Глава 4. ТЕНЕВАЯ ЦИФРОВАЯ ЭКОНОМИКА И ЕЕ ОСНОВНЫЕ СЕГМЕНТЫ

Вру и я, ребята, вам, в сущности, не ведая,
Как нам быть, чего нам ждать, кто всему виной.
И когда у нас привал, и когда победа. И...
Кого нам побеждать? И какой ценой?
Александр Градский,
«Экспедиция» 1987 г.

Предисловие

Наш мир стремительно изменяется под влиянием цифровой трансформации, и необходима серьезная подготовка к новым вызовам и угрозам. Состав последних постоянно изменяется вследствие развития и совершенствования вычислительной техники, программного обеспечения и технологий сбора, обработки и хранения информации. В этих условиях возрастает актуальность научно-исследовательских работ по тематике, связанной с оценкой возможных угроз в цифровой экономике. Дополнительным фактором влияния выступают изменения в цифровой информационной структуре, переход к удаленной (домашней) работе пользователей и др. Современное общество все больше полагается на робототехнические и цифровые операции вместо человеческого труда. Все это ставит под угрозу хакерских атак информационные и коммуникационные ресурсы государства и отдельных фирм. Особенно сильно пострадала глобальная цепочка поставок в условиях пандемии COVID-19 [1,2,3]. Риски усиливаются при переходе к «надомной», удаленной работе. К сожалению, все вышеперечисленное все больше и больше привлекает внимание и усилия кибер-преступников.

Наступила эпоха новой информационной реальности. Волна инноваций, которую назвали «четвертой промышленной революцией» или «второй эрой машин», принесла с собой искусственный интеллект, современную робототехнику, автономные транспортные средства, которые, увы, используются не только для общественного прогресса. Как следствие, сегодняшние компьютерные преступления отличаются качественными характеристиками от тех, которые были 20–30 и даже 10 лет назад: трансформируются способы преступлений, факторы и мотивы

преступной деятельности, сама преступность перемещается в цифровую среду. Серьезную опасность представляет также деятельность специализированных групп (государственных и частных), чья деятельность направлена на организацию нападения и преодоление защиты государственных и коммерческих интересов в кибернетической среде.

...Немного статистики

Отдельной весьма важной проблемой является исследование экономических основ киберпреступности. В данном плане ошеломляющими на фоне собранной статистики о деятельности теневой цифровой экономики выглядят данные об экономике киберпреступности. Согласно исследованию, проведенному компанией Bromium, деятельность киберпреступности в 2018 году оценивается в 1,5 триллиона долларов [21]. Это было первое исследование такого рода, направленное на изучение «динамики киберпреступности» в контексте потока доходов и распределения прибыли. В ходе проведения исследования были определены новые криминальные платформы и процветающая экономика киберпреступности, которая является самодостаточной и стирает границы законности. Грегори Уэбб (Gregory Webb), Генеральный директор Bromium, прокомментировал результаты исследования следующим образом: «Это шокирует, насколько широко распространенной и прибыльной стала киберпреступность. Модель преступности заключается в создании вредоносного ПО и обеспечении им киберпреступников с такой же легкостью, как совершаются покупки в Интернете. Мало того, что очень легко получить доступ к инструментам, услугам и опыту киберпреступников, это означает, что предприятия и правительства будут сталкиваться с более изощренными, дорогостоящими и разрушительными атаками, поскольку сеть основана на прибыли и набирает обороты. Мы не в состоянии решить эту проблему, используя старое мышление или устаревшие технологии. Настало время новых подходов» [21].

Отчет сопровождается итоговой таблицей, в которой приведены данные о годовом доходе, получаемом при реализации отдельных киберпреступлений. Следует отметить, что, как

и в случае законного бизнеса, теневой сегмент преследует максимизацию прибыли и выгоды от его деятельности. Данный факт способствует тому, что, со временем, киберпреступники могут планировать и организовать более комплексные мероприятия для достижения целей.

Таблица 3.17

Годовой доход от киберпреступлений (в млрд $) в 2018 году

№ п\п	Преступление	Годовой доход*
1	Незаконные, нелегальные онлайн рынки	860
2	Коммерческая тайна, кража IP	500
3	Торговля данными**	160
4	Кибермошенничество, CaaS (Cybercrime-as-a-Service)	1,6
5	Вымогательское ПО***	1,0
Примечание:	* — данные приблизительные;	
	** — доходы от торговли украденными данными, такими как информация о кредитных и дебетовых картах, банковские данные для входа, схемы лояльности и т.д.	
	*** —доходы от вымогательства, основанные на шифровании данных и требованиях платежей	

Источник: Jason Williams. (2019). Cybercrime as an Economy. URL: https://thefintechtimes.com/cybercrime-economy/ [21]

В данной главе высказывается интересное предположение о том, что если бы киберпреступность, с экономической точки зрения была бы суверенной страной, то она занимала бы 13 место в мире по величине ВВП. Общий доход, по приблизительным данным, равен $1,5 трлн и включает: $860 млрд — действия на незаконных, нелегальных онлайн рынках; $500 млрд — кража коммерческой тайны, IP; $160 млрд — торговля данными; $1,6 млрд — кибермошенничество и киберпреступление, как услуга; $1 млрд — вымогательское программное обеспечение. В отчете указывается, что киберпреступность функционирует на нескольких уровнях, при этом некоторые крупные торговые операции в «корпоративном» стиле приносят более $1 млрд а заказы в стиле «малого и среднего бизнеса» — от $30 000 до $50 000. Киберпреступники располагают достаточно большим набором инструментария для совершения компьютерных

преступлений. Это порождает рост соответствующих угроз. Основные угрозы кибербезопасности приведены на следующем рисунке.

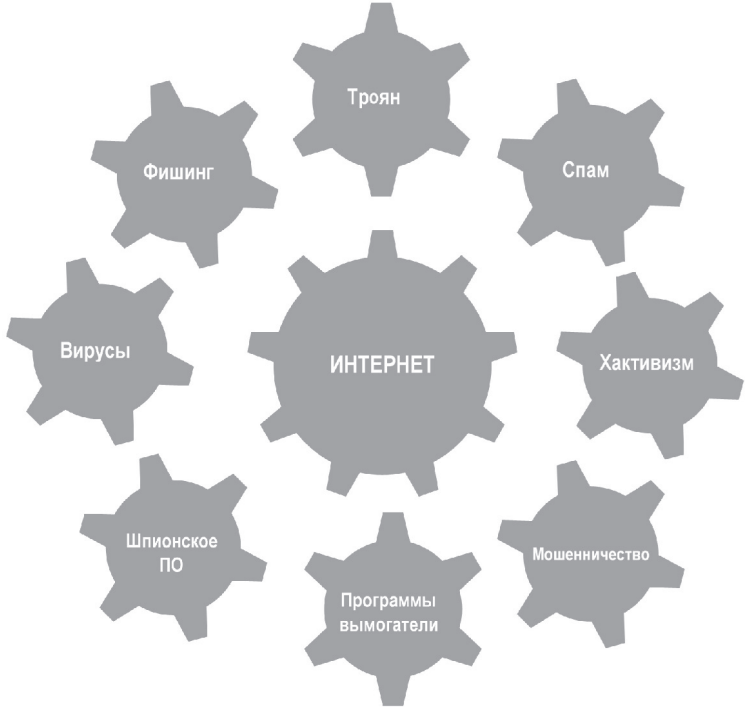

Рис. 3.27. Состав угроз кибербезопасности

Источник: Ramjee Prasad, Vandana Rohokale (2020). Cyber Security: The Lifeline of Information and Communication Technology. Springer Nature Switzerland AG. P. 2. URL: https://doi.org/10.1007/978–3–030–31703–4 [44].

Для сравнения можно использовать подход, предложенный исследователями Университета Карнеги-Меллон. Изменяются угрозы, изменяются риски, изменяются решения для противостояния угрозам. Все возможные аспекты нашли отражение в данной модели [45].

Рассмотрим далее отдельные экспертные оценки. Так, Стив Морган, главный редактор журнала Cybercrime Magazin [4], представил на суд экспертов материал, описывающий пятерку наиболее значимых фактов по кибербезопасности. В частности,

1. Согласно прогнозам, к 2025 году глобальный ущерб от киберпреступности составит 10,5 трлн долларов в год.

Если бы этот ущерб оценивали, как страну, то киберпреступность, которая, по прогнозам, нанесет ущерб на общую сумму 6 триллионов долларов США во всем мире в 2021 году, была бы третьей по величине экономикой мира после США и Китая.

По оценкам ведущего мирового исследователя и издателя Cybersecurity Ventures, который освещает глобальную киберэкономику и является надежным источником фактов, цифр и статистики по кибербезопасности, ожидает, что глобальные затраты на киберпреступность будут расти на 15 процентов в год в течение следующих пяти лет, достигнув 10,5 триллиона долларов США в год к 2025 году по сравнению с 3 триллионами долларов США в 2015 году. Инновации и инвестиции в киберпреступность, значительно превышают ущерб, нанесенный стихийными бедствиями за год, и будут более прибыльными, чем глобальная торговля всеми основными незаконными продуктами вместе взятыми (в том числе наркотики, порнография, торговля оружием и т.д.).

Затраты киберпреступности включают стоимость повреждения и уничтожения данных, кражу денег, потерю производительности, кражу интеллектуальной собственности, кражу личных и финансовых данных, хищение, мошенничество, нарушение нормального ведения бизнеса после атаки, судебно-медицинское расследование, восстановление и удаление взломанных данные и системы, а также репутационный ущерб.

2. Глобальные расходы на кибербезопасность в 2021–2025 годах в совокупности превысят 1,75 триллиона долларов. По данным Cybersecurity Ventures, необходимость защиты все более оцифрованных предприятий, устройств Интернета вещей (IoT) и потребителей от киберпреступности приведет к увеличению глобальных расходов на продукты и услуги в области кибербезопасности до 1,75 триллиона долларов в совокуп-

ности за пятилетний период с 2021 по 2025 год. Для сравнения в 2004 году мировой рынок кибербезопасности оценивался всего в 3,5 миллиарда долларов, и теперь это один из крупнейших и наиболее быстрорастущих секторов информационной экономики. Ожидается, что рынок кибербезопасности вырастет на 15 процентов в годовом исчислении с 2021 по 2025 год.

3. К концу 2021 года в мире будет 3,5 миллиона незаполненных рабочих мест в сфере кибербезопасности. Каждое ИТ-рабочее место также является позицией кибербезопасности. Каждый ИТ-работник, каждый технологический работник должен участвовать в защите приложений, данных, устройств, инфраструктуры и людей. По данным Cybersecurity Ventures, в 2021 году во всем мире будет 3,5 миллиона незаполненных рабочих мест в сфере кибербезопасности — этого достаточно, чтобы заполнить 50 стадионов Национальной футбольной лиги США. Это больше, чем предыдущая оценка Cisco в 1 миллион свободных мест в области кибербезопасности в 2014 году. Уровень безработицы в сфере кибербезопасности в 2021 году составит ноль процентов (для опытных работников, а не для должностей начального уровня), где он находился с 2011 года. Рост киберпреступности приведет к столь же большому количеству незаполненных вакансий в течение следующих 5 лет.

4. Согласно прогнозам, к 2031 году глобальный ущерб от программ-вымогателей превысит 265 миллиардов долларов.

Согласно прогнозам, глобальные убытки от ущерба от программ-вымогателей достигнут 20 миллиардов долларов в год в 2021 году по сравнению с 325 миллионами долларов в 2015 году, что в 57 раз больше. Через десять лет затраты превысят 265 миллиардов долларов.

Cybersecurity Ventures ожидает, что к 2021 году бизнес станет жертвой атаки программ-вымогателей каждые 11 секунд, по сравнению с 14 секундами в 2019 году. Это делает программы-вымогатели самым быстрорас-тущим видом киберпреступлений.

Частота атак программ-вымогателей на правительства, предприятия, потребителей и устройства будет продолжать расти

в течение следующих 5 лет и достигнет каждые две секунды к 2031 году.

Средняя сумма выкупа по оценкам [5,6] составляет значительную сумму — 220 298 долларов США ($220,298 против $154,108, что на 43 % больше, чем в четвертом квартале 2020 года), медианная сумма выкупа составляет $78,398 ($78,398 против $49450 или на 59 % больше, чем в 4 квартале 2020 г.), что предвещает количественный и качественный рост новых атак.

Дополнительным фактом усложнения противодействия программам-вымогателям является изменение тактики их реализации, так называемые программы-вымогатели с двойным вымогательством. Суть этого действия заключается в следующем — стандартные программы-вымогатели, после проникновения в информационную систему, шифровали файлы с помощью шифра RSA с открытым ключом и, если жертва не выплачивала требуемый выкуп, проходило удаление этих файлов. В результате реализации известных атак с использованием программ-вымогателей типа WannaCry и NotPetia компании усилили средства киберзащиты и должное внимание стали уделять процессам резервного копирования и восстановления. Но этого оказалось недостаточно. Впечатляют также прогнозы по частоте реализуемых атак. По прогнозам ожидается, что бизнес будет подвергаться атакам программ-вымогателей каждые 11 секунд в 2021 году по сравнению с 40 секундами в 2016 году.

5. По прогнозам, к 2025 году общий объем глобального хранилища данных превысит 200 зеттабайт. Сюда входят данные, хранящиеся в частных и общедоступных ИТ-инфраструктурах, в коммунальных инфраструктурах, в частных и общедоступных облачных центрах обработки данных, на персональных вычислительных устройствах — ПК, ноутбуках, планшетах и смартфонах — и на устройствах IoT (Интернет вещей).

Компания Cybersecurity Ventures (https://cybersecurityventures.com) прогнозирует, что общий объем данных, хранящихся в облаке, включая общедоступные облака, управляемые поставщиками и компаниями социальных сетей (например, Apple, Facebook, Google, Microsoft, Twitter и т.д.),

Государственные облака, доступные для граждан предприятия, частные облака, принадлежащие средним и крупным корпорациям, и поставщики облачных хранилищ — достигнут 100 зеттабайт к 2025 году, или 50 процентов мировых данных на тот момент, по сравнению с примерно 25 процентами, хранящимися в облаке в 2015 году.

Широкий диапазон экономических агентов с их глубокой специализацией (от разработки специфических злонамеренных программных механизмов, до сдачи в аренду готовых бот систем и т.д.), экономических отношений и других экономических факторов способствует генерации, поддержке и подтверждению высоких доходов в беспрецедентных масштабах.

Характеристики теневой цифровой экономики

В первую очередь, следует проанализировать такие категории как теневая, ненаблюдаемая, криминальная экономика и т.д. Отправной точкой следует принять и считать методологию, предложенную Организацией экономического сотрудничества и развития (ОЭСР) и рассмотренную в некоторых публикациях [8,9,10]. В частности, выделяются следующие категории:

- подпольное производство (Underground production) — деятельность, которая является продуктивной и законной, но намеренно скрыта от государственных органов, чтобы избежать уплаты налогов или соблюдения законов (правил);
- незаконное производство (Illegal production) — производственная деятельность, в результате которой создаются товары и услуги, запрещенные законом или которые являются незаконными, при осуществлении несанкционированных процедур;
- производство в неформальном секторе (Informal sector production) — производственная деятельность, проводимая некорпоративными предприятиями в секторе домашних хозяйств или других единиц, которые не зарегистрированы и/или меньше указанного размера с точки зрения занятости, и имеют рыночное производство;
- производство товаров для собственного использования (Production of households for own-final use) — производственная деятельность, в результате которой товары или услуги потребляются, или капитализируются домашними хозяйствами, которые их произвели;
- статистическое подполье (Statistical underground) — определяется как все производительные виды деятельности, которые должны учитываться в основных программах сбора данных, но пропущены из-за недостатков в статистической системе.

Многие авторы связывают незаконные действия в области информационных и коммуникационных технологий, являющиеся основой ТЦЭ (Теневая Цифровая Экономика), с кибертерроризмом и возросшими рисками в управлении обществом [11]. Для формирования общей картины считаем необходимым рассмотреть статистические данные, характеризующие некоторые виды деятельности, подпадающие, по нашему мнению, под определение ТЦЭ [12–18]. Но следует иметь в виду, что приведенные статистические данные получены путем опросов и не в полной мере характеризуют исследуемые явления. Это еще одна из нерешенных проблем, для ее решения следует разработать новые методологические подходы и методики измерения.

В отчете «The Global Risks Report 2018» [20], который был подготовлен Мировым Экономическим Форумом, информационные угрозы вошли в рейтинг глобальных рисков. Такие угрозы, как «Кибератаки» и «Кража данных и мошенничество» вошли в пятерку высоковероятных, присутствует также угроза критическим инфраструктурам. Там же, выделяются основные области рисков: экономические, геополитические, экологические, социальные и технологические. Именно в последней области сосредоточены глобальные преобразования, направленные на: информационную безопасность, информационные технологии, управление интернетом, цифровую экономику и общество, рабочую силу и занятость, будущее экономического прогресса, перспективы молодежи, поставки и транспорт, миграция, 4-ю промышленную революцию. В этом отчете рассматриваются 10 глобальных рисков. Безработица и неполная занятость представляют собой большой риск для ведения бизнеса. Это мнение более чем 12000 экспертов из 140 стран. Второй

по величине риск — «отказ от национального управления». Эти выводы должны вызывать тревожные звонки. В то время, когда мир часто отвлекается на последние повороты ускоряющихся информационных циклов, они дают предостерегающие доказательства слабых сторон в основе наших политических и экономических систем.

22 января 2020 года «Четырьмя всадниками Апокалипсиса» назвал Генеральный секретарь ООН главные угрозы человечеству: геостратегическую напряженность, изменение климата, рост недоверия на глобальном уровне и опасность новых технологий («Обратная сторона» цифровой революции) [36].

Рис. 3.28. Четыре всадника Апокалипсиса.
©Siran Maxim 2022

По словам Генерального секретаря, новые технологии развиваются настолько быстро, что мы не успеваем не только отреагировать на них, но порой даже понять их суть. При том, что они сулят огромные преимущества, цифровые технологии и искусственный интеллект становятся инструментом подстрекательства, распространения ложной информации, вмешательства в частную жизнь, эксплуатации людей и совершения преступлений.

Так, он считает неприемлемым использование боевых автономных систем — «машин, способных убивать без всякого участия человека и не несущих никакой ответственности», и призывает запретить применение «роботов-убийц».

А. Гутерриш настоятельно рекомендовал навести порядок и в киберпространстве, которое он назвал цифровым «Диким западом». «Террористы, поборники чистоты белой расы и другие им подобные злоупотребляют интернетом и социальными сетями, — отметил глава ООН. — Боты распространяют дезинформацию, подталкивают к поляризации и подрывают демократию. В следующем году киберпреступность обойдется нам в 6 триллионов долларов».

Еще один фронт борьбы с издержками новых технологий — это рынок труда, где, как предсказывает А. Гутерриш, автоматика в ближайшее десятилетие лишит работы сотни миллионов трудящихся. Он видит выход в реформе системы образования, задачей которой будет научить людей учиться в течение всей жизни. По словам Генерального секретаря, ООН — это самая подходящая платформа для того, чтобы правительства, частный сектор, гражданское общество смогли противопоставить «цифровому расколу» глобальное сотрудничество.

В глобальном плане наблюдается широкий диапазон киберпреступлений, которые включают преступления, совершаемые в целях получения финансовой выгоды, преступления, связанные с использованием информации, которая содержится в компьютере, а также преступления, направленные против конфиденциальности, целостности и доступности компьютерных систем.

«Но для того, чтобы это было успешным, мы также должны обратить внимание на темные стороны цифрового мира» высказалась председатель ЕвроКомиссии Урсула ван дер Лейен перед участниками совещания в Давосе [39].

Для дополнительной характеристики ТЦЭ считаем возможным сослаться на разработку RAND Corp. «Экономическая конкуренция в XXI веке» [37]. В данном отчете рассматриваются различные формы экономической конкуренции, включая концепцию национальной конкурентоспособности, конкуренцию

за рынки и инвестиции, использования экономических инструментов в других сферах международной конкуренции, а также конкуренцию за природу глобальной экономической системы. В качестве главной мысли используется тезис о том, что геополитическая конкуренция с использованием экономических инструментов может быть эффективной, но использование подобных инструментов может быть весьма дорогостоящим. В любом случае следует взвешивать затраты на их осуществление и получаемыми преимуществами. Среди других экономических инструментов для геополитической конкуренции США выделяются следующие: торговая политика; инвестиционная политика; санкции; киберинструменты; помощь; финансовая и денежно-кредитная политика; производство и экспорт энергии и товаров.

Особый интерес уделяется киберинструментам, поскольку они могут быть использованы для нанесения ущерба, а также кражи объектов интеллектуальной собственности, технологий и коммерческой тайны.

Как отмечается в [38], тематика цифровой экономики весьма обширна и в настоящее время является крайне популярной. «Ажиотаж вокруг этой области, с одной стороны, и отсутствие единого понятийного поля, с другой, приводит к появлению огромного количества, казалось бы, несовместимых мнений и, как следствие, к невозможности диалога».

Авторы [42, с. 3–4], высказывают важный и справедливый тезис о том, что цифровая экономика — это новая форма экономического и социального развития общества после аграрной экономики и индустриальной экономики. Понимание людьми основ цифровой экономики пришло постепенно. Среди многочисленных определений цифровой экономики наиболее представительным является определение, высказанное в рамках проекта «Развитие и сотрудничества цифровой экономики G20» и представленное на Саммите G20 в Гуанжоу в 2016 году. Данная инициатива утверждает, что цифровая экономика относится к ряду видов экономической деятельности с оцифрованными знаниями и информацией, как ключевыми факторами производства, современной информационной сетью как их основной носитель, а также эффективное использование информационных и коммуникационных технологий (ИКТ) как основной движущей силы повышения эффективности и оптимизации экономической структуры.

В свою очередь, автор [43, с. 3], рассматривает цифровую экономику сквозь призму моделей и теорий и приводит перечень основных моделей, используемых для исследований в области экономики и управления. Перечень данных моделей и теорий приведен в следующей таблице.

Таблица 3.18

Цифровая экономика: модели для исследования

Номер модели	Название модели/теорий
1	Экономика данных
2	Сервисная экономика
3	Платформенная экономика
4	Экономика Интернета вещей
5	Совместная экономика
6	Потребительская экономика
7	Экономика с длинным хвостом
8	Инклюзивная экономика
9	Совместная экономика
10	Умная экономика
11	Теневая цифровая экономика

Источник: Xiaoming Zhu (2019). Emerging Champions in the Digital Economy. New Theories and Cases on Evolving Technologies and Business Models. Shanghai Jiao Tong University Press and Springer Nature Singapore Pte Ltd. P. 3. URL: https://doi.org/10.1007/978–981–13–2628–8

Авторы настоящей работы считают необходимым внести добавление в состав данной таблицы и использовать модель теневой цифровой экономики, как предмет будущих исследований и пристального анализа.

Противостояние между легальными и нелегальными средствами и способами ведения экономических операций присутствовало всегда. Поэтому, авторы считают, что теории и модели следует исследовать в том числе с теневой стороны. Особенно в случае цифровизации области экономики и управления, где скорость планирования и реализации экономических операций со знаком минус является очень высокой, а комплекс используемого инструментария и техник становится очень комплексным.

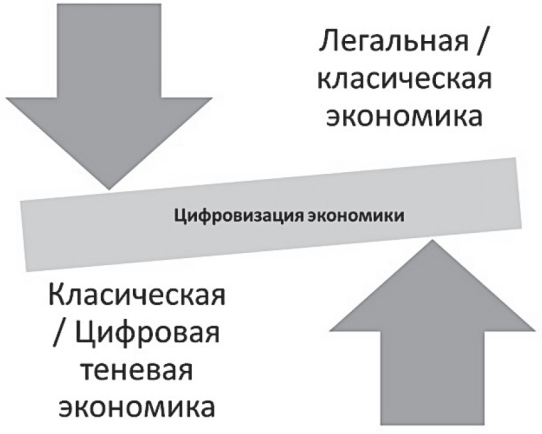

Рис. 3.29. Противостояние между легальной и теневой экономикой

Существуют основания предполагать, что интерес к противоправной деятельности в области цифровой экономики будет стремительно нарастать и данный процесс, и действия необходимо исследовать во всех аспектах, в первую очередь, по отношению к критическим технологиям для предотвращения серьезных последствий.

Недостаточно разработанной проблемой является использование статистических данных для определения доли ТЦЭ в процессах информатизации. В настоящее время уровень развития информационного общества измеряется через призму композиционных индексов информационно-коммуникационных технологий (е-индексы), основными из которых являются следующие:

1. Индекс информационного общества (Information Socity Index, ISI) характеризует уровень развития информационных технологий, возможности распространения и доступность информации в 53 странах. ISI рассчитывают и публикуют две организации World Times и Корпорация международных данных (IDC) начиная с 1997 г. Индекс ISI вычисляется на основе 15 показателей, сгруппированных в четыре категории: 1) компьютеры, 2) телекоммуникации, 3) интернет, 4) социальное развитие общества.
2. Индекс электронной готовности (E-Readiness Index, ERI) разработан компанией Economist Intelligence Unit (EIU) совместно с Институтом бизнес-ценностей IBM, которые начиная с 2000 г. проводят ежегодное исследование возможностей использования ИКТ для обеспечения устойчивого развития экономики и укрепления благосостояния граждан. В 2010 г. ERI переименован в «рейтинг цифровой экономики» (Digital Economy Ranking). Индекс включает 6 составляющих: 1) инфраструктура подключения и технологий; 2) бизнес-окружение; 3) социальная и культурная среда; 4) правовая среда; 5) государственная политика и стратегия; 6) принятие обществом и бизнесом.
3. Индекс экономики знаний (Knowledge Economy Index, KEI) — комплексный показатель эффективности использования знаний в целях экономического и общественного развития. В основе расчета индекса лежит предложенная Всемирным банком (ВБ) «Методология оценки знаний» (The Knowledge Assessment Methodology — KAM), в которой установлена прямая взаимосвязь между так называемой «интеллектуальностью» экономики и долгосрочным, стабильным экономическим ростом, а также конкурентоспособностью страны. Индекс оценивается ежегодно на основании 109 показателей.
4. Индекс развития электронного правительства (E-Government Development Index, EGDI) — комплексный показатель, который оценивает возможности государственных структур использовать ИКТ для предоставления гражданам государственных услуг. Индекс разработан

ООН и выпускается раз в два года. Он включает три группы показателей: 1) степень охвата и качество интернет-услуг, 2) уровень развития ИКТ-инфраструктуры, 3) человеческий капитал.

5. Индекс развития информационно-коммуникационных технологий (ICT Development Index, IDI) — рассчитывается по методике Международного союза электросвязи (МСЭ — International Telecommunication Union, ITU), публикуется регулярной основе. IDI состоит из трех субиндексов: 1) доступа, 2) использования и 3) практических навыков, каждый из которых отражает различные аспекты и компоненты процесса развития ИКТ.
6. Индекс цифровой доступности (Digital Access Index, DAI) — показатель, который измеряет общие возможности доступа и использования ИКТ для граждан. Индекс разработан в 2003 г. подразделением по анализу информационных и статистических рынков МСЭ и рассчитывается для 181 страны. DAI построен на основе четырех составляющих:

✓ инфраструктура,
✓ доступность,
✓ знания и качество,
✓ фактическое использование ИКТ.

7. Индекс технологических достижений (Technology Achievement Index, TAI) включает четыре блока показателей: 1) создание новых технологий; 2) распространение инноваций; 3) распространение актуальных технологий; 4) построение базы человеческих навыков для создания и принятия технологий.
8. Индекс сетевой готовности (Networked Readiness Index, NRI) — комплексный показатель, характеризующий уровень развития ИКТ в странах мира. Индекс рассчитывается Всемирным экономическим форумом (WEF) и международной школой бизнеса INSEAD с 2002 г. на основе статистических данных ООН, МСЭ, ВБ и других организаций, а также результатов ежегодного опроса мнения руководителей. Индекс измеряет уровень развития ИКТ по 68 параметрам, объединенным в три группы: 1) внешняя среда, 2) готовность государства, бизнеса и гражданского общества к использованию ИКТ, 3) использование ИКТ государством, бизнесом и гражданским обществом.
9. Индекс цифровых возможностей (Digital Opportunity Index, DOI) измеряет возможности ИКТ посредством анализа инфраструктуры, доступности и покрытия, качества. Он оценивается на основе 3 субиндексов: 1) возможности, 2) инфраструктура и 3) использование.
10. Индекс возможностей развития ИКТ (ICT Opportunity Index, ICT-OI) разработан в 2002–2003 гг. МСЭ. Он состоит из подиндексов в 2 группах: 1) информационная плотность — включает подиндексы развития сетей и квалификации; 2) использование ИКТ — включает подиндексы восприимчивости ИКТ и интенсивности использования.
11. Индекс диффузии ИКТ (ICT Diffusion Index, ICT-DI) предназначен для оценки развития ИКТ на основе показателей их распространения. Он измеряется на основе 2 показателей: 1) связь (количество интернет-хостов, персональных компьютеров, телефонных линий и абонентов мобильной связи на душу населения); 2) доступ (количество интернет-пользователей, грамотность взрослого населения, стоимость местного звонка и ВВП на душу населения).
12. Индекс глобальной конкурентоспособности (Global Competitiveness Index, GCI) — рейтинг стран мира по показателю экономической конкурентоспособности, рассчитывается с 2004 г. по методике WEF, основанной на комбинации статистических данных и результатов опроса менеджмента. Индекс составлен из 113 переменных, которые объединены в 12 показателей: 1) качество институтов, 2) инфраструктура, 3) макроэкономическая стабильность, 4) здоровье и начальное образование, 5) высшее образование и профессиональная подготовка, 6) эффективность рынка товаров и услуг, 7) эффективность рынка труда, 8) развитость финансового рынка,

9) уровень технологического развития, 10) размер внутреннего рынка, 11) конкурентоспособность компаний, 12) инновационный потенциал.

13. Глобальный индекс инноваций (Global Innovation Index, GII) разработан Европейским институтом делового администрирования (INSEAD) в сотрудничестве с Конфедерацией индийской промышленности при поддержке Canon Inc.
14. Индекс цифрового разделения (Infostates, IS) был предложен Orbicom и Международной сетью кафедр ЮНЕСКО в области связи. Он включает 2 сводных показателя: 1) инфо-плотность (запасы капитала и рабочей силы ИКТ, навыки в области ИКТ, необходимые для функционирования информационного, ориентированного на знания общества) и 2) инфо-использование (потоки ИКТ, интенсивность их фактического использования домашними хозяйствами, предприятиями и правительством).

Определение теневой цифровой экономики (тцэ)

Интерес к теневым процессам, протекающим в экономике отдельных стран, возник в середине 20 столетия. Результаты отдельных разрозненных исследований привели к формированию нового научного направления в экономике, на уровне государства начали разработку программ противодействия процессам теневой экономики и вывода их из тени. Проведенные на раннем этапе исследования позволили зафиксировать уровень теневой экономики, ее структуру и, самое главное, были сделаны заключения о возможности вывода результатов деятельности из тени.

В основу настоящего исследования положены работы отечественных и зарубежных ученых [22–35] и необходимо отметить работы австрийского ученого профессора Фридриха Шнейдера, в которых отражены все аспекты проблем теневой экономики не только развитых, но и развивающихся стран.

«Теневая экономика» — это неформальная часть национальной экономики, не учитываемой официальной статистикой.

Она охватывает все виды деятельности, неучтенной и незафиксированной официально, в том числе такие, как [30]:

- операции, не запрещенные законом (так называемый «серый рынок»);
- криминальная деятельность, запрещенная законом («черный рынок»);
- внерыночная деятельность, когда продукты и услуги производятся и потребляются в домашних хозяйствах;
- бартерный обмен продуктами и услугами, при условии невыхода на рынок.

Рассмотрим сегменты «классической» теневой экономики. Основными из них являются следующие:

1. Неформальная экономика («серый рынок») — в принципе законные экономические операции, масштаб которых скрывается или занижается хозяйствующими субъектами, как, например, трудовой наем без оформления, нерегистрируемые ремонтно-строительные работы, репетиторство, сдача в аренду недвижимости и другие способы уклонения от налогов.
2. Криминальная экономика («черный рынок») — экономическая деятельность, запрещенная законом в любой экономической системе и в подавляющем большинстве стран: наркобизнес, контрабанда, проституция, рэкет и др.
3. Фиктивная экономика — предоставление взяток, индивидуальных льгот и субсидий на основе организованных коррупционных связей.

В отличии от «классической» теневой экономики ТЦЭ отличается составом и структурой, которые будут рассмотрены далее.

Наряду с определением категории «теневая» экономика очень часто используются и другие, такие как: альтернативная экономика, скрываемая, скрытая, сумеречная, невидимая, автономная, черная, наличная, тайная, незаконная, параллельная, неофициальная и др.

Считаем важным отметить, что некоторые из этих определений ссылаются на отдельные аспекты теневой экономики, покрывают один из определенных её сегментов. Правда, большинство из этих определений охватывают явление целиком.

Например, «серая», «подпольная», «теневая», «параллельная» в основном указывают на целостное явление, в то время как определения «черная» и «криминальная» — ссылаются лишь на его отдельные, более узкие участки незаконной деятельности.

Сформулируем определение теневой цифровой экономики, основываясь на ее специфике с точки зрения производства продуктов и услуг, жизненного цикла производства и услуг и т.д. Таким образом, *теневая цифровая экономика (ТЦЭ) — сектор экономических отношений, охватывающих все виды производственно-хозяйственной деятельности, которые по своей направленности, содержанию, характеру и форме противоречат требованиям законодательства и осуществляются вопреки государственному регулированию экономики и в обход контроля над ней.*

Основу ТЦЭ составляет теневая предпринимательская деятельность, общими чертами которой являются:

- скрытый, латентный (тайный) характер, то есть та деятельность, которая не регистрируется государственными органами и не находит отражение в официальной отчетности;
- охват всех фаз процесса общественного воспроизводства (производство, распределение, обмен и потребление);
- паразитический характер всех процессов, от раскрытия исходного кода программного продукта до монетизации сдачи в аренду бот-нетов.

Следует отметить, что первыми авторами, которые использовали категорию «теневая информационная экономика» — были авторы монографии «Рынок информационных услуг и продуктов». В 5 главе монографии выделен параграф 5.2.4 «Теневая информационная экономика», который начинается с использованием главной посылки нашего исследования — «Рассмотрение теневого сектора информационной экономики и информационной деятельности требуется для оценки ее объема и потенциального ущерба, который она наносит». Вместе с тем указывается, что реальные потери бюджета России из-за теневого характера частного бизнеса в области информационных услуг и продуктов не так велики и, по сути, данный тип теневого бизнеса является одним из немногих, которые заслуживает

вывода из тени путем введения для него безналогового режима в целях поддержки развития. Таким образом, в России определенная часть информационной деятельности и рынка информационных услуг и продуктов находится в тени. Теневой сектор не имеет криминальной основы и связан с низкой эффективностью информационной деятельности, уровень развития которой не позволяет не только финансировать рост, но и осуществлять простое воспроизводство при условии оплаты всех налогов». Следует обратить внимание на выделение авторами части рынка информационных услуг и продуктов, который находится в тени и отсутствие криминальной основы. За прошедшее время картина кардинальным образом изменилась — часть рынка информационных продуктов и услуг стала подпольной и криминальной, приносящей высокую прибыль [24].

Научные споры ведутся вокруг качественных характеристик участников, занятых в ТЦЭ. В частности, в [47], предложен следующий перечень специальностей:

- Программисты (Programmers). Они разрабатывают код вредоносных программ различной ориентации, в том числе программные продукты для вымогательства или кражи данных у потенциальных жертв;
- Торговцы (Merchants). Именно эта категория является последним звеном в процессе разработки программного продукта. Они продают программные злоупотребления и похищенные данные жертвы. Одновременно они обеспечивают обратную связь между разработчиком и пользователем;
- ИТ-специалисты (IT Technicians). Они создают и поддерживают инфраструктуру (сети, серверы, базы данных и т.д.) для ТЦЭ;
- Хакеры (Hackers). Осуществляют поиск и отработку уязвимостей в информационных системах, приложениях, сетях и т.д.;
- Мошенники (Fraudsters). Анализируют и создают новые схемы мошенничества и манипулирования потенциальными жертвами;

– Услуги хостинга (Hosting Services). Осуществляют предоставление услуг хостинга преступников, поддерживают мошеннический контент и соответствующие сайты;
– Управление (Management). Осуществляют поиск новых членов команды, формируют команды по соответствующим направлениям и управляют реализацией операций.

Сегменты теневой цифровой экономики

Обобщенная структура ТЦЭ предусматривает деление на продукты и услуги, с учетом постоянной их изменчивости. Данное свойство является определяющим, поскольку достижения научно-технического прогресса и нововведения в области информационных и коммуникационных технологий обеспечивает достаточно быструю сменяемость аппаратной и программной платформ.

Следует отметить, что в практике информационной безопасности используют множество классификаций [48–54].

К продуктам в сфере ТЦЭ следует отнести, прежде всего, специализированное программное обеспечение (вредоносные программы). Это огромный класс программ, состав которого постоянно изменяется и это заставляет специалистов по информационной безопасности предпринимать комплекс мер и выстраивать технические и программные барьеры для исключения их проникновения в информационные системы. Более подробное рассмотрение состава и структуры продуктов и услуг криминальной направленности приведено в [55].

Какие выводы можно сделать в результате анализа?

Во-первых, следует отметить, что риск использования вредоносного ПО явно недооценивается, что затрудняет усилия по защите критической инфраструктуры и информационных ресурсов. Это приводит к тому, что потери от воздействия криминального ПО растут, принимаемые контрмеры снижают эффективность противостояния. Воздействие криминального ПО огромно, и если существенно не увеличить усилия по противостоянию, то могут иметь место последствия более серьезные и масштабные по проявлению и стоимости.

Во-вторых, рост преступного ПО является устойчивым, частота распространения новых разновидностей растет из года в год. И как результат, криминальное ПО представляет собой более серьезную угрозу воздействия на бизнес, чем целевые атаки на информационные системы.

В-третьих, внедрение криминального ПО не является дорогим и не требует больших усилий со стороны мотивированных участников, что обеспечивает оптимизацию проводимых атак для достижения прибыльных целей. Возможность увеличения оперативности и смены стратегии привели к появлению все более изощренных и целенаправленных программ нападения на бизнес.

В-четвертых, отмечается, что эффективность усилий правоохранительных органов по противостоянию криминального ПО со временем уменьшается. Способности разработчиков и атакующих за счет адаптации к изменяющимся условиям, традиционно опережает возможности правоохранительных органов в поиске, нахождении и привлечении к уголовной ответственности. Атакующая сторона моделирует риск привлечения к уголовной ответственности на основе практики работы правоохранительных органов и полностью основывается на возможности получения прибыли. И как результат, с учетом таких факторов, как время, географическое положение и другие, деятельность правоохранительных органов серьезно ограничивается и усилия сводятся к мизерным результатам. Одновременно, эти факторы позволяют разработчикам и анализаторам криминального ПО обладать запасом времени для адаптации новых версий и делает это ПО более «эффективным» и вредным по отношению к пользователям информационных систем.

В-пятых, все повсеместно признают, что crimeware — это серьезный бизнес. Разработчики моделируют свою деятельность в соответствии с корпоративными стандартами для максимизации прибыли. В качестве примера можно рассматривать появление «crimeware-as-a-service» (преступное программное обеспечение как услуга) в качестве демонстрации своих возможностей. Киберпреступники в течение трехмесячного периода кардинально изменяют наборы своих инструментов

для достижения новых результатов. Дополнительным примером может служить также «криптомайнинг как операция» (Cryptomining as an operation). Рынок криптовалют подвергнут значительным колебаниям. Волатильность криптовалют (Биткойн и другие) напрямую отражается на активности и стоимости «Cryptomining-as an-operation», которая резко изменяется в течение короткого периода времени. Статистическая корреляция между скачками индекса Биткойн и популярностью «Cryptomining- as an-operation» может рассматриваться как высокодоходный инструмент влияния на бизнес.

В-шестых, изменились цели кибермошенников. Если ранее в качестве цели рассматривался пользователь персонального компьютера, то сейчас в качестве цели выступают корпорации и корпоративные жертвы. По мере того, как опасность реальных угроз возрастает, организованные преступные группировки переключились на корпорации.

Еще одним подтверждением тезиса о том, что crimeware — это серьезный бизнес, является публикация в июле 2020 года информации о том, что Cerberus представляет собой первое в мире вредоносное ПО с функцией похищения кодов двухфакторной аутентификации [56]. Разработчики банковского Android-трояна Cerberus намеревались продать весь свой проект целиком. Торги предполагалось проводить в виде аукциона, и стартовая цена объявлена $50 тыс. За $100 тыс. разработчики готовы расстаться со своим детищем, не торгуясь. За свои деньги покупатель получит исходный код трояна, APK, модули, панель администрирования, серверы, списки действующих и потенциальных клиентов, руководство по установке и скрипты, необходимые для слаженной работы всех компонентов.

В течение как минимум одно года разработчики Cerberus активно рекламировали свои услуги и сдавали вредонос в аренду за $12 тыс. в год. Клиентам также была доступна аренда на более короткий срок ($4 тыс. за 3 месяца и $7 тыс. за 6 месяцев). Согласно публикации продавцов на одном из русскоязычных киберпреступных форумов, бизнес приносит доход в размере $10 тыс. ежемесячно. По их словам, команда Cerberus распалась, а у оставшихся разработчиков не хватает времени на круглосуточную ежедневную поддержку трояна.

Авторы изучили состав основных продуктов и услуг криминальной направленности, относящихся к ТЦЭ, представленный на рис. 3.30. Но их спектр постоянно изменяется, появляются новые сегменты, требующие исследования и описания.

Рис. 3.30. Основные сегменты теневой цифровой экономики

Далее будут рассмотрены и проанализированы следующие сегменты: кибероружие, как сосредоточение всех достижений информационных и коммуникационных технологий на уровне противодействия между государствами; целенаправленные атаки и АТР-группы; утечки информации, нападение на криптобиржи, кража личных данных.

Кибернетическое оружие

Под кибероружием понимается, прежде всего, вредоносное программное обеспечение, используемое в военных или разведывательных целях. В последнее время всплывает все больше и больше случаев подобного использования программного обеспечения. Одна из основных характерных черт подобных атак — узкая направленность, в отличие от киберпреступников, стремящихся заразить как можно большее количество жертв. Чаще всего подобные разработки спонсируются или проводятся государственными учреждениями. Наиболее яркими примерами

подобного программного обеспечения служат Stuxnet, Falme, Duqu, Gauss. Почти всегда в подобных вредоносных программах используются уязвимости нулевого дня.

К числу стран, официально объявивших о наличии специальных подразделений, чья деятельность связана не только с кибероборонои, но и кибератаками, являются следующие: США, Великобритания, Российская Федерация, Франция, Германия, Эстония, Иран, Израиль, Южная и Северная Корея, Китай, Австралия и др.

Международный институт стратегических исследований (IISS) подготовил доклад [57], в котором перечислил 15 основных мировых кибердержав и определил возможности стран по семи критериям: стратегия и доктрина; управление, командование и контроль; возможности киберразведки; зависимость от киберпространства; кибербезопасность; глобальное лидерство в вопросах киберпространства, а также наступательный кибернетический потенциал. Было предложено выделить три группы стран. В первую группу были отнесены только США вследствие того, что цифровой суверенитет и самые мощные наступательные возможности в киберпространстве имеют только Соединенные Штаты. Они также лидируют и по внедрению цифровых технологий во все сферы жизни человека. Во вторую группу включены следующие страны: Россия, Австралия, Канада, Китай, Франция, Израиль и Великобритания. К третьей группе отнесены Индия, Индонезия, Иран, Япония, Малайзия, Северная Корея и Вьетнам.

Основными событиями в данном сегменте выступают следующие [41]:

1) 1982 — Взрыв на советском газопроводе в Сибири. По слухам, причина взрыва — «закладка» в программном обеспечении, которое использовалось в управляющей системе.
2) 1997 — Операция —Eligible Receiver‖. Первые полноценные киберучения. Внутренняя операция американских спецслужб, в процессе которой были атакованы сервера других государственных институтов США.
3) 1998–2000 — Операция —Moonlight Maze‖. Атакованы

Пентагон, NASA, Департамент энергетики, исследовательские компании и университеты США.

4) 2003–2006 — Операция «Титановый дождь». Атакованы NASA, Lockheed Martin, Sandia National Laboratories, Redstone Arsenal. Точные масштабы нападения неизвестны, однако в нем подозревают китайских хакеров либо кого-то, кто использовал для этого расположенные на территории Китая компьютеры.
5) 2006 — Израиль использует киберсредства в ходе конфликта с группировкой Hezbollah.
6) 2007 — Множественные хакерские атаки на правительственные и военные структуры США, Германии, Индии.
7) Апрель 2007 — DDOS против Эстонии. Серия массированных DDoS-атак на эстонские государственные порталы началась 27 августа, сразу после решения правительства перенести статую бронзового солдата в Таллине. Данная атака привела к созданию в Эстонии Европейского центра по борьбе с киберугрозами. В организации нападения некоторые специалисты обвиняют структуры, близкие к движению «Наши».
8) Сентябрь 2007 — Операция Orchard. Израильская бомбардировка ядерного центра в Сирии. Кроме массированных авиаударов использовалась специальная, предварительно внедренная вредоносна программа, которая влияла на работу радаров.
9) 2008 — Массовые атаки и взломы правительственных и прочих Интернет-ресурсов Грузии во время операции «Принуждение к миру» в Южной Осетии.
10) 2009 — Операция «Аврора». Серия кибератак, инициированных в 2009 году структурами, близкими к Китайской народной освободительной армии, против американских интернет-гигантов, по большей части Google.
11) Нападение на Корею. Более 166 тыс. компьютеров были инфицированы вирусом, сделавшим их частью огромного ботнета, чей атакующий потенциал был направлен против правительственных, финансовых и медийных сайтов Южной Кореи.

12) 2010 — Операция Myrtus. Червь Staxnet был обнаружен в Иране. Целью червя стали программируемые логические контроллеры. Эти устройства обслуживают моторы, работающие на крайне высоких частотах, которые установлены в Иране только на заводе по обогащению урана.
13) Атака на Бирму. Мощнейшая DDoS-атака на крупнейшего интернет-провайдера Бирмы началась незадолго до первых за 20 лет всеобщих выборов, впоследствии признанных фиктивными.
14) АЭС В БУШЕРЕ, ИРАН. По версии New York Times, компьютерный червь Stuxnet был разработан спецслужбами США и Израиля специально для саботажа иранской ядерной программы. По данным Symantec, вирусом оказалось заражено 58,85 % компьютеров Ирана, 18,22 % компьютеров Индонезии и 8,31 % машин в Индии.
15) 2012 — Операция ABABIL. Общее название для серии кибератак на американские финансовые институты, инициированной группировкой Cyber fighters of Izz Ad-Din Al Qassam, названной в честь мусульманского проповедника.
16) 2013 — Атака «МЕССИИ». 1 июня государственными регуляторными органами Сингапура были приняты новые правила: в течение 24 часов все местные сайты с посещаемостью от 50 тыс. посетителей должны были удалить с серверов любые статьи, призывающие к «нарушению расовой либо религиозной гармонии» в стране. В ответ на это хакерская группировка «Анонимусы» инициировала атаку на государственные сайты Сингапура, в том числе сайт премьер-министра.
17) Утечка данных из JPMorgan Chase. Крупнейший американский банк, один из старейших финансовых институтов на планете подвергся серьезной хакерской атаке, в результате чего более 83 млн счетов были скомпрометированы. По одной из версий, за нападением стояли русские хакеры, также атаковавшие другие банки США.
18) Операция CLEAVER. Согласно отчету компании Cylance, к массовой атаке на 50 объектов из 16 стран (в том числе

Korean Air, Qatar Airlines, Pemex) оказались причастны иранские хакеры, тесно связанные с Корпусом стражей исламской революции.

Нельзя не отметить и масштабные акции группировки «Anonymous» на ресурсы критической инфраструктуры России в феврале-марте 2022 года. Данные атаки еще подлежат анализу исследователей, но уже можно констатировать что нанесенный ущерб был существенным и что действия и используемые инструменты, и техники были несоизмеримы с многими другими похожими атаками.

Считаем необходимым отметить, что программы-вымогатели (ransomware) очень часто выступают в качестве геополитического оружия. Большинство подобных программ имеют финансовую мотивацию. Но часть ориентирована на геополитические цели для достижения обмана, шпионажа, нанесения ущерба репутации и срыв операций противника. Создаваемые вредоносные программы направлены на воздействие в следующих отраслях [64]: гостиничный бизнес и питание; образовательные услуги; финансы и страхование; здравоохранение; информация; производство; государственное управление; розничная торговля.

Данные программы-вымогатели используются в качестве прикрытия и обмана, поскольку реализация атак с их использованием является по стоимости достаточно низкой и дает возможность отрицания выполненных действий. Всегда можно утверждать, что подобные атаки были совершены простыми киберпреступниками или другим государством и реализовать меру правдоподобного отрицания.

Но все действия злоумышленников оставляют следы своей деятельности, и государственные органы безопасности владеют достаточными средствами анализа и отслеживания. Но следует иметь в виду, действия киберпреступников постоянно совершенствуются и в ближайшей перспективе существенно изменятся. Например, используя программы-вымогатели, преступники заставляют выплачивать выкуп не только в Биткойн, но и криптовалютой Монеро, которая ориентирована на повышенную конфиденциальность транзакций.

Программы-вымогатели не просто опасны. Это также один из самых динамичных, постоянно меняющихся сегментов ТЦЭ, связанных с программным обеспечением криминальной направленности и криптовалютой.

Авторами допускается, что в скором будущем, преступники будут использовать искусственный интеллект для выбора целей/жертв, выбора наиболее подходящей платформы атак и инструментов, организации и реализации самой атаки.

Утечки критической информации

Одной из самых серьезных глобальных проблем в области ИТ является утечка информации. По данным российской компании Infowatch, утечки данных встречаются повсеместно. Рассмотрим статистику, характеризующую виновников утечек, основные каналы и распределение утечек по типам информации, которая приведена в следующих таблицах [40].

Таблица 3.19

Виновники утечек информации (в %)

№ п\п	Виновник	2016	20 17*	2018*
1	Внешний злоумышленник	55,4	41,7	37,6
2	Сотрудник	33,9	50,3	53,5
3	Подрядчик	6,1	2,2	3,5
4	Руководитель	2,2	2,2	2,3
5	Бывший сотрудник	2,1	2,4	1,9
6	Системный администратор	0,4	1,1	1,2

* — первая половина года

Источник: Отчеты компании Infowatch и Solar Jsoc (https://www.infowatch.ru/report2018_half и https://vc.ru/flood/46212-issledovanie-sotrudniki-kompaniy-stanovyatsya-prichinoy-utechek-dannyh-vdvoe-chashche-chem-hakery)

Анализ данных, приведенных в таблице, позволяет сделать предварительные выводы о значительном росте утечек информации по вине сотрудников (более 50 %), незначительном снижении утечек за счет внешних злоумышленников (с 55,4 % в 2016 году до 37,6 % в первом полугодии 2018 года) и подрядчиков. Относительно стабильными остались утечки, организованные руководителями, бывшими сотрудниками. Значительный рост наблюдается в отношении системных администраторов (с 0,4 % в 2016 г. до 1,2 % в первом полугодии 2018 г.).

Таблица 3.20

Каналы утечек информации

№ п\п	Каналы утечек информации	2016	2017*	2018*
1	Сеть	69,5	67,4	69,8
2	Съемные носители	4,1	2,3	2,1
3	Мобильные устройства	0,4	0,1	0,3
4	Кража и потеря оборудования	4,8	3,0	3,4
5	Текст, голос, видео	2,0	2,0	3,4
6	Бумажные документы	10,8	8,1	10,8
7	Электронная почта	8,5	2,0	4,1

* — первая половина года

Источник: Отчеты компании Infowatch и Solar Jsoc (https://www.infowatch.ru/report2018_half и https://vc.ru/flood/46212-issledovanie-sotrudniki-kompaniy-stanovyatsya-prichinoy-utechek-dannyh-vdvoe-chashche-chem-hakery)

Основным каналом утечки информации, по-прежнему, остаются информационные сети и технологии — утечки через Интернет (на уровне 69 %), а также бумажные документы (чуть больше 10 %). Существенное снижение отмечается по отношению к таким каналам утечки, как съемные носители (с 4,1 до 2,1), кража и потеря оборудования (с 4,8 до 3,4), и электронная почта (с 8,5 до 4,1).

В следующей таблице приведены данные о распределении утечек по типам информации.

Таблица 3.21

Распределение утечки данных по типам информации

№ п\п	Типы информации	2016	2017*	2018*
1	Персональные данные	85,6	65,8	69,0
2	Платежная информация	7,3	26,8	21,3
3	Государственная тайна	1,7	4,0	5,3
4	Коммерческая тайна	5,4	3,4	4,4

*- первая половина года

Источник: Отчеты компании Infowatch и Solar Jsoc (https://www.infowatch.ru/report2018_half и https://vc.ru/flood/46212-issledovanie-sotrudniki-kompaniy-stanovyatsya-prichinoy-utechek-dannyh-vdvoe-chashche-chem-hakery)

Чаще всего в открытый доступ попадают персональные данные (утечки составляют 85,6 % в 2016 году и 69,0 % в 2018 году). На втором месте утечки платежной информации (значительный рост с 7,3 % в 2016 году до 21,3 % в 2018 году). На государственную и коммерческую тайну приходится 5,3 % и 4,4 % в первой половине 2018 году.

Данные, характеризующие количественные оценки утечки, приведены в следующей таблице.

Таблица 3.22

Самые известные утечки данных за всю историю

№ п\п	Компания	Взломанные учетные записи	Дата взлома
1	Yahoo	3 млрд	Август 2013 г.
2	Marriott	500 млн	2014–2018 г.г.
3	Yahoo	500 млн	После 2014 г.
4	Adult FriendFinder	412 млн	Октябрь 2016 г.
5	MySpace	360 млн	Май 2016 г.
6	Under Armor	150 млн	Февраль 2018 г.
7	Equifax	145,5 млн	Июль 2017 г.
8	EBay	145 млн	Май 2014 г.
9	Target	110 млн	Ноябрь 2013 г.
10	Heartland Payment Systems	Более 100 млн	Май 2008 г.
11	LinkedIn	100 млн	Июнь 2012 г.

Окончание таблицы 3.22

№ п\п	Компания	Взломанные учетные записи	Дата взлома
12	Rambler.ru	98 млн	Февраль 2012 г.
13	TJX	94 млн	2003–2004 г.г.
14	AOL	92 млн	2004 г.
15	MyHeritage	92 млн	Октябрь 2017 г.
16	Sony PlayStation Network	77 млн	Апрель 2011 г.
17	JP Morgan Chase	83 млн	Июль 2014 г.
18	Tumblr	65 млн	Февраль 2013 г.
19	Uber	57 млн	После 2016 г.
20	Home Depot	53 млн	Апрель 2014 г.
21	Facebook	50 млн	Июль 2017 г.

Источник: Nicolas Rivero. The biggest data breaches of all time, ranked https://qz.com/1480809/the-biggest-data-breaches-of-all-time-ranked/

В следующей таблице приведены данные, характеризующие самые значительные взломы и утечки данных в 2017 году.

Таблица 3.23

Самые большие взломы и утечки данных в 2017 году

Цель	Объект компрометации	Вектор атаки
TSA	Тысячи документов	Резервные диски
Verizon	14 млн записей подписчиков	Незащищенный сторонний сервер хранения данных Amazon S3
NSA	Более 100 Гб данных военной разведки	Образ виртуального диска
Equifax	143 млн персональных данных потребителей	Незащищенная web-уязвимость
Bell Canada	1,9 млн записей клиентов (частичная утечка после невыплаты выкупа)	Нет данных
Freedom Hosting	данные на скомпрометированных серверах Dark Web	Повышение системных привилегий

Продолжение таблицы 3.23

Цель	Объект компрометации	Вектор атаки
Handbrake	Инфицирование трояном удаленного доступа	Вредоносная программа для кражи паролей
HipChat	информация об учетной записи пользователя, некоторых сообщениях и контент	Облачное приложение (уязвимость сторонней библиотеки)
Cloudflare	данные клиентов из Uber, 1Password и OKCupid	Утечка данных SSL с пограничных серверов
Wonga	данные клиентов из 270 000 аккаунтов	Нет данных
PoliceOne	данные об 715 000 аккаунтов (взломаны в 2015 году, выставлены в 2017 году)	Нет данных
[multiple, including UK NHS]	> 300 000 компьютеров заражены программой-вымогателем по всему миру	Червь WannaCry (на основе украденных хакерских утилит АНБ)
TigerSwan	Персональные данные будущих сотрудников	незарегистрированный сервер хранения AWS
Uber	данные о 57 млн пользователей (взломаны в 2016 году, выставлены в 2017 году)	Доступ к учетной записи AWS через частный репозиторий GitHub
Cellebrite	900 ГБ конфиденциальных корпоративных данных	Веб серверы фирмы Cellebrite
Sabre	данные об оплате и клиенте	Система бронирования SynXis (приложение SaaS)
ai.type	> 577 ГБ персональных данных о > 31 млн пользователей	Сервер базы данных без пароля
US Air Force	1000 документов USAF	незащищенный резервный диск
CIA	1000 взломанных документов	WikiLeaks
Virgin America	логин и пароли для 3120 сотрудников	Нет данных
Deloitte	конфиденциальные документы и электронные письма	учетная запись администратора почтового сервера (без 2FA)

Окончание таблицы 3.23

Цель	Объект компрометации	Вектор атаки
DaFont	информация об учетной записи для 699 000 пользователей	SQL-инъекция
Universities & US Federal agencies	Персональные данные, конфиденциальные документы, IP-адреса (потенциально)	SQL-инъекция
iCloud	доступ к 250м аккаунтам + требование выкупа	ранее скомпрометированные сторонние сервисы
Dallas Texas	общегородское зондирование всех аварийных сирен	атака радиопередачи
OneLogin	Информация о едином входе для тысяч клиентов	Доступ к экземпляру AWS через промежуточный хост

Источник: Charles Mclellan. Cybersecurity in 2018: A roundup of predictions. URL: http://www.techproresearch.com/article/cybersecurity-in-2018-a-roundup-of-predictions/

Кибернетические (целевые) атаки

Проанализируем содержание данного термина. Специалисты по информационной безопасности по-разному трактуют термин advanced persistent threat (APT). Среди вариантов: «расширенные постоянные угрозы»; «продвинутые», «развитые», «сложные», «целевые», «целенаправленные» и «таргетированные» угрозы. Эксперты Positive Technologies определяют APT как хорошо организованную, тщательно спланированную кибератаку, направленную на конкретную компанию или целую отрасль. В ходе нее злоумышленник получает несанкционированный доступ к сети, закрепляется в инфраструктуре и надолго остается незамеченным. За такими атаками, как правило, стоят APT-группировки, имеющие значительные финансовые ресурсы и технические возможности [58,59].

Рассмотрим классификацию кибернетических атак, приведенную в следующей таблице [44,46].

Таблица 3.24

Классификация кибератак

№	Категория атак	Описание атаки	Под-атаки
1	Вредоносная программа (malware)	Вредоносное программное обеспечение, используемое для запуска определенной атаки в компьютерные системы	Adware, Spyware, Virus, Worm, Trojan, Rootkit, Backdoors, Key loggers, Rogue Security Software, Ransomware, Browser Hijacker, и т.д.
2	Сетевая атака	Активный или пассивный мониторинг компьютерных коммуникаций и сетевого трафика	Passive, Active, Distributed, Insider, Close-in, Phishing, Hijacking, Spoofing, Buffer overflow, Exploit, Password attack, и т.д.
3	Сетевые вторжения	Любая несанкционированная деятельность в компьютерных сетях	Asymmetric routing, Buffer overflow, Protocol specific attacks, Traffic flooding, Trojans, Worms, и т.д.
4	Атаки социальной инженерии	Используя социальные сети и телефонные звонки, злоумышленники применяют человеческие психологические трюки, чтобы заставить пользователей предоставлять доступ к конфиденциальной информации	Phishing, Pre-texting, Baiting, Quid Pro Quo, Tailgating, и т.д.
5	Кибершпионаж	Отслеживание конфиденциальной информации пользователя или организации без их разрешения	Industrial espionage, Nation-State espionage, Economic espionage, Corporate espionage, Information theft and sabotage
6	Киберразведка	После обнаружения слабых мест в сетевых системах и службах, злоумышленник собирает конфиденциальную информацию	Internet information lookup, Ping sweeps, Port scans, Packet sniffers

Окончание таблицы 3.24

№	Категория атак	Описание атаки	Под-атаки
7	Атаки доступа к сети	Выявляя вредоносные действия в сетевой аутентификации, FTP и веб-сервисах, злоумышленник получает доступ к сетевой системе для получения конфиденциальной информации	Eavesdropping, Data modification, Identity spoofing, Password-based, Denial of service, man in the middle attack, Compromised key attack, Sniffer attack, Application layer Attack, Trust exploitation, и т.д.
8	Кибертерроризм	Использование Интернета для электронной террористической деятельности, такой как, крупномасштабное нарушение работы компьютерных сетей, высококлассных национальных компонентов, критически важных национальных инфраструктур или важных деловых операций	Sabotage, Website defacement and Denial of service, Destruction of critical physical infrastructures, и т.д.
9	Кибервойна	Серьезный сбой в национальной критической и очень важной Инфраструктуре за счет злонамеренного использования цифровой информации	Disruption of nation's public services, Financial Institutions, Industrial espionage, blocking military and civilian responders, и т.д..

Источник: [44,46].

Анализ данных, приведенных в таблице, свидетельствует об использовании большого набора механизмов нанесения ущерба информационным системам.

Несмотря на относительную новизну целевых атак на информационные ресурсы, специалисты выделяют несколько этапов в их развитии, которые представлены в следующей таблице.

Таблица 3.25

Поколения кибератак

Поколение	Временной интервал	Средства нападения
1-е поколение	80-е годы	Компьютерные вирусы
2-е поколение	90-е годы	Сетевые угрозы
3-е поколение	2000 годы	Прикладные угрозы
4-е поколение	2010	Полезная нагрузка
5-е поколение	Настоящее время	Мега-угрозы

Источник: Vijini Wickramanayake (2017). 5TH GENERATION CYBER ATTACKS. https://www.cyberonsecurity.no

В следующей таблице приведено описание целевых кибератак (АТР), нацеленных на интересы ЕС.

Таблица 3.26

Список целевых кибератак, нацеленных на интересы ЕС

Инцидент, угроза	Предполагаемый правительственный спонсор	Год	Затрагиваемые интересы стран ЕС	Примечания
APT 10	Китай	2017	Великобритания, Франция, Швеция, Финляндия	Китайская группа APT 10 (или Red Apollo) осуществляет кражу информации, характеризующую интеллектуальную собственность и других конфиденциальных данных из нескольких информационных систем сервис-провайдеров относительно энергетических, финансовых, технологических и медицинских фирм
OPERATION BUGDROP	Россия	2017	Австрия	Американскими и европейскими СМИ сообщается, что операция BugDrop была спонсирована Россией для сбора информации в различных областях, включая данные о критической инфраструктуре, средствах массовой информации и научных исследованиях, включая аудиозаписи разговоров, скриншоты, документы и пароли
"OCEAN LOTUS"	Вьетнам	2015	Германия	Ocean Lotus — группа, поддерживаемая правительством Вьетнама, которая реализовала доступ для получения информации в целях ослабления конкурентных преимуществ (данные частного сектора, правоохранительных органов, кражи интеллектуальной собственности и мер по борьбе с коррупцией) иностранных компаний, проявляющих интерес к потребительским товарам из Вьетнама, производству, гостиничному бизнесу, технологической инфраструктуре и банковскому сектору

Продолжение таблицы 3.26

Инцидент, угроза	Предполагаемый правительственный спонсор	Год	Затрагиваемые интересы стран ЕС	Примечания
UPS	Китай	2015	Великобритания	Фишинговая операция, спонсируемая Китаем. Цель — информация аэрокосмических, оборонных, строительных, инженерных, технологических, телекоммуникационных и транспортных фирм.
EMISSARY PANDA	Китай	2015	Великобритания, Франция	Emissary Panda — китайская операция, направленная на фирмы авиакосмические, автомобильные, технологические и энергетические и другие сектора производства и обороны, а также получение политической и коммерческой информации о конкурентах, инноваций, финансовых, ценовых возможностях и планах развития
ÄXIOM	Китай	2014	Великобритания, Германия, Нидерланды, Бельгия, Италия	Китайская группа, нацеленная на организации, имеющие отношение к стратегическим технологиям, телекоммуникациям, инфраструктуре, экологической и энергетической политике для развития конкурентной борьбы и избавления от иностранных технологий в рамках специального плана
CARETO	Испания	2014	Великобритания, Франция, Испания, Германия, Польша	Возможно, спонсируется Испанией, и нацелена на деятельность энергетических и нефтегазовых компаний, научно-исследовательские институты и частные инвестиционные компании. Создана и использовалась сложная программа, способная перехватывать и собирать важную информацию по каналам связи
CROUC HING YETI	Россия	2014	Испания, Германия, Франция, Италия, Ирландия, Польша	Осуществлял слежку за рядом предприятий различных секторов экономики (фармацевтика, автомобильная, сетевая инфраструктура, ИТ). Имел потенциал для совершения диверсий. Приписывается поддержке РФ

Окончание таблицы 3.26

Инцидент, угроза	Предполагаемый правительственный спонсор	Год	Затрагиваемые интересы стран ЕС	Примечания
PEOPLE'S LIBERATION ARMY	Китай	2014	SolarWorld	Пять офицеров Народно-освободительной армии Китая были обвинены властями США в нацеливании предприятия металлургической, атомной и солнечной энергетики, в том числе на американскую дочернюю компанию немецкой фирмы SolarWorld. Цель — кража информации для использования в конкурентных целях
PEOPLE'S LIBERATION ARMY 61398	Китай	2013	Великобритания, Франция, Бельгия, Люксембург	Подразделение 61398 или APT1, было нацелено на деятельность 141 компаний в 20 основных отраслях, в том числе ИТ, транспорт, технологии, финансовые услуги, инжиниринг, химикаты, энергетика и здравоохранение, которые связаны со стратегическими приоритетами Китая
COMPROMISE OF EADS (AIRBUS) AND THYS-SENKRUPP	Китай	2013	EADS/Airbus ThyssenKrupp	Целью была компания ThyssenKrupp из-за позиции основного игрока в мире производства стали. Кража интеллектуальной собственности у EADS (сейчас Airbus), а также планов проектирования, аэродинамических расчетов и смет
NITRO ATTACKS	Китай	2011	Великобритания, Германия, Чехия, Нидерланды, Финляндия, Франция	Спонсируемые Китаем атаки Nitro касались деятельности компаний по разработке и производству химических веществ и интеллектуальной собственности (проектная документация, формулы и производственные процессы)

Источник: Hosuk Lee-Makiyama. Stealing Thunder. ECIPE, No. 2/18. URL: https://ecipe.org/wp-content/uploads/2018/02/ECIPE_Occasional0218_HLM_V7.pdf [60].

Кража персональных данных

Кража личных данных включает такие действия, как перехват идентификационных данных, кредитных карт, логинов и паролей.

В мае 2018 года Европейский Союз ввел обновлённые правила обработки персональных данных, установленные Общим регламентом по защите данных (Регламент ЕС 2016/679 от 27 апреля 2016 г. или GDPR — General Data Protection Regulation) [61]. Данный регламент, имеющий прямое действие во всех 28 странах ЕС, призван заменить рамочную Директиву о защите персональных данных 95/46/ЕС от 24 октября 1995 года. Важным нюансом GDPR является экстерриториальный принцип действия новых европейских правил обработки персональных данных. Новый регламент предоставляет резидентам ЕС инструменты для полного контроля над своими персональными данными. В частности, ужесточается ответственность за нарушение правил обработки персональных данных: по GDPR штрафы достигают 20 миллионов евро или 4 % годового глобального дохода компании.

Регламент определяет персональные данные, как любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу (субъект данных), по которой прямо или косвенно можно его определить. К такой информации относится в том числе имя, данные о местоположении, онлайн идентификатор или один, или несколько факторов, характерных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности этого физического лица. Данное определение широкое и достаточно четко дает понять, что даже IP адреса также могут быть персональными данными.

Общий подход к обработке персональных данных сформулирован в виде 6 основных принципов:

1) Законность, справедливость и прозрачность. Персональные данные должны обрабатываться законно, справедливо и прозрачно. Любую информацию о целях, методах и объёмах обработки персональных данных следует излагать максимально доступно и просто.

2) Ограничение цели. Данные должны собираться и использоваться исключительно в тех целях, которые заявлены компанией (онлайн-сервисом).

3) Минимизация данных. Нельзя собирать личные данные в большем объёме, чем это необходимо для целей обработки.

4) Точность. Личные данные, которые являются неточными, должны быть удалены или исправлены (по требованию пользователя).

5) Ограничение хранения. Личные данные должны храниться в форме, которая позволяет идентифицировать субъекты данных на срок не более, чем это необходимо для целей обработки.

6) Целостность и конфиденциальность. При обработке данных пользователей компании обязаны обеспечить защиту персональных данных от несанкционированной или незаконной обработки, уничтожения и повреждения.

Специалисты по информационной безопасности высказывали противоречивые мнения относительно эффективности использования данного регламента. В первую очередь, никто не ставит под сомнение благие намерения законодателей или необходимость того, чтобы компании были более осторожны с конфиденциальной информацией, которой они обладают о клиентах, пациентах и других людях, с которыми они регулярно общаются. Несмотря на то, что положения в GDPR действительно помогают повысить эффективность защиты персональных данных, они также создали новые возможности для использования хакерами и похитителями личных данных этих данных [62].

GDPR установил набор руководящих принципов для управления сбором и хранением данных о потребителях и частной собственности. Многое из этого относится к личной информации, предоставляемой физическими лицами. Участниками этого процесса являются все структуры и организации, которые так или иначе, обрабатывают персональные данные физических лиц, в том числе банковские учреждения, страховые компании, инвестиционные службы или медицинское учреждение, государственные органы, некомерческие организации, и т.д. Основная цель заключается в обеспечении надлежащей защиты и исключения возможности третьей стороной несанкционированного использования личной информации сотрудников, клиентов

и пациентов этих организаций. Данный регламент устанавливает ключевые области безопасности данных: согласие на сбор и хранение личных данных; уведомление в случае взлома данных; шифрование данных, которое защищает личную информацию в случае нарушения; доступ к личной информации для проверки точности (целостности) и для установки ограничений на предполагаемое использование. Некоторые положения в рамках GDPR были отозваны.

Следует отметить, что требования GDPR разработаны таким образом, что они являются обязательными не только для структур, регистрированных в странах Европейского Союза, но и за её пределами. Например, если организация владеет филиалами в других странах, они обязаны внедрить требования регламента. Более, если европейская организация, в результате экономической деятельности, передает персональные данные, тогда она должна убедиться, что партнер соблюдает требования GDPR. Таким образом, несмотря на то, что на первый взгляд GDPR является документом обязательным на территориях стран Европейского Союза, его требования применимы за его пределы.

Если ранее выявлялись случаи утечки информации, они не подлежали большой огласки. После принятия GDPR такие случаи, в обязательном порядке, должны быть сообщены. Анализ доступной информации помог выделить важные заключения.

В январе 2020 года юридическая фирма DLA Piper опубликовала обзор данных о нарушениях, связанных с реализацией GDPR в части утечки персональных данных [63] в 28 странах-членах ЕС, а также Норвегии, Исландия и Лихтенштейна. Приведем основные положения данного отчета.

С 25 мая 2018 года (время ввода обновленного GDPR в действие) по 20 января 2020 года в общей сложности было отмечено 160921 случай нарушения данного закона, получивших уведомление надзорными органами по защите данных в рамках Европейской Экономической Зоны. За период с 25 мая по 27 января 2019 года в среднем было отмечено 247 уведомлений о нарушениях в день. За период с 28 января 2019 года по 20 января 2020 количество сообщений в день о нарушениях составило уже 278 или рост на 12,6 %. Общее количество нарушений персональных данных приведено в следующей таблице.

Таблица 3.27

Общее количество нарушений обработки персональных данных

№ п\п	Страна	Общее количество нарушений персональных данных, за период с 25 мая 2018 года по 27 января 2020 года	Количество нарушений персональных данных, с 28 января 2019 года по 27 января 2020 года	Кол. нар. персональных данных с 25 мая 2018 года по 27 января 2019 года	Рейтинг уведомлений о нарушениях в расчете на душу населения	Общая стоимость штрафов GDPR, 25 мая 2018 по 7 января 2020 года в евро
1	Нидерланды	40647	25247	15400	147,2	460 000
2	Германия	37636	25036	12600	31,12	24 574 525
3	Великобритания	22181	11581	10600	17,79	320 000
4	Ирландия	10516	6716	3800	132,52	-
5	Дания	9806	6706	3100	115,43	360 000
6	Польша	7478	5278	2200	13,74	947 345
7	Швеция	7333	4833	2500	48,14	53 639
8	Финляндия	6355	3938	2500	71,11	51 100 000
9	Франция	3459	2159	1300	3,2	-
10	Норвегия	2824	2004	820	37,31	406 210
11	Италия	1886	1276	610	2,05	11 550 000
12	Словения	1845	1105	740	52,55	-
13	Испания	1698	1028	670	2,08	1 381 060
14	Австрия	1644	1964	580	12,1	18 107 700
15	Бельгия	1332	912	420	7,88	39 000

Окончание таблицы 3.27

№ п\п	Страна	Общее количество нарушений персональных данных, за период с 25 мая 2018 года по 27 января 2020 года	Количество нарушений персональных данных, с 28 января 2019 года по 27 января 2020 года	Кол. нар. персональных данных с 25 мая 2018 года по 27 января 2019 года	Рейтинг уведомлений о нарушениях в расчете на душу населения	Общая стоимость штрафов GDPR, 25 мая 2018 по 7 января 2020 года в евро
16	Венгрия	749	479	270	4,87	198000
17	Чехия	720	430	290	4,03	291717
18	Румыния	668	408	260	1,9	329500
19	Люксембург	545	345	200	56,97	-
20	Исландия	338	313	25	91,15	-
21	Мальта	239	139	100	31	35500
22	Греция	232	162	70	1,5	550000
23	Литва	222	118	105	4,18	67500
24	Эстония	188	121	67	9,74	-
25	Латвия	173	117	55	6,13	168930
26	Кипр	94	59	35	4,8	151900
27	Лихтенштейн	30	15	15	39,18	-
28	Болгария	-	-	-	-	3156500
29	Португалия	-	-	-	-	424000
30	Словакия	-	-	-	-	132600

Источник: Рассчитано по DLA Piper GDPR data breach survey: January 2020. URL: https://www.dlapiper.com/en/asiapacific/insights/publications/2020/01/gdpr-data-breach-survey-2020/

Отмечается четкая тенденция роста, хотя подробная информация об утечках не публикуется. Лидерами утечек персональных данных признаны Нидерланды, Германия и Великобритания.

В то же время, феномен кражи и торговли персональными данными является еще более масштабным, если не ограничивать анализ только странами Европейского Союза. Более полную картину можно получить при анализе ситуации в целом, по всем странам. Данный анализ, в настоящее время, видится авторами почти невозможным, так как не все страны задаются задачей обеспечить безопасность персональных данных, либо не все страны публикуют и ведут учет случаев компрометации персональных данных. Анализ, в данном случае, возможен только в результате проведения аналитических действий.

Криптовалюты, криптобиржи и криптообменники

Относительно новым сегментом ТЦЭ является криминальная деятельность по отношению и с использованием средств управления криптовалютами. Эта деятельность вызвана и привлекает внимание киберпреступников за счет вливания огромных средств в эту область, а также низким уровнем регламентирования на уровне государств. Высокая рыночная капитализация отдельных криптовалют привлекает хакеров (по состоянию на 11.03.22 было зарегистрировано 12811 криптовалют и 571 криптобирж). В качестве примера используем данные, приведенные в следующей таблице.

Таблица 3.28

Состояние некоторых криптовалют на 11.03.2022

№ п.п.	Наименование криптовалюты	Цена $	Капитализация (Долл.)
1	Bitcoin	39 269,00	744 870 146 121
2	Ethereum	2 619,18	314 191 542 797
3	Tether	1,00	80 063 330 189
4	BNB	374,28	62 918 741 505
5	USD Coin	1,00	52 559 181 569
6	Terra	97,01	36 438 500 406
7	XRP	0,74	35 510 517 474
8	Solana	82,66	26 703 675 955
9	Cardano	0,81	25 912 948 413
10	Avalanche	75,12	20 017 318 032

Источник: Курс криптовалют к доллару на 11.03.22. URL: https://coinmarketcap.com/

Одной из относительно новых видов атак является организация нападения на криптообменники. Специалисты Group-IB провели анализ атак на криптовалютные биржи за последние два года и выявили общие потери в сумме 882 млн $. В отчете указывается, что в 2019 году криптовалютные биржи станут для агрессивных хакерских групп новой целью и их усилия будут перенесены с атак на коммерческие банки. Но в качестве целей выдвигаются не только биржи-криптообменники, но и криптовалютные компании, организующие запуск ICO, сбор средств и предусматривающие продажу токенов частным инвесторам.

По прогнозам, капитализация рынка криптовалют в 2022 году составит 4 трлн дол. [65]. Наибольшее внимание инвесторов и трейдеров приковано к тем криптовалютам, которые имеют самую высокую капитализацию. Несмотря на то, что сравнение криптовалют по данному показателю некоторые аналитики считают не полностью объективным, именно капитализация является главным фактором, определяющим интерес к отдельной монете со стороны не только покупателей, но и кибермошенников. Для обзора действий криминала на рынке криптовалют, используем данные отчетов Group-IB (https://www.group-ib.ru) — одного из ведущих разработчиков решений для детектирования и предотвращения кибератак, выявления мошенничеств и защиты интеллектуальной собственности в сети Интернет. Group-IB обнаружила, что более 10 % средств, привлеченных во время ICO, были украдены. Речь идет о периоде с 2017 года по сентябрь 2018 года. Более половины украденных у ICO средств были связаны с фишинговыми атаками. Целью хакерских групп была не только сама виртуальная валюта, но и списки инвесторов, заинтересованных в ICO, для реализации в будущем таких действий, как шантаж или целевые фишинговые атаки. Примеры успешных атак на криптообменники и соответствующие потери приведены в следующей таблице.

Таблица 3.29

Примеры успешных кибератак на криптообменники

Дата	Наименование проекта	Страна	Криминальная группа	Потери в криптовалюте	Потери в $
Февраль 2017 г.	Bithumb	Южная Корея	-	-	7 млн $
Апрель 2017 г.	YouBit	Южная Корея	-	-	5,6 млн $
Апрель 2017 г.	Yapizon	Южная Корея	Lazarus	3,816 BTC	5,3 млн $
Апрель 2017 г.	Ether Delta	-	Неизвестна	-	225 K$
Август 2017 г.	OKEx	Гонконг	Неизвестна	-	3 млн $
Сентябрь 2017 г.	Coinis	Южная Корея	Lazarus	-	-
Декабрь 2017 г.	YouBit	Южная Корея	Lazarus	17 % всех активов	-
Январь 2018 г.	Bitstamp	Luxemburg	Неизвестна	18.000 BTC	5 млн $
Январь 2018 г.	Coincheck	Япония	Lazarus	532.000.000 NEM	534 млн $
Февраль 2018 г.	Bitgrail	Италия	Неизвестна	17.000.000 NANO	170 млн $
Июнь 2018 г.	Bithumb	Южная Корея	Lazarus	-	32 млн $
Июнь 2018 г.	Coinrail	Южная Корея	Неизвестна	-	37 млн $
Июнь 2018 г.	Bancor	-	Неизвестна	-	23 млн $
Сентябрь 2018 г.	Zaif	Япония	Неизвестна	-	60 млн $
				Итого	882 млн $

Источник: Report: Cryptocurrency Exchanges Lost $882 Million to Hackers. URL: https://www.bankinfosecurity.com/cryptocurrency-exchanges-lost-882-million-to-hackers-a-11624

Анализ данных, приведенных в таблице, позволяет сделать предварительные выводы. Во-первых, из 14 событий (с февраля 2017 г. по сентябрь 2018 г.) 7 успешных атак были реализованы в Южной Корее, 2 в Японии и по 1 атаке в Гонконге, Люксембурге и Италии. То есть из 14 атак 10 приходятся на Юго-Восточную Азию (71 %).

Во-вторых, единственной криминальной группой, которой приписываются успешные атаки, является Lazarus (5 атак из 14, то есть 36 %). Хакерская группировка Lazarus (она же Hidden Cobra) получила известность после успешной атаки на информационные ресурсы Sony Pictures Entertainment (2014 год). Ее деятельность связывают с Северной Кореей (КНДР) и ей приписывают ряд успешных инцидентов, таких как, эпидемия Wannacry, атаками на коммерческкие банки в Мексике и Польше и другими фишинговыми атаками.

В-третьих, основной криптовалютой выступает биткойн (BTC), но встречаются и другие альтернативные криптовалюты. В частности, криптовалюта NEM и NANO. Японская криптобиржа Coincheck стала жертвой крупной хакерской атаки взлома 26 января 2018 года, в результате чего потеряла 523 миллиона монет NEM на сумму около $534 миллионов. Взлом коснулся только NEM. Поскольку причиной кражи стало отсутствие мер безопасности на самой бирже Coincheck, команда разработчиков NEM отказалась провести хардфорк, чтобы вернуть потерянные средства.

Увеличение интереса к криптовалютам породило развитие массовых атак на данные сервисы. Так, с 2016 по 2017 годы число скомпрометированных учетных записей пользователей криптобирж увеличилось на 369 %. В январе 2018 года количество инцидентов выросло на 689 % по сравнению со среднемесячным показателем 2017 года. Эксперты Group-IB провели анализ краж 720 пользовательских учетных записей 19 крупнейших криптовалютных бирж и установили, что лидерами по количеству жертв кибератак стали США, Россия и Китай, данные об этом приведены в следующей таблице.

Таблица 3.30

Распределение жертв криптобирж по странам

№ п\п	Страна	% украденных активов
1	США	34,3
2	Россия	10,5
3	Китай	5,0
4	Индонезия	4,5
5	Германия	3,6
6	Украина	2,8
7	Иран	2,8
8	Словакия	2,6
9	Гонконг	2,6
10	Вьетнам	2,4
11	Турция	2,4
12	Другие	11,1

Источник: Число взломанных аккаунтов на биткоинбиржах в начале 2018 года выросло на 689 %. URL: https://forklog.com/chislo-vzlomannyh-akkauntov-na-bitkoin-birzhah-v-nachale-2018-goda-vyroslo-na-689/

Эксперты Group-IB отмечают, что киберпреступники используют те же инструменты, использовавшиеся при атаках на коммерческие банки, ориентируют их на проведение взлома криптобирж, электронных кошельков и получения доступа к личным данным пользователей. В отчете «2018 Криптовалютные биржи. Анализ утечек учетных записей пользователей» указано, что по меньшей мере 5 из 19 криптобирж стали жертвами целенаправленных атак: Bitfinex, Bithumb, HitBTC, Huobi [66].

Таблица 3.31

Утечки и жертвы целенаправленных кибератак

Название биржи	Год	Торги 31.01.18 (в $)	Торговые пары	Число утечек	Инциденты с биржей
Binance	2017	2 222 672 484	252	39	Нет
Bit-Z	2016	236 374 114	69	2	Нет
Bitfinex	2012	1 881 119 042	103	48	Да
BitHumb	2013	1 783 489 020	12	1	Да
Bitstamp	2011	514 697 740	14	48	Да
Bittrex	2014	743 909 464	261	112	Нет
BTCC	2011	103 530 000	4	9	Нет
CEX.io	2013	53 713 354	23	95	Нет
Coinone	2014	222 211 947	9	3	Нет
Gate.io	2017	103 092 086	226	4	Нет
GDAX	2012	926 158 460	12	2	Нет
Gemeni	2014	474 980 277	3	19	Нет
HitBTC	2014	494 363 548	421	83	Да
Huobi	2013	1 256 939 172	171	10	Возможно
Kraken	2011	884 409 505	45	61	Нет
KuCoin	2017	157 142 723	212	2	Нет
OKEx	2014	2 701 097 580	422	5	Нет
Poloniex	2014	383 900 716	99	174	Да
Wex.nz	2017	69 440 237	35	3	Нет

Источник: 2018 Криптовалютные биржи. Анализ утечек учетных записей пользователей. URL: https://www.group-ib.ru/resources/threat-research/cryptocurrency-exchanges.html

В апреле 2019 года криптовалютная биржа Binance сообщила о том, что хакерам удалось за один день вывести более 7 тыс. биткойнов, а также похитить часть данных ее пользователей. Сумма украденных хакерами средств превышает $40 млн. Биржа подверглась «крупномасштабному взлому», причем все средства — более 7 тыс. биткойнов на сумму, превышающую $40 млн — были выведены в несколько этапов и переведены на один кошелек. Binance, одна из крупнейших в мире онлайн-сервисов обмена цифровых валют, была основана в 2017 году в Гонконге. Предоставляет платформу для торговли более чем 100 разных видов криптовалют. В начале 2018 года Binance была крупнейшей криптобиржей по объему капитализации собственной криптовалюты BNB. Ее капитализация составляет $2,9 млрд (7 место в мире). В первом квартале 2019 года прибыль Binance выросла на 66 % по сравнению с аналогичным отчетным периодом 2018 года.

Хакеры провели транзакцию так, что она не вызвала подозрений у системы защиты Binance, и та сработала лишь после завершения операции. Средства были выведены с так называемого горячего кошелька биржи, который всегда подключен к сети интернет, в отличие от «холодного кошелька», который работает автономно. В «горячих кошельках» хранится около 2 % имеющихся у криптобиржи запасов биткойна. Кроме того, хакерам, по-видимому, удалось похитить часть данных клиентов биржи, в частности, коды двухуровневой авторизации, необходимые для входа в пользовательский аккаунт на сайте Binance [67].

Хакерские атаки на криптобиржи превращаются в норму. Так, по данным отчета аналитической компании Chainalysis [68], получили распространение рискованные и незаконные сервисы, в том числе такие, как P2P-обмены, микшерные сервисы, высоко рискованные биржи и игровые площадки, даркнет-рынки, связанные с мошенничеством, похищением и отмыванием средств. Количество атак в 2019 году почти удвоилось по сравнению с 2018 годом (6 и 11, соответственно), а потери сократились с 875,5 млн дол до 282,6 млндол. Самый большой взлом в 2019 году был осуществлён против сингапурской криптобиржи Coinbene, которая потеряла $105 млн в токенах ERC-20. Далее

идут Upbit, Binance и BITPoint, у которых украли криптовалют на $49 млн, $40 млн и $32 млн соответственно.

При содействии криптобиржи Binance удалось задержать трех мошенников, предлагавших киберпреступникам отмывать добычу от шифровальщиков-вымогателей через два десятка «криптообменников» [69]. Киберполицейские, при поддержке операторов криптобиржи Binance, нейтрализовали банду кибермошенников, которые за два года отмыли около $42 млн через два десятка криминальных «обменников» — точек обналичивания криптовалют.

Группа, состоявшая из трех человек, начала деятельность в 2018 г. Злоумышленники активно рекламировали свои услуги на подпольных форумах, предлагая, в частности, конвертацию криптовалютных средств, полученных нелегальным образом (то есть, через кибератаки, вымогательство и т.д.), в реальные деньги. Судя по объему отмытых таким образом средств, услуги группировки пользовались большим спросом.

Подводя промежуточные итоги анализа программ-вымогателей, можно использовать данные, приведенные в отчете Международного Экономического форума за 2022 год, и отраженные в следующей таблице [70].

Таблица 3.32

Общая стоимость криптовалюты, полученной с помощью программ-вымогателей в 2013–2020 гг. (в млн $)

№ п.п.	Год	Стоимость криптовалюты (млн $)
1	2013	0,51
2	2014	1,11
3	2015	0,89
4	2016	17,78
5	2017	37,68
6	2018	27,3
7	2019	92,94
8	2020	406,34

Примечание: Включены следующие криптовалюты: BCH (Bitcoin Cash), BTC (Bitcoin), ETH (Ethereum), USDT (Tether).

Источник: The Global Risks Report 2022, 17th Edition, is published by the World Economic Forum. URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Анализ данных свидетельствует о резком росте объемов криптовалют, уплаченных за указанный интервал времени. Рост составил более 4000 %. В 2020 году был достигнут максимум и составил более 400 млн и можно высказать осторожный прогноз о возможном дальнейшем росте.

Следует выделить еще одну, немаловажную особенность криптовалют — получение взяток криптовалютой уже несколько лет пользуется огромной популярностью у чиновников и юристов. Такие сделки могут отслеживаться, но ни фактически, ни юридически их нельзя привязать к человеку. То есть формальных доказательств для следствия и суда априори получить невозможно. Более того, криптовалюта сразу оказывается за пределами государства, и конфисковать ее практически невозможно. Но при наличии интернета они все время остаются в распоряжение хозяина.

Заключение

Отмечаем, что теневая цифровая экономика, как социально-экономическое явление, представляет собой совокупность развитых, но подпольных, рынков информационных и коммуникационных технологий, обладает высоким интеллектуальным потенциалом, большим количеством материальных и финансовых средств и огромными экономическими возможностями. По своей структуре рынки неоднородны как с точки зрения объемов, так и перспектив нанесения ущерба личности, обществу и государству.

Цифровая экономика несёт с собой новые вызовы и риски, которые напрямую связаны с расширением области применения цифровых технологий в экономике частной жизни. В их числе выделяются следующие: снижаются возможности контроля цифровых сервисов и увеличиваются возможности для реализации широкого спектра противозаконных действий; повышаются риски утечек информации, влияния на работу оборудования (например, бытовые приборы, кардиостимуляторы и др.); появляются совершенно новые угрозы, связанные с взрывным ростом значимости социальных сетей в жизни общества и развитием технологии Интернета вещей (IoT).

Собранный и проанализированный материал, по мнению авторов, не исчерпывает многообразия проблем, связанных с определением роли и места теневой информационной экономики в процессах трансформации. Предстоит сделать еще многое, в том числе:

— внести коррективы в определение категории ТЦЭ;

— определить экономическую и технологическую природу действий, попадающих под определение ТЦЭ;

— построить интегрированную бизнес-модель процессов ТЦЭ с выделением этапа монетизации;

— проанализировать возможность появления новых сегментов и обосновать их удельный вес в ТЦЭ.

Ощущается острая нехватка концепции противостояния современным угрозам, в том числе ТЦЭ, как одной из современных угроз личности, обществу, государству. Данная концепция должна включать кардинальное изменение законодательной базы и создание условий, при которых реализация и сокрытие всех видов незаконной деятельности станут не только уголовно наказуемой, но и экономически невыгодными.

Обязательным условием является развитие сотрудничества на государственном, региональном и международным уровнях с целью противостояния киберпреступлениям и кибертерроризму.

Литература к главе 4:

1. Adrian T.H. Kuah, Roberto Dillon (2021). Digital Transformation in a Post-COVID World. Sustainable Innovation, Disruption, and Change. CRC Press. ISBN: 978–1–003–14871–5 DOI: 10.1201/9781003148715.
2. Levi West (2020). The Coronavirus Cybersecurity Survival Guide. Top Tips to Protect You from a Cyber Attack. ASIN: B086JBZ3BX.
3. Robert Slade (2021). Cybersecurity Lessons from CoVID-19. CRC Press. ISBN: 978–1–003–13667–5.
4. Steve Morgan (2021). Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2021 To 2025. — URL: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/ (дата обращения: 03.06.2022).

5. Mathew J. Schwartz (2021). Cyber Extortion Thriving Thanks to Accellion FTA Hits. –— URL: https://www.databreachtoday.com/blogs/cyber-extortion-thriving-thanks-to-accellion-fta-hits-p-3024/ (дата обращения: 03.06.2022).
6. Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound. — URL: https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound/ (дата обращения: 03.06.2022).
7. 2021 Ransomware Threat Report. — URL: https://www.darktrace.com/en/resources/ds-ransomware.pdf (дата обращения: 03.06.2022).
8. Gyomai, Peter van de Ven. The Non-Observed Economy in the System of National Accounts. — URL: https://www.oecd.org/sdd/na/Statistics%20Brief%2018.pdf (дата обращения: 03.06.2022).
9. Measuring the Non-Observed Economy. A Handbook. http://www.oecd.org/sdd/na/1963116.pdf (дата обращения: 03.06.2022).
10. Marcena Hunter (2018). Capturing the proceeds of crime in illicit financial flow models. The Global Initiative Against Transnational Organized Crime. — URL: https://globalinitiative.net/wp-content/uploads/2018/06/TGIATOC–Illicit-financial-Flows-report-1941-hi-res-2–1.p (дата обращения: 03.06.2022).
11. Friedrisch Schneider (2017). Restricting or Abolishing Cash: An Effective Instrument for Fighting the Shadow Economy, Crime and Terrorism? — URL: https://www.bundesbank.de/Redaktion/EN/Downloads/Tasks/Cash_management/Conferences/2017_04_24_schneider.pdf?__blob=publicationFile (дата обращения: 03.06.2022).
12. Cost of Cyber Crime Study: Global Benchmark Study of Global Companies. — URL: http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf (дата обращения: 03.06.2022).
13. 2016: Current State of Cybercrime. — URL: https://www.rsa.com/content/dam/rsa/PDF/2016/05/2016-current-state-of-cybercrime.pdf (дата обращения: 03.06.2022).
14. 2017 Cyber Attack Trends and New Global Cyber Threats — URL: https://pages.checkpoint.com/global-cyber-attack-trends-2017.html?utm%20source=research&utm%20medium=cp-website&%20utm%20campaign=CM%20WR%2018Q1%20WW%20Threat%20Intelligence%20Trends%20Report%202017%20H2 (дата обращения: 03.06.2022).

15. Adjusting the Lens on Economic Crime. — URL: https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf (дата обращения: 03.06.2022).
16. Comprehensive Study on Cybercrime. — URL: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (дата обращения: 03.06.2022).
17. Cybercrimes/e-Crimes: Assessment Report. ITU2012. — URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/HIPCAR%20Assessment%20Cybercrimes.pdf (дата обращения: 03.06.2022).
18. Cyber security. Report. Special Eurobarometer 423. — URL: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs423en.pdf (дата обращения: 03.06.2022).
19. Hackmageddon. Information Security Timelines and Statistics. — URL: https://www.hackmageddon.com (дата обращения: 03.06.2022).
20. Global Risks Report 2018. 13th Edition. — URL: http://www3.weforum.org/docs/wefgrr18report.pdf (дата обращения: 03.06.2022).
21. Jason Williams. (2019). Cybercrime as an Economy. — URL: https://thefintechtimes.com/cybercrime-economy/ (дата обращения: 03.06.2022).
22. Барсукова, С.Ю. Неформальная экономика: Экономико-социологический анализ / Гос. ун-т — Высшая школа экономики. — М.: Изд. дом ГУ ВШЭ, 2004.— 448 с.
23. Латов В. Социальные функции теневой экономики в институциональном развитии постсоветской России: Дис. д-ра соц. н. / Высшая Школа Экономики. — Тюмень, 2008. URL: https://fdp.hse.ru/data/327/566/1238/avtoref_Latov.pdf (дата обращения: 03.06.2022).
24. Родионов И., Гиляревский Р., Цветкова В., Залаев З. Рынок информационных услуг и продуктов. — М.: МК-Периодика, 2002.— 552 с.
25. Филиппова Т. Деактивация теневой экономики в России. — Томск: STT, 2013.— 254 с.
26. Boehme R. Vulnerability Markets. What is the economic value of a zero-day exploit? Technische Universitat Dresden, Institute for System Architecture. — URL: https://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf дата обращения: 03.06.2022).

27. Gaspareniene L., Remeikiene R., Schneider F. The factors of digital shadow consumption. Intellectual Economics 9 (2015) 108–119. — URL: https://reader.elsevier.com/reader/sd/pii/s1822801115300072?token=c49e382daee81b81db17c158517a07065f311a7bf3458dc7d029a8a0d597d40ec9325e32b283fa3fa4020975e69fbed6&originregion=eu-west-1&origincreation=20220603114111 (дата обращения: 03.06.2022).
28. Rentrop C., Zimmermann S. Shadow IT Evaluation Model. Proceedings of the Federated Conference on Computer Science and Information Systems. — URL: https:// https://annals-csis.org/proceedings/2012/pliks/394.pdf (дата обращения: 03.06.2022).
29. Krebs B. Crimeware Author Funds Exploit Buying Spree. Krebs on Security. — URL: http://krebsonsecurity.com/2013/01/crimeware-author-funds-exploit-buying-spree/ (дата обращения: 03.06.2022).
30. Schneider F. Implausible Large Differences in the Sizes of Underground Economies in Highly Developed European Countries? A Comparison of Different Estimation Methods. — URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2999761 (дата обращения: 03.06.2022).
31. Stu Sjouwerman. CYBERHEIST: The biggest financial threat facing American businesses since the meltdown of 2008. — URL: https://cdn2.hubspot.net/hubfs/241394/Cyberheist_2016-B.pdf (дата обращения: 03.06.2022).
32. F. Korzeniowski. SECURITOLOGIA. Nauka o bezpieczeństwie człowieka i organizacji społecznych. — EAS Kraków, 2016.
33. A Framework for Programming and Budgeting for Cybersecurity. — URL: https://www.rand.org/content/dam/rand/pubs/tools/TL100/TL186/RAND_TL186.pdf (дата обращения: 03.06.2022).
34. Markets for Cybercrime Tools and Stolen Data. https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf (дата обращения: 03.06.2022).
35. A Cyberworm that Knows no Boundaries. — URL: https://www.rand.org/content/dam/rand/pubs/occasional_papers/2011/RAND_OP342.sum.pdf (дата обращения: 03.06.2022).
36. Глава ООН рассказал о своих приоритетах на 2020 год. — URL: https://news.un.org/ru/story/2020/01/1371131 (дата обращения: 03.06.2022).
37. HOWARD J. SHATZ (2020). Economic Competition in the 21st Century. — URL: https://www.rand.org/pubs/research_reports/RR4188.html (дата обращения: 03.06.2022).

38. Введение в «Цифровую» экономику / А.В. Кешелава В.Г. Буданов, В.Ю. Румянцев др.; под общ. ред. А.В. Кешелава; гл. «цифр.» конс. И.А. Зимненко. — ВНИИГ, 2017.— 28 с. — URL: http://spkurdyumov.ru/uploads/2017/07/vvedenie-v-cifrovuyu-ekonomiku-na-poroge-cifrovogo-budushhego.pdf (дата обращения: 03.06.2022).
39. Ursula von der Leyen's message to Davos Agenda: Full transcript. — URL: https://www.weforum.org/agenda/2021/01/ursula-von-der-leyen-european-commission-davos-agenda/?utm_source=sfmc&utm_medium=email&utm_campaign=2740992_Agenda_weekly-29January2021&utm_term= &emailType=Newsletter (дата обращения: 03.06.2022).
40. Глобальное исследование утечек конфиденциальной информации в I полугодии 2018 года. — URL: https://www.infowatch.ru/analytics/analitika/globalnoe-issledovanie-utechek-informatsii-v-i-polugodii-2018-goda (дата обращения: 03.06.2022).
41. Овчинский В.С., Ларина Е.С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. IT в оборонно-промышленном комплексе. Вторник, 26 мая 2015 // Тематическое приложение к газете «Коммерсантъ». — № 17. — URL: https://public.wikireading.ru/124168 (дата обращения: 03.06.2022).
42. Ma Huateng, Meng Zhaoli, YanDeli Wang Hualei (2021). The Chinese Digital Economy. Palgrave Macmillan. — URL: https://doi.org/10.1007/978–981–33–6005–1 (дата обращения: 20.05.2022).
43. Xiaoming Zhu (2019). Emerging Champions in the Digital Economy. New Theories and Cases on Evolving Technologies and Business Models. Shanghai Jiao Tong University Press and Springer Nature Singapore Pte Ltd. — URL: https://doi.org/10.1007/978–981–13–2628–8 (дата обращения: 20.05.2022).
44. Ramjee Prasad, Vandana Rohokale (2020). Cyber Security: The Lifeline of Information and Communication Technology. Springer Nature Switzerland AG. — URL: https://doi.org/10.1007/978–3–030–31703–4 (дата обращения: 20.05.2022).
45. Global Issue. Cybersecurity. Curation: Carnegie Mellon University. — URL: https://intelligence.weforum.org/topics/a1Gb00000015LbsEAE (дата обращения: 03.06.2022)
46. Yassine Maleh, Youssef Baddi, Mamoun Alazab, Loai Tawalbeh, Imed Romdhani (2021). Artificial Intelligence and Blockchain for Future Cybersecurity Applications. — URL: https://doi.org/10.1007/978–3–030–74575–2 (дата обращения: 20.05.2022).

47. Under the Hood of Cyber Crime. The Rise of Stealthy and Targeted Cyber Attacks. 2019 Security Report. Volume 02. Check Point Research. — URL: https://bezpecneit.cz/wp-content/uploads/2019/03/SR2019_Single-Pages_Vol-2_R2.pdf (дата обращения: 03.06.2022)
48. Dhanya Thakkar. Preventing Digital Extortion. Mitigate ransomware, DDoS, and other cyber-extortion Attacks // 2017 Packt Publishing. — P. 334.
49. Вавренюк А.Б., Васильев Н.П., Вельмякина Е.В., Гуров Д.В., Иванов М.А., Матвейчиков И.В., Мацук И.А., Михайлов Д.М., Шустова Л.И. Разрушающие программные воздействия. — М.: НИЯУ МИФИ, 2011. — 328 с. — URL: http://www.aha.ru/~msa/razrushayuschie.pdf (дата обращения: 03.06.2022).
50. The Underground Hacker Markets are Booming with Counterfeit Documents, Premiere Credit Cards, Hacker Tutorials and 100% Satisfaction Guarantees. DELL Secureworks. — URL: http://resources.infosecinstitute.com/wp-content/uploads/Secureworks-Underground-Hacking-Report.pdf (дата обращения: 03.06.2022).
51. The Internet Organised Crime Threat Assessment (IOCTA) 2016. Europol. — URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 (дата обращения: 03.06.2022)
52. The Cost of Cybercrime. Detica. — URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf (дата обращения: 03.06.2022).
53. A Cyberworm That Knows No Boundaries. RAND Corporation. — URL: https://www.rand.org/content/dam/rand/pubs/occasional_papers/2011/RAND_OP342.sum.pdf (дата обращения: 03.06.2022).
54. Lillian Ablon, Martin C. Libicki, Andrea A. Golay. Markets for Cybercrime Tools and Stolen Data. — URL: https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf (дата обращения: 03.06.2022).
55. Охрименко С., Борта Г. Тень цифровой экономики. Годишник на СА "Д.А. Ценов". — Свищов. 2018. — С. 79–134. — URL: http://security.ase.md/materials/publications/pdf/2019-p1366_3-Godishnik.pdf (дата обращения: 03.06.2022).
56. Android-троян Cerberus выставлен на аукцион. — URL: https://www.securitylab.ru/news/510564.php (дата обращения: 03.06.2022).

57. Cyber Capabilities and National Power: A Net Assessment. — URL: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power (дата обращения: 03.06.2022).
58. Что такое целевая атака: признаки, объекты и последствия. — URL: https://www.ptsecurity.com/ru-ru/research/knowledge-base/chto-takoe-celevaya-ataka-priznaki-obekty-i-posledstviya/ (дата обращения: 03.06.2022).
59. Report: Cryptocurrency Exchanges Lost $882 Million to Hackers. — URL: https://www.bankinfosecurity.com/cryptocurrency-exchanges-lost-882-million-to-hackers-a-11624 (дата обращения: 03.06.2022).
60. Hosuk Lee-Makiyama. Stealing Thunder. ECIPE, № 2/18. — URL: https://ecipe.org/wpcontent/uploads/2018/02/ECIPE_Occasional0218_HLM_V7.pdf (дата обращения: 03.06.2022).
61. General Data Protection Regulation GDPR. — URL: https://gdpr-info.eu, https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1–0.pdf (дата обращения: 03.06.2022).
62. Stephen Willis. Is GDPR the new hacker scare tactic? — URL: https://betanews.com/2019/03/29/is-gdpr-the-new-hacker-scare-tactic (даата обращения: 03.06.2022).
63. DLA Piper GDPR data breach survey: January 2020. — URL: https://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020/ (дата обращения: 03.06.2022).
64. 2017 Data Breach Investigation Report. 10th Edition. — URL: https://enterprise.verizon.com/resources/reports/2017/2017_dbir.pdf (дата обращения: 03.06.2022).
65. Мария Колобова. Эфир и ум: в 2022-м капитализация крипторынка достигнет $4 трлн. Почему Ethereum станет лучшим активом для инвестиций, чем биткоин. — URL: https://iz.ru/1270357/mariia-kolobova/efir-i-um-v-2022-m-kapitalizatciia-kriptorynka-dostignet-4-trln (дата обращения: 03.06.2022).
66. 2018 Криптовалютные биржи. Анализ утечек учетных записей пользователей. — URL: https://www.group-ib.ru/resources/threat-research/cryptocurrency-exchanges.html (дата обращения: 03.06.2022).
67. Хакеры похитили более 7 тысяч биткойнов с криптобиржи Binance. — URL: https://www.kommersant.ru/doc/3965956?from=four_mir (дата обращения: 03.06.2022).

68. Crime Report. Decoding increasingly sophisticated hacks, darknet markets, and scams. — URL: https://theblockchaintest.com/uploads/resources/file-528293540315.pdf (дата обращения: 03.06.2022).
69. На постсоветском пространстве нейтрализована банда, отмывшая десятки миллионов долларов от кибервымогательства. https://safe.cnews.ru/news/top/2020–08–20_na_postsovetskom_prostranstve (дата обращения: 03.06.2022).
70. The Global Risks Report 2022, 17th Edition, is published by the World Economic Forum. — URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf (дата обращения: 03.06.2022).
71. Adrian T.H. Kuah, Roberto Dillon (2021). Digital Transformation in a Post-COVID World. Sustainable Innovation, Disruption, and Change. CRC Press.
72. Levi West (2020). The Coronavirus Cybersecurity Survival Guide. Top Tips to Protect You from a Cyber Attack.
73. Robert Slade (2021). Cybersecurity Lessons from CoVID-19. CRC Press.
74. Steve Morgan (2021). Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2021 To 2025. — URL: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/ (дата обращения: 15.05.2022).
75. Mathew J. Schwartz (2021). Cyber Extortion Thriving Thanks to Accellion FTA Hits. — URL: https://www.databreachtoday.com/blogs/cyber-extortion-thriving-thanks-to-accellion-fta-hits-p-3024 (дата обращения: 15.05.2022).
76. Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound. — URL: https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound (дата обращения: 15.05.2022).
77. 2021 Ransomware Threat Report. — URL: https://www.darktrace.com/en/resources/ds-ransomware.pdf (дата обращения: 15.05.2022).
78. György Gyomai, Peter van de Ven. The Non-Observed Economy in the System of National Accounts. — URL: https://www.oecd.org/sdd/na/Statistics%20Brief%2018.pdf (дата обращения: 15.05.2022).
79. Measuring the Non-Observed Economy. A Handbook. http://www.oecd.org/sdd/na/1963116.pdf (дата обращения: 15.05.2022).

80. Marcena Hunter (2018). Capturing the proceeds of crime in illicit financial flow models. The Global Initiative Against Transnational Organized Crime. — URL: https://globalinitiative.net/wp-content/uploads/2018/06/TGIATOC–Illicit-Financial-Flows-report-1941-hi-res-2–1.p (дата обращения: 15.05.2022).
81. Friedrisch SCHNEIDER (2017). Restricting or Abolishing Cash: An Effective Instrument for Fighting the Shadow Economy, Crime and Terrorism? — URL: https://www.bundesbank.de/Redaktion/EN/Downloads/Tasks/Cash_management/Conferences/2017_04_24_schneider.pdf?__blob=publicationFile (дата обращения: 15.05.2022).
82. 2015 Cost of Cyber Crime Study: Global Benchmark Study of Global Companies. — URL: http://www.cnmeonline.com/myresources/hpe/docs/HPESIEMAnalyst Report-2015CostofCyberCrimeStudy–Global.pdf (дата обращения: 15.05.2022).
83. 2016: Current State of Cybercrime. — URL: https://www.rsa.com/content/ dam/rsa/PDF/2016/05/2016-current-state-of-cybercrime.pdf (дата обращения: 15.05.2022).
84. 2017 Cyber Attack Trends and New Global Cyber Threats. — URL: https://pages.checkpoint.com/global-cyber-attack-trends-2017.html?utm source=research&utm medium=cp-website& utm campaign=CM WR18Q1 WW Threat Intelligence Trends Report 2017 H2 (дата обращения: 15.05.2022).
85. Adjusting the Lens on Economic Crime. — URL: https://www.pwc.com/gx/en/economic-crime- survey/pdf/GlobalEconomicCrimeSurvey2016.pdf (дата обращения: 21.05.2022).
86. Comprehensive Study on Cybercrime. — URL: https://www.unodc.org/documents/organized-crime/UNODC CCPCJ EG.42013/CYBERCRIME STUDY210213.pdf (дата обращения: 21.05.2022).
87. Cybercrimes/e-Crimes: Assessment Report. ITU2012. — URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/HIPCAR%20Assessment%20Cybercrimes.pdf (дата обращения: 16.05.2022).
88. Cyber security. Report. Special Eurobarometer 423. — URL: http://ec.europa. eu/commfrontoffice/publicopinion/archives/ebs/ebs 423en.pdf
89. Hackmageddon. Information Security Timelines and Statistics. — URL: https://www.hackmageddon.com (дата обращения: 16.05.2022).
90. The Global Risks Report 2018. 13th Edition. — URL: https://www3.weforum.org/maintenance/public.htm (дата обращения: 16.05.2022).

91. Jason Williams. (2019). Cybercrime as an Economy. — URL: https://thefintechtimes.com/cybercrime-economy/ (дата обращения: 16.05.2022).
92. С.Ю. Неформальная экономика: Экономико-социологический анализ / Гос. ун-т — Высшая школа экономики. — М.: Изд. дом ГУ ВШЭ, 2004.— 448 с.
93. Латов В. Социальные функции теневой экономики в институциональном развитии постсоветской России: Дис. ... д-ра соц. н. / Высшая Школа Экономики. — Тюмень, 2008.
94. Родионов И., Гиляревский Р., Цветкова В., Залаев З. Рынок информационных услуг и продуктов. — М.: МК-Периодика, 2002.
95. Филиппова Т. Деактивация теневой экономики в России. — Томск: STT, 2013.
96. Boehme R. Vulnerability Markets. What is the economic value of a zero-day exploit? Technische Universitat Dresden, Institute for System Architecture. — URL: https://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf (дата обращения: 16.05.2022).
97. Gaspareniene L., Remeikiene R., Schneider F. The factors of digital shadow consumption. Intellectual Economics 9 (2015) 108–119. — URL: http://www.econ.jku.at/members/Schneider/files/publications/2016/DigitalShadowConsumption.pdf (дата обращения: 16.05.2022).
98. Rentrop C., Zimmermann S. Shadow IT Evaluation Model. FedCSIS, 2012 г. — URL: https://fedcsis.org/proceedings/2012/pliks/394.pdf. (дата обращения: 16.05.2022).
99. Krebs B. Crimeware Author Funds Exploit Buying Spree. Krebs on Security. URL: http://krebsonsecurity.com/2013/01/crimeware-author-funds-exploit-buying-spree/ (дата обращения: 16.04.2022).
100. F. Implausible Large Differences in the Sizes of Underground Economies in Highly Developed European Countries? A Comparison of Different Estimation Methods. — URL: https://www.cesifo-group.de/ifoHome/publications/docbase/DocBase_Content/WP/WP (дата обращения: 16.04.2022).
101. Stu Sjouwerman. CYBERHEIST: The biggest financial threat facing American businesses since the meltdown of 2008. — URL: https://cdn2.hubspot.net/hubfs/241394/Cyberheist_2016-B.pdf (дата обращения: 21.04.2022).
102. F. Korzeniowski. SECURITOLOGIA. Nauka o bezpieczeństwie człowieka i organizacji społecznych. — EAS Kraków, 2008.

103. A Framework for Programming and Budgeting for Cybersecurity. — URL: https://www.rand.org/content/dam/rand/pubs/tools/TL100/TL186/RAND_TL186.pdf (дата обращения: 02.04.2022).
104. Markets for Cybercrime Tools and Stolen Data. https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf (дата обращения: 21.04.2022).
105. A Cyberworm that Knows no Boundaries. — URL: https://www.rand.org/content/dam/rand/pubs/occasional_papers/2011/RAND_OP342.sum.pdf (дата обращения: 16.05.2022).
106. Глава ООН рассказал о своих приоритетах на 2020 год. — URL: https://news.un.org/ru/story/2020/01/1371131 (дата обращения: 16.05.2022).
107. HOWARD J. SHATZ (2020). Economic Competition in the 21st Century. — URL: https://www.rand.org/pubs/research_reports/RR4188.html (дата обращения: 16.05.2022).
108. Введение в «Цифровую» экономику / А.В. Кешелава В.Г. Буданов, В.Ю. Румянцев др.; под общ. ред. А.В. Кешелава; гл. «цифр.» конс. И.А. Зимненко. — ВНИИГ, 2017.— 28 с. — URL: http://spkurdyumov.ru/uploads/2017/07/vvedenie-v-cifrovuyu-ekonomiku-na-poroge-cifrovogo-budushhego.pdf (дата обращения: 03.06.2022).
109. Ursula von der Leyen's message to Davos Agenda: Full transcript. — URL: https://www.weforum.org/agenda/2021/01/ursula-von-der-leyen-european-commission-davos-agenda/?utm_source=sfmc&utm_medium=email&utm_campaign=2740992_Agenda_weekly-29January2021&utm_term=&emailType=Newsletter (дата обращения: 25.05.2022).
110. Глобальное исследование утечек конфиденциальной информации в I полугодии 2018 года. — URL: https://www.infowatch.ru/report2018_half (дата обращения: 06.03.2022).
111. Овчинский В.С., Ларина Е.С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. IT в оборонно-промышленном комплексе. Вторник, 26 мая 2015 // Тематическое приложение к газете «Коммерсантъ». — № 17. — URL: https://public.wikireading.ru/124168 (дата обращения: 06.03.2022).
112. Ma Huateng, Meng Zhaoli, YanDeli Wang Hualei (2021). The Chinese Digital Economy. Palgrave Macmillan. — URL: https://doi.org/10.1007/978–981–33–6005–1 (дата обращения: 06.03.2022).

113. Xiaoming Zhu (2019). Emerging Champions in the Digital Economy. New Theories and Cases on Evolving Technologies and Business Models. Shanghai Jiao Tong University Press and Springer Nature Singapore Pte Ltd. — URL: https://doi.org/10.1007/978–981–13–2628–8 (дата обращения: 06.03.2022).
114. Ramjee Prasad, Vandana Rohokale (2020). Cyber Security: The Lifeline of Information and Communication Technology. Springer Nature Switzerland AG. — URL: https://doi.org/10.1007/978–3–030–31703–4 (дата обращения: 06.03.2022).
115. Global Issue. Cybersecurity. Curation: Carnegie Mellon University. — URL: https://intelligence.weforum.org/topics/a1Gb00000015LbsEAE (дата обращения: 03.06.2022).
116. Yassine Maleh, Youssