ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/2226-7867-2024-14-5-20-29
УДК 004.056:327(6)(045)

Эволюция экосистемы даркнета и вызовы международной информационной безопасности в Африке

А.И. Ильинский
Финансовый университет, Москва, Россия

АННОТАЦИЯ

В статье рассматривается эволюция экосистемы даркнета и ее влияние на международную информационную безопасность в Африке. Анализируются ключевые угрозы, исходящие из даркнета, включая нелегальную торговлю, киберпреступность и распространение дезинформации. Выделяются специфические вызовы, с которыми сталкиваются африканские страны в области кибербезопасности, такие как недостаток ресурсов и низкий уровень осведомленности. Также обсуждаются возможные стратегии повышения устойчивости и эффективности борьбы с киберугрозами в регионе, включая международное сотрудничество и развитие российско-африканских инициатив в области информационной безопасности.

***Ключевые слова*:** Даркнет; кибербезопасность; киберпреступность; Африка; нелегальная торговля; дезинформация; эволюция; международное сотрудничество; информационная безопасность; российско-африканское партнерство; устойчивость

Для цитирования: **Ильинский А.И. Эволюция экосистемы даркнета и вызовы международной информационной безопасности в Африке. *Гуманитарные науки. Вестник Финансового университета.* 2024;14(5):20-29. DOI: 10.26794/2226-7867-2024-14-5-20-29**

ORIGINALPAPER

Evolution of the Darknet Ecosystem and Challenges of International Information Security in Africa

A.I. Ilyinsky
Financial University, Moscow, Russia

ABSTRACT

The article examines the evolution of the darknet ecosystem and its impact on international information security in Africa. It analyzes key threats emanating from the darknet, including illegal trade, cybercrime, and the spread of disinformation. Specific challenges faced by African countries in the realm of cybersecurity are highlighted, such as lack of resources and low levels of awareness. Possible strategies for enhancing resilience and effectiveness in combating cyber threats in the region are also discussed, including international cooperation and the development of Russian-African initiatives in information security area.

Keywords: darknet; cybersecurity; cybercrime; Africa; illegal trade; disinformation; evolution; international cooperation; international information security; Russian-African partnership; resilience

***For citation*: Ilyinsky A.I. Evolution of the darknet ecosystem and challenges of international information security in Africa. *Humanities and Social Sciences. Bulletin of the Financial University*. 2024;14(5):20-29. DOI: 10.26794/2226-7867-2024-14-5-20-29**

© Ильинский А.И., 2024

ВВЕДЕНИЕ

Международная информационная безопасность (МИБ) — это системная социотехническая концепция устойчивой защиты информации и информационных систем на мировом уровне от кибератак. Она включает в себя меры по предотвращению, выявлению и реагированию на киберугрозы и инциденты. Для достижения целей МИБ и построения безопасной и надежной среды обмена информацией в Африке предполагается глубокое партнерство между государствами, международными организациями и частным бизнесом. Основным источником киберугроз для глобальных информационных систем является система даркнета. Экосистема даркнета — это совокупность взаимосвязанных элементов и структур, образующих анонимную, децентрализованную и закрытую часть всемирной паутины, которая служит средой для незаконной и нелегальной деятельности [1]. Даркнет сегодня представляет собой сложную, динамично развивающуюся, но изолированную от публичной всемирной паутины систему, которая создает значительные вызовы для обеспечения международной информационной безопасности, особенно в таких быстро развивающихся, но уязвимых регионах, как Африка.

ТЕХНОЛОГИЧЕСКАЯ ЭВОЛЮЦИЯ ТЕМНОЙ СЕТИ

Интернет представляет глобальную сетевую инфраструктуру, объединяющую совокупность всех устройств, которые могут обмениваться данными с помощью протоколов типа TCP/IP. Всемирная паутина представляет социотехническую систему множества веб-сайтов, социальных сетей и баз данных, имеющих доступ к инфраструктуре интернета с помощью протоколов обмена гипертекстами. Для работы с колоссальным объемом информации, представленной во всемирной паутине и поиском необходимых для пользователя данных, были созданы специализированные инструменты — браузеры и поисковые роботы, которые автоматически индексируют веб-сайты. Стандартные браузеры, такие как Google Chrome, Safari, Yandex и Baidu, позволяют просматривать открытые для широкой публики сайты и анализировать их содержимое по запросу клиента. Однако далеко не все информационные ресурсы всемирной паутины могут быть обработаны и однозначно индексированы с помощью стандартных браузеров.

