способен привести к снижению уровня инвестиций, уменьшению покупательной способности населения и, как следствие, к замедлению экономического роста. Важно учитывать взаимосвязь, своевременно отвечать на возможные угрозы, идти в ногу со временем, чтобы обеспечить устойчивое экономическое развитие.

В завершение еще раз подчеркнем, что даркнет представляет собой двойственный феномен, в котором анонимность играет ключевую роль. С одной стороны, она является инструментом защиты прав человека и личной свободы, с другой – угрозой общественной безопасности. Ведь пользователи, попадая в темную сеть, действуют без боязни привлечения за содеянное, злоупотребляют возможностями. Регулирование этой среды, становится сложной задачей для государств и их центральных банков, правоохранительных органов, международных организаций из-за непрерывного совершенствования технологии цифровых преступников, транснациональных аспектов, отсутствия возможности идентифицировать пользователей. К тому же, различия в нормах законодательства и подходах к обеспечению кибербезопасности в разных странах усложняют сотрудничество в борьбе с данным явлением.

С момента своего возникновения даркнет значительно изменил общественное понимание приватности в интернете, заставляя людей задумываться о том, насколько важно защищать свои данные, права в условиях цифрового мира. Данная тема еще долгое время будет оставаться значимой, поскольку распространенная киберпреступность в даркнете оказывает негативное влияние на многие сферы жизни, в первую очередь, экономическую, от которой на прямую зависит уровень жизни и благосостояние нации.

Литература

1. *Васильев А. А., Ибрагимов Ж. И., Васильева О. В.* Даркнет как ускользающая сфера правового регулирования // Юрислингвистика. 2019. № 12 (23). С. 10–12.

2. *Дворянкин О. А.* Даркнет – темная сторона интернета или неужели все так плохо? // Национальная ассоциация ученых. 2021. № 71-1. С. 14–20.

3. *Свищёв А. В., Лаухина А. С.* Darknet: полезный инструмент или источник угрозы // Colloquium-journal. 2020. № 10-2 (62). С. 66-69.

4. *Жмуров Д. В.* Даркнет как ускользающая сфера правового регулирования // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. № 1 (27). С. 89-98.

[26] Слово «дипфейк» «происходит от соединения двух английских слов: deep learning – «глубинное обучение», и fake – «подделка». Если говорить коротко, то это изображение, где лицо человека не настоящее, а создано или изменено искусственным интеллектом». URL: https://blog.eldorado.ru/publications/chto-takoe-deepfake-10-luchshikh-prilozheniy-dlya-sozdaniya-dipfeykov-35408 (дата обращения: 22.10.2024).

[27] Сбербанк подтвердил, что сначала этого года количество дипфейков в Сети выросло в 30 раз. URL: https://overclockers.ru/blog/Fn_portfolio/show/178714/Sberbank-podtverdil-chto-s-nachala-etogo-goda-kolichestvo-dipfejkov-v-Seti-vzletelo-v-30-raz (дата обращения: 22.10.2024).

[28] Отчет об атаках на финансовый сектор в 2023 году (с. 22). URL: https://rt-solar.ru/upload/iblock/a63/ 5b5veyxliulzjrd2eq5zo1kizwk6750f/Otchet-finsektor-2023_final.pdf (дата обращения 20.10.2024).

Сведения об авторах

Следнева Кристина Евгеньевна – студент Омского государственного университета путей сообщения (ОмГУПС), Омск, Россия.
Email: ksledneva2003@gmail.com

Кувалдина Татьяна Борисовна – доктор экономических наук, профессор кафедры «Экономическая безопасность и управление финансами», Омский государственный университет путей сообщения (ОмГУПС), Омск, Россия.
Email: kuvaldina2004@mail.ru

ANONYMITY ON THE DARKNET: THE KEY TO THE SECURITY OF FINANCIAL INSTITUTIONS OR A THREAT TO SOCIETY

K. Sledneva, T. Kuvaldina
Omsk State Transport University (OSTU),
Omsk, Russia

With the progressive development of digital technologies, online security and anonymity are becoming important conditions in the virtual world, which is reflected in the darknet phenomenon. Cybercrime, being the main threat on the darknet, covers a wide range of illegal activities, including the distribution of stolen data. The motives of digital criminals vary, ranging from monetary gain to undermining trust in financial organizations and government agencies. Russia takes the leading position in ads for the sale of stolen databases, and the frequency of information leaks is only increasing. It is noted that the dark web is becoming not only a platform for illegal actions, but also a place to attract new specialists to hacker groups. Financial organisations are of great interest to them, as it is through them that large money flows. This fact creates favourable conditions for receiving significant ransoms for stolen information, and also makes the financial sector the second largest leader in losses from data breaches. Despite growing attention to the security of the domestic financial industry, it remains underfunded compared to global standards. The darknet is a complex phenomenon where anonymity can serve as both a defence of human rights and a threat to public safety. Users act without fear of being caught, punished, which leads to abuse. Regulation of the darknet is a serious task for the authorities and international organisations due to the constant improvement of digital criminals' technologies and significant differences in legislation. The article considers the essence of the darknet, its pros and cons, and concludes that anonymity in the darknet plays a key role. On the one hand, it is a tool to protect human rights and personal freedom, on the other hand, it is a threat to public safety. Therefore, the issues of privacy and cybercrime on the darknet will remain relevant for a long time due to the directly proportional relationship between the economic stability of countries and the living standards of their citizens.

Keywords: darknet, security, economic losses, data protection, social implications, anonymous networks.

References

1. Vasiliev A. A., Ibragimov Zh. I., Vasilyeva O. V. Darknet as an elusive sphere of legal regulation, *Yurislingvistika*, 2019, No. 12 (23), pp. 10-12.

2. Dvoryankin O. A. Darknet – the dark side of the Internet or is it really that bad?, *Nacional'naja associacija uchenyh*, 2021, No. 71-1, pp. 14-20.

3. Svishchev A.V., Laukhina A. S. Darknet: a useful tool or a source of threat, *Colloquium-journal*, 2020, No. 10-2 (62), pp. 66-69.

4. Zhmurov D. V. Darknet as an elusive sphere of legal regulation, *Sibirskie ugolovno-processual'nye i kriminalisticheskie chtenija*, 2020, No. 1 (27), pp. 89-98.

About the authors

Kristina E. Sledneva – student of the Department of Information Security, Omsk State University of Railway Engineering (OmGUPS), Omsk, Russia.
Email: ksledneva2003@gmail.ru

Tatyana B. Kuvaldina – Professor of the Department of Economic Security and Financial Management, Omsk State University of Railway Engineering (OmGUPS) Omsk, Russia.
Email: kuvaldina2004@mail.ru