Развитие технологии динамического контента или технологии динамических сайтов, использующих файлы cookie, делают сам процесс индексирования неоднозначным и зависящим от предпочтений, местонахождения, времени обращения и другой априорной информации о клиенте. Поэтому одинаковые запросы двух различных клиентов могут давать два различных ответа. Технология динамических сайтов с использованием множества шаблонов, контента и скриптов позволяет более точно удовлетворить запрос конкретного клиента с учетом априорной информации, ранее собранной о клиенте с помощью файлов cookie. Таким образом, технология динамического контента делает сам процесс индексирования сайтов более субъективным, и при каждом новом посещении клиентом/поисковым роботом динамически генерируется обновленное содержание. Значительная часть информационных ресурсов всемирной паутины защищена паролями, специальными программными средствами или требует оплаты доступа, что делает их недоступными для индексирования стандартными браузерами. Это позволяет разделить всемирную паутину на два неравных слоя. Сравнительно небольшой слой всемирной паутины объемом около 20 терабайт, открытый для широкой публики и индексируемый поисковыми системами, получил название видимая сеть (Surfacenet или Clearnet). Видимая сеть построена так, что ее контент должен быть легко обнаружен с помощью стандартных браузеров, и эта сеть сегодня является важнейшим инструментом политического, культурного и экономического маркетинга.

Огромный объем информации всемирной паутины, скрытый от широкой публики и недоступный для индексирования стандартными браузерами, образует глубокую сеть (deep web). Глубокая сеть включает личную информацию на почтовых серверах, цифровые данные на защищенных корпоративных интрасетях и записи в государственных хранилищах данных. В глубокую сеть попадают также колоссальные информационные потоки в реальном времени, которые собираются, обрабатываются и хранятся в системах интернета вещей, умных городов и т.д. Объем информации в глубокой сети составляет сегодня около 7500 терабайт, при этом 95% этой информации доступны широкой публике, но защищены паролями. Собственники информа-

ции, хранящейся в глубокой сети, тщательно ее защищают. Так феномен WikiLeaks был связан с обеспечением свободного публичного доступа к небольшой части материалов Министерства обороны США, которые всегда находились в глубокой сети, но были надежно защищены сложной системой защиты информации [2]. Анонимность пользователей как в видимой сети, так и в глубокой сети является относительной, потому что в каждом сетевом сообщении протокола TCP/IP указаны IP-адреса отправителя и получателя, которые однозначно определяют местонахождение компьютера или сервера. Для обеспечения анонимности клиентов и секретности сообщений при использовании интернет-коммуникаций было предложено несколько технологий, которые обеспечивают решение этой задачи.

Скрытая, анонимная и децентрализованная часть глубокой сети получила название даркнет (darknet). Эта узкоспециализированная сеть зародилась в 1990-х гг. с развитием технологий анонимности, таких как TOR (The Onion Router) и I2P (Invisible Internet Project), и сегодня эта секретная сеть приобретает все большую значимость в глобальном масштабе. По оценкам трафик в даркнете составляет от 5 до 10% общего трафика всемирной паутины.

Происхождение и развитие даркнета как анонимной онлайн-среды было положено исследованиями Министерства обороны США в середине 1990-х гг., которое поставило задачу обеспечения высокой анонимности и секретности передачи скрытых сообщений через публичную инфраструктуру интернета с использованием технологий всемирной паутины. Эта задача была успешно решена в Исследовательской лаборатории ВМС США, где криптограф Пол Сайверсон разработал технологию «луковой» маршрутизации [3]. Изначально проект TOR разрабатывался ВМС США для защиты правительственных коммуникаций. Однако впоследствии он был открыт для общественного пользования, послужил технологическим фундаментом современного даркнета и сегодня продолжает активно развиваться в форме некоммерческой организации TOR Project. Разработанная технология TOR представляет систему так называемой «луковой» маршрутизации, которая обеспечивает анонимность и конфиденциальность интернет-соединения пользователей путем многослойного шифрования трафика, использования случайно распределенной сети узлов, отделения секретных «луковых» адресов от IP-адресов отправителя и получателя. Информация проходит через несколько промежуточных «луковых» узлов-маршрутизаторов, каждый из которых расшифровывает только один слой, что скрывает источник и назначение данных. Трафик проходит через случайно выбранные волонтерские узлы TOR, распределенные по всему миру, что затрудняет отслеживание и перехват сообщения. TOR использует псевдонимные «луковые» адреса, не связанные с реальной идентификацией пользователя, а IP-адреса отправителя и получателя недоступны публично. Другими словами, с помощью технологии TOR формируется даркнет в виде системы стохастических динамических виртуальных каналов внутри существующей инфраструктуры интернета. Таким образом, «луковая» маршрутизация TOR позволяет пользователям даркнета относительно безопасно и анонимно просматривать веб-сайты, обмениваться сообщениями и совершать другие интернет-действия, избегая цензуры и слежки. Эти возможности широко используются как для законных, так и для незаконных целей в рамках экосистемы даркнета. Однако, по оценкам CloudFlare, около 95% трафика в даркнете имеют высокую вероятность связи с киберугрозами [4]. Для работы в даркнете в среде TOR большую популярность среди его обитателей получил TOR Browser, построенный на платформе Mozilla Firefox, который обеспечивает прямое подключение к сети, что дает возможность работы как в видимой сети с использованием стандартного IP-адреса, так и в даркнете с использование сгенерированного программой уникального «лукового» адреса длиной 56 символов и расширением «.onion». Использование сложного математического алгоритма многослойного шифрования в «луковой» маршрутизации делает процесс работы в даркнете значительно более медленным, что часто приводит к техническим сбоям, особенно при обмене файлами больших размеров.

ЭВОЛЮЦИЯ СООБЩЕСТВА ДАРКНЕТА

Обитатели даркнета формируют сложную сетевую социальную структуру с определенной системой ценностей и развитой субкультурой. Сегодня всех обитателей даркнета принято обобщенно называть хакерами, а сам образ хакера в массовой культуре убедительно рисует нам цифрового фанатика-психопата, который скло-

нен к преступной деятельности и стремится разрушить существующий мировой порядок. Однако первоначально смысл англоязычного существительного hack был определен в начале 1960-х в Лаборатории искусственного интеллекта Массачусетского технологического института и соответствовал «невероятно хорошей и, возможно, очень трудоемкой работе, которая производит именно то, что нужно»[1]. Авторитетный The Hacker's Dictionary определяет хакера как профессионала в области цифровых технологий, «который с энтузиазмом (даже одержимо) программирует или кому нравится программирование, а не просто теоретизировать о программировании»[2]. Именно на базе крупнейших университетских исследовательских центров в технологической среде ранних компьютерных и телекоммуникационных систем было сформировано первое поколение хакеров-первопроходцев, которые были увлечены изучением технологий, часто ради интеллектуального вызова, а не ради нанесения вреда и получения криминальной выгоды. Они ставили задачу глубокого проникновения в функционирование компьютерных систем и сетей и понимание того, как работает система и что позволяет изменять ее использование и преобразовывать ее способами, которые изначально считались невозможными. Хакерское мышление ищет нестандартные методы достижения стандартных целей, широко использует методы обратного реинжиниринга для нахождения существующих лазеек и уязвимостей в системе, использование которых позволяет совершенно изменить функционирование всей системы. Философия хакера выходит далеко за рамки простого знания конструирования программных кодов: она связана с проектированием, деконструкцией и перепроектированием будущих сценариев эволюции цифровых систем. Эрик С. Рэймонд описал архетип хакера, который известен в фольклоре под именем J. Random Hacker как любопытного, интровертного и умного антиконформиста с высоким показателем синдрома дефицита внимания, у которого проблемы с эмоциями и который ненавидит смурфов, эвоков, Microsoft, COBOL и BASIC[3]. Другими словами, J. Random Hacker являлся цифровым двойником архетипа хиппи, хакеры-первопроходцы представляли программистов самой высокой квалификации, которые были мотивированы показать свое выдающееся мастерство программирования и остроумие. Однако уже в 1990-х гг. сформировалось второе поколение хакеров, которые использовали растущие возможности интернета для взлома систем, нанесения ущерба и получения финансовой выгоды. Мотивированным желанием второго поколения хакеров было стремление продемонстрировать свои технические навыки, самоутвердиться и заработать. Хакеры, которые в одиночку взламывали информационные системы с финансовыми целями, получили название черных хакеров. Для противодействия черным хакерам в 2000-х гг. Microsoft начал платить хакерам первого поколения за поиск уязвимостей и возможности проникновения в систему Windows. Этот так называемый этичный взлом находил существующие уязвимости и исправлял их в интересах корпорации, прежде чем ими могли воспользоваться черные хакеры. Хакеры, участвующие в этичном взломе, получили название белых хакеров. Значительная доля хакеров даркнета зарабатывала тем, что меняла в зависимости от ситуации свою роль от черных к белым и наоборот. Такие обитатели даркнета получили название серых хакеров. Исследования показывают, что психология современного хакера обыкновенно включает три личностные черты: нарциссизм, макиавеллизм и психопатию, которые формируют темную триаду личности. В исследовании Гайа и др. [5] было показано, что все типы хакеров набирают высокие баллы по шкалам макиавеллианства и психопатии, при этом белые хакеры являются нарциссами, серые противостоят власти, а черные набирают высокие баллы по показателю поиска острых ощущений. Вероятность быть задержанным правоохранительными органами оказывает сдерживающее влияние на поведение серых и черных хакеров.

Некоторые исследования по кибербезопасности предполагают, что существует более миллиона человек, которые считают себя хакерами в различных сферах, включая любителей и участников подпольных сообществ. По статистике TOR Project ежедневно в даркнет в 2023 г. входило около 2,5 млн пользователей и регистрировалось порядка 4000 атак за день, исходящих из

[1] URl: http://www.catb.org/jargon/html/meaning-of-hack.html
[2] URL: https://hackersdictionary.com/html/index.html
[3] http://www.catb.org/jargon/html/appendixb.html

темной сети[4]. Точное число хакеров в даркнете неизвестно, а состав популяции темной сети очень подвижен, каждый активный участник даркнета может легко изменять свое поведение и исполнять роль как нападающего, так и защитника, однако сегодня численность только белых хакеров, сертифицированных в рамках программы Certified Ethical Hacker (CEH)[5], более 230 000. Оценки показывают, что в даркнете могут быть десятки тысяч опытных темных хакеров, объединенных в подвижные преступные группировки и работающих на разных уровнях цифровой сложности.

Бурное развитие асимметричного шифрования с открытым ключом, появление браузера TOR в 2008 г. и развертывание экосистемы биткоина в 2009 г. привело к созданию анонимного, децентрализованного и закрытого даркнета и возникновению третьего поколения хакеров, которые активно участвовали в формировании организованной трансграничной киберпреступности с целью получения финансовой выгоды через кражу данных, вымогательство, мошенничество. Оказалось, что эффект специализации и разделения труда в организованной киберпреступности является ключевым фактором, который позволил преступным группировкам повысить эффективность и масштаб своей деятельности. До наступления эпохи организованной киберпреступности хакеры-одиночки второго поколения выполняли весь спектр преступных действий. Но по мере развития даркнета и роста популяции хакеров стали формироваться более структурированные устойчивые группировки, где каждый участник специализировался на определенной части криминального процесса. Например, существовали группы, занимающиеся только взломом и получением доступа к системам и данным, с которыми работали уже другие группы хакеров, специализирующиеся на краже и монетизации украденных данных. В завершении ответственность за отмывание денег и вывод денежных средств лежала на третьих группах. Такая специализация позволила повысить эффективность каждого этапа, а также масштабировать всю преступную деятельность. Участники могли сосредоточиться на своих узких функциях и развить свои преступные навыки, обмениваясь информацией и координируя усилия в рамках единой структуры. Это стало важным фактором, который способствовал превращению изначально относительно простой и разрозненной киберпреступности в сложные, корпоративно организованные структуры в даркнете. Однако развитие структур организованной киберпреступности требовало дальнейшего развития инфраструктуры даркнета, что привело к формированию торговых площадок, форумов и платформ для планирования и координации. Для сокрытия цифровых следов и проведения анонимных безналичных транзакций стали широко использоваться криптовалюты Bitcoin, Monero, Zcash и др. Особое внимание стало уделяться формированию между участниками кибергруппировок надежных зашифрованных каналов связи, таких как PGP, Signal, Wickr и др. Традиционная организованная преступность для повышения своей доходности и снижения рисков стала устанавливать связи и интегрироваться с сетевыми преступными структурами, что привело к созданию гибридных преступных структур, сочетающих онлайн- и оффлайн-методы. По мере развития и роста преступных групп в даркнете, они начали принимать все более структурированные и жесткие иерархические формы, напоминающие современные легальные корпорации с четким разделением ролей и обязанностей между участниками группировки. В современных группах сетевой преступности организовано планирование, бюджетирование, инвестиции в развитие и расширение проектов, продуктов и услуг, существует система подотчетности и контроля, подобная корпоративному легальному бизнесу. Этот процесс «корпоратизации» киберпреступности значительно повысил ее эффективность, устойчивость и масштаб. Преступные группировки стали действовать как слаженные и профессиональные организации, используя весь арсенал современных бизнес-практик. Это крайне усложняет противодействие со стороны правоохранительных органов, требуя применения комплексных и системных мер.

Если первые два поколения хакеров основной упор в своей деятельности делали на использование передовых цифровых технологий, то третье поколение стало в своей деятельности широко использовать социальную инженерию и продвинутые методы психологического ма-

[4] URL: https://metrics.torproject.org/userstats-relay-country.html

[5] URL: https://www.eccouncil.org/ec-council-in-news/ec-council-unveils-the-certified-ethical-hacker-hall-of-fame-2021

нипулирования, направленные на психологические уязвимости человека. Кроме того, жесткие требования к персональным цифровым компетенциям хакеров начали постепенно снижаться из-за широкого распространения инструментов взлома в даркнете и появления платформ аренды инструментов кибератак как сервиса, что существенно снизило входные технологические барьеры доступа в ряды хакеров и открыло доступ широким массам к преступной деятельности. Появился новый тип низкоквалифицированных хакеров, неспособных самостоятельно написать вредоносный эксплойт, но которые используют уже готовые вредоносные скрипты и программы для нанесения вреда компьютерным системам. Они получили название скрипт-киддис (буквально «малыши со скриптами») и обычно их целью являются попытки произвести своим вандализмом впечатление на свое сообщество начинающих хакеров. Парадоксальность развития противоправной деятельности в темной сети состоит в том, что квалификация и знания подавляющего большинства хакеров постоянно снижаются, но при этом сложность кибератак устойчиво растет [6].

Киберпреступность сегодня — это корпоративно организованный и сложный бизнес со структурированным персоналом, которым управляют профессионалы. Банды вымогателей имеют менеджеров различных уровней, разработчиков вредоносных программ, майнеров данных и других; отдельные лица и команды работают анонимно, координированно и организованно в темных сетях. Доходность киберпреступного бизнеса сопоставима с доходностью бизнеса 1990-х гг. колумбийских наркокартелей. Средний доход, приносимый атакой программой-вымогателем, составляет около 140 000 долл. при операционных расходах 2500 долл., что дает 98% маржи прибыли, но при этом вероятности задержания хакера при атаке вымогателем в 625 раз ниже, чем в случае колумбийского наркобизнеса[6]. Сегодня в условиях глобальной цифровизации процесс хакинга можно рассматривать как акт нахождения уязвимостей компьютерных систем и сетей и затем их использования для получения или защиты от несанкционированного доступа к персональным и корпоративным данным и/или внесения изменений в работу самих систем и сетей в финансовых и/или политических целях.

Резкое обострение геополитических отношений в последнее десятилетие и транснациональный характер темной сети привели к формированию четвертого поколения хакеров, которое обслуживает уже не только корпоративную киберпреступность, но часто работают на иностранные государства или спецслужбы в политических и идеологических целях в условиях глобального кибершпионажа и кибервойны под чужим флагом.

МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В АФРИКЕ

Африка активно движется к цифровой экономике. В период с 2019 по 2022 г. более 160 миллионов африканцев получили широкополосный доступ в интернет. Число интернет-пользователей в странах Африки к югу от Сахары увеличилось на 115 процентов в период с 2016 по 2021 г.[7] Сегодня половина всех зарегистрированных и активных счетов мобильных денег в мире находится в Африке. На их долю приходится около 30 миллиардов транзакций на сумму 500 млрд долл. На страны Африки к югу от Сахары приходится 64% всех мировых мобильных денег[8]. Африка наиболее «перспективна» с точки зрения глобального преступного сообщества. Только в Кении за последний год было зафиксировано 860 миллионов инцидентов[9]. Во втором квартале 2024 г. в Африке наблюдалось самое большое среднее количество еженедельных кибератак на организацию — в среднем 2960 атак, что на 37% больше, чем за аналогичный период 2023 г.[10] Для сравнения отметим, что средний мировой показатель составил 1636 атак на организацию в неделю. Только в 39 африканских странах действует законодательство о кибербезопасности, а в 15 странах континента правовое регулирование цифровой безопасности отсутствует, что делает борьбу с киберпреступлениями в Африке

[6] URL: https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts#vectors

[7] URL: https://www.worldbank.org/en/results/2024/01/18/digital-transformation-drives-development-in-afe-afw-africa

[8] URL: https://www.itweb.co.za/article/what-the-future-holds-for-fintech-in-africa/wbrpOMg2WXg7DLZn

[9] URL: https://www.africanews.com/2023/10/03/kenya-hit-by-record-860m-cyber-attacks-in-a-year//

[10] URL: https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/

неэффективной и затрудняет обеспечение информационной безопасности в регионе.

Важную роль в защите цифровых данных в Африке сегодня играет Конвенция Малабо[11], известная также как Конвенция Африканского союза о кибербезопасности и защите персональных данных. В настоящее время 15 африканских стран, включая Бенин, Камерун, Чад, Коморские Острова, Джибути, Гамбию, Гвинею-Бисау, Южную Африку, Сьерра-Леоне, Сан-Томе и Принсипи, Судан и Тунис, ратифицировали Конвенцию Малабо. Африканский союз подчеркивает важность сохранения открытого, безопасного, стабильного, доступного и мирного киберпространства, что является важным элементом содействия экономическому росту, привлечения инвестиционных возможностей и содействия устойчивому развитию, особенно в развивающихся и наименее развитых государствах.

Согласно Экономической комиссии ООН для Африки UNECA низкий уровень готовности стран Африки к противодействию киберугрозам обходится их экономикам в среднем в 10% их ВВП[12]. Нехватка квалифицированных кадров является одной из самых существенных проблем, с которыми сталкивается индустрия кибербезопасности в Африке. Торговые площадки и форумы даркнета широко используются террористическими и экстремистскими группировками в африканских странах для пропаганды, вербовки сторонников и координации своей деятельности. Это представляет значительную угрозу национальной безопасности для ряда государств Африки.

Категории организаций-жертв успешных кибератак в Африке за период с начала 2022 г. по первую половину 2023 г. приведены в *табл. 1*.

Обычно преступники тщательно выбирают цель своей атаки — организацию или влиятельное физическое лицо, собирают всю доступную корпоративную и персональную информацию на сотрудников и детально разрабатывают убийственную цепочку атаки. Статистика говорит, что 68% успешных кибератак являлись тщательно спланированными целевыми атаками. Самые многочисленные атаки осуществлялись с целью получения конфиденциальной информации, и их доля составляла 38%. В результате 35% кибератак нарушалась основная деятельность компаний, а 5% атак заканчивались прямыми финансовыми потерями.

Таблица 1 / Table 1

Категории организаций-жертв / Categories of victim organizations

Сектор экономики	Доля, %
Финансы	18
Телекоммуникации	13
Правительство	12
Торговля	12
Промышленность	10
Наука и образование	7
Здравоохранение	5
Другие	23

Источник / Source: Составлено автором по / Complied by the author using: URL: https://global.ptsecurity.com/analytics/africa-cybersecurity-threatscape-2022-2023

Рассмотрим особенности наиболее опасных и популярных тактик преступных кибергруппировок в Африке. Фишинговые атаки с использованием социальной инженерии, включая Business Email Compromise (BEC), представляют собой основную киберугрозу для африканских организаций и физических лиц. Более половины групп, осуществляющих атаки BEC, действуют в Африке и знакомы с особенностями этого региона. BEC — это тип киберпреступности, представляющий эффективную комбинацию фишинга и социальной инженерии, при котором мошенник использует электронную почту, чтобы обманом заставить кого-то отправить деньги или раскрыть конфиденциальную информацию компании. Преступник выдает себя за доверенное лицо жертвы (руководителя или коллегу), затем просит оплатить поддельный счет или предоставить конфиденциальные данные, которые он может использовать в другом мошенничестве. Мошенничество BEC растет в Африке из-за относительной технологической простоты операций BEC, увеличения удаленной работы сотрудников, природной доверчивости африканцев и высокой молодежной безработицы в регионе. Финансовые трудности подталкивают молодое поколение к поиску способов быстрого заработка, а все более

[11] URL: https://dataprotection.africa/wp-content/uploads/malabo_roadmap_Sept_2022.pdf

[12] URL: https://www.uneca.org/stories/eca-launches-the-guideline-for-a-model-law-on-cybersecurity-during-the-17th-igf

низкий порог входа в киберпреступную деятельность делает эту перспективу все более заманчивой для молодежи. Большой резонанс в регионе вызвало дело о BEC мошенничестве при покупке недвижимости в ЮАР. Г-жа Джудит Хаварден решила купить недвижимость в Форест-Тауне за 6 млн рандов и внесла депозит в размере 500 000 рандов. Ведущая юридическая фирма ЮАР ENS была выбрана гарантом по передаче права собственности. Покупатель Хаварден провела серию телефонных переговоров с сотрудниками ENS, и были согласованы все условия платежа. Однако преступники перехватили эти переговоры, и Хаварден получила электронное письмо от человека, которого она посчитала Эдвардом Натаном Зонненбергсом, управляющим партнером ENS, с реквизитами счета, на который она перевела остаток денег, причитающихся за продажу недвижимости. К сожалению, это электронное письмо было мошенническим, неизвестный преступник перехватил подлинное электронное письмо и изменил реквизиты банковского счета фирмы. Г-жа Хаварден не заметила, что адрес электронной почты был ensafirca.com, а не ensafrica.com и перевела мошенникам 5,5 млн рандов[13].

Второй серьезной киберугрозой в Африке является практика широкого использования программ-вымогателей. Рассмотрим методы и тактики действий преступных группировок, специализирующиеся на использовании программ-вымогателей, которые собрали только в 2023 г. со своих жертв около 30 млрд долл.[14] Выделяют несколько видов тактик использования программ-вымогателей. Простая тактика вымогательства предполагает заражение системы жертвы, шифрование всех файлов и требование выплаты за дешифрование данных. Двойная тактика вымогательства предполагает шифровку данных и угрозу их утечки в случае неуплаты выкупа. Тройная тактика вымогательства предполагает шифровку данных, их публикацию и последующую DDoS-атаку. Крупнейшей преступной группой в области производства и использования программ-вымогателей является LockBit, которая являлась мировым лидером по операциям RaaS (программы-вымогатели как сервис) и которая получила около 91 млн долл. за 1700 атак на предприятия США[15]. Самая популярная в современном даркнете бизнес-модель RaaS предполагает, что разработчик программ-вымогателей предоставляет партнерам вредоносное программное обеспечение по подписке и создает инфраструктуру управлениям им. Обычно в пакет услуг RaaS входят сама программа-вымогатель, инструменты для ее настройки и инфраструктура ее управления, закрытый форум для полной технической поддержки и подробная инструкция для пользователя[16]. Таким образом, группировка LockBit создала эффективную сеть филиалов, которые поддерживаются технологически и информационно головным офисом в обмен на авансовые платежи, абонентскую плату, долю прибыли или комбинацию авансового платежа, абонентской платы и доли прибыли филиала.

Группировка LockBit активно работает во франкофонной Африке и сумела провести более 30 успешных атак на банки, финансовые организации и телекоммуникационные компании в Западной Африке. Кибератаки этой опасной группировки в первую очередь нацелены на платежные шлюзы и международную межбанковскую систему SWIFT, которые используют африканские финансовые организации. В результате атак только одной LockBit африканский финансовый сектор потерял не менее 11 млн долл. Географическое распределение кибератак группировки LockBit показано в *табл. 2*.

LockBit была самой активной преступной группой по распространению программ-вымогателей в мире до того, как правоохранительные органы десяти стран при координации Интерпола в рамках операции «Кронос» нанесли 19 февраля 2024 г. серьезный удар по инфраструктуре группировки в даркнете, взяв под свой контроль основные информационные ресурсы LockBit в даркнете, что серьезно подорвало ее операционные возможности и саму репутацию преступной организации. В результате операции было арестовано два подозреваемых в Польше и Украине, заморожено около 200 криптовалютных счетов, 34 сервера были конфискованы, и 14 000 учетных записей

[13] URL: https://groundup.org.za/article/largest-law-firm-in-africa-ordered-to-pay-victim-cyber-crime/

[14] URL: https://www.blackfog.com/the-top-10-ransomware-groups-of-2023/

[15] URL: https://www.bleepingcomputer.com/news/security/cisa-lockbit-ransomware-extorted-91-million-in-1-700-us-attacks/

[16] URL: https://encyclopedia.kaspersky.ru/glossary/ransomware-as-a-service-raas/

Таблица 2 / Table 2

География атак / Geography of Attacks

Страна	2018	2019	2020	2021	2022
Мали	0	1	1	0	0
Нигер	0	0	1	0	0
Буркина-Фасо	0	0	1	2	0
Бенин	0	0	0	2	0
Камерун	0	1	1	0	0
Уганда	0	0	2	0	0
Габон	0	0	1	0	0
Нигерия	0	0	0	1	0
Того	0	0	1	0	0
Кот-д'Ивуар	2	8	2	0	4
Сьерра-Леоне	0	0	2	0	0
Сенегал	0	0	2	0	2

Источник / Source: составлено автором по / Complied by the author using: URL: https://www.group-ib.com/blog/opera1er-apt/

было закрыто[17]. Три международных ордера на арест и пять обвинительных заключений также были выданы французскими и американскими судебными органами. Было ликвидировано около 187 филиалов, которые были в распоряжении группировки LockBit, хотя полное число филиалов остается неизвестным правоохранительным органам. Однако сразу после операции «Кронос» уже в начале марта 2024 г. группировка LockBit провела успешную атаку на крупнейший пенсионный фонд в Африке — Южноафриканское государственное пенсионное агентство GPAA. Агентство GPAA администрирует пенсии около 1,7 миллионов государственных служащих, а деятельность агентства была остановлена более чем на неделю[18].

В апреле 2023 г. в 25 африканских странах Интерполом и Афрополом была запущена операция Africa Cyber Surge II с целью выявления киберпреступников и скомпрометированной инфраструктуры. Было арестовано 14 подозреваемых киберпреступников и выявлено 3786 вредоносных серверов управления и контроля, 1415 фишинговых ссылок и доменов, 939 мошеннических IP-адресов и более 400 других вредоносных URL-адресов, IP-адресов и бот-сетей. В ходе операции Africa Cyber Surge II были выявлены потери африканской экономики на сумму более 40 млн долл. в результате деятельности международных преступных сетей. Компания Group-IB, созданная выпускниками МВТУ им Н. Э. Баумана[19], активно участвовала с правоохранительными органами в организации сбора данных в даркнете и внесла большой вклад в успех этой международной операции.

ВЫВОДЫ

Соотношение между ежегодными потерями мировой экономики от атак из даркнета в размере 10,5 трлн долл. и ежегодными мировыми инвестициями в системы информационной безопасности объемом около 172 млрд долл. показывает, что в гонке вооружений между цифровыми нападающими и охранителями однозначно выигрывает киберпреступность. Африканский континент становится все более активной зоной для деятельности хакеров и киберпреступников.

[17] URL: https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

[18] URL: https://therecord.media/lockbit-ransomware-takes-credit-for-south-african-pension-fund-attack

[19] URL:https://www.interpol.int/News-and-Events/News/2023/Cybercrime-14-arrests-thousands-of-illicit-cyber-networks-disrupted-in-Africa-operation

Многие африканские страны сталкиваются с недостаточным развитием технологий кибербезопасности. Даркнет активно используется для координации и проведения различных видов незаконных операций, наносящих существенный ущерб экономике и безопасности стран Африки. Слабость национальных систем информационной безопасности и устойчиво высокие темпы роста национальных экономик делает африканский регион привлекательной мишенью для преступных элементов в даркнете. Трансграничная природа даркнета затрудняет правоприменение на национальном уровне и требует скоординированных усилий международного сообщества. Африканские страны нуждаются в укреплении международного сотрудничества для противодействия киберугрозам, исходящим из даркнета. Данная тема приобретает все большую актуальность в контексте стремительной цифровой трансформации континента. Африканские страны проявляют интерес к российскому опыту в области подготовки специалистов по информационной безопасности, а также к участию России в укреплении международного сотрудничества в сфере кибербезопасности. Для эффективного экспорта российских услуг по кибербезопасности в страны Африки предлагается создать российско-африканский консорциум по МИБ на базе передовых технологических компаний и ведущих вузов, который способствовал бы усилению роли России в регионе. В качестве первого шага предлагается рассмотреть возможность создания и поддержки стандартизированного Панафриканского профессионального сертификационного экзамена для специалистов по кибербезопасности для обеспечения высокого уровня экспертизы в регионе.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Holt T. J., Bossler, A. M. The Palgrave handbook of international cybercrime and cyberdeviance. London: Palgrave Macmillan; 2020. 1489 p. DOI: 10.1007/978-3-319-78440-3
2. Brevini B. WikiLeaks: Between disclosure and whistle-blowing in digital times. *Sociology Compass*. 2017:11(3):124-157. DOI: 10.1111/soc4.12457
3. David Goldschlag, Michael Reed, Paul Syverson. Onion routing. *Communications of the ACM*. 1999;42(2):39-41. DOI: 10.1145/293411.293443
4. Saleem J., Rafiqul I. Md., Zahidul I. Darknet traffic analysis: A systematic literature review. *IEEE Access*. 2024:1-1. DOI: 10.1109/ACCESS.2024.3373769
5. Gaia J., Ramamurthy B., Sanders G., Sanders S., Upadhyaya S., Wang Xunyi, Yoo Chul. Psychological profiling of hacking potential. 2020. DOI: 10.24251/HICSS.2020.273
6. Aslan Ö., Aktug S. S., Ozkan-Okay M., Yilmaz A. A., Akin, E. A. Comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*. 2023;12(6):1333. DOI: 10.3390/electronics12061333

ИНФОРМАЦИЯ ОБ АВТОРЕ / ABOUT THE AUTHOR

Александр Иоильевич Ильинский — доктор технических наук, профессор, заслуженный работник высшей школы Российской Федерации, научный руководитель Института глобальных исследований, Финансовый университет, Москва, Россия

Alexander I. Ilyinsky — Dr. Sci. (Tech.), Prof., Honored Worker of Higher Education of the Russian Federation, Scientific Supervisor of the Institute of Global Studies, Financial University, Moscow, Russia

https://orcid.org/0000-0002-7803-9146

ailyinsky@fa.ru

Конфликт интересов: автор заявляет об отсутствии конфликта интересов.
Conflicts of Interest Statement: The author has no conflicts of interest to declare.

Статья поступила 12.08.2024; принята к публикации 9.12.2024.
Автор прочитал и одобрил окончательный вариант рукописи.
The article was received on 12.08.2024; accepted for publication on 9.12.2024.
The author read and approved the final version of the manuscript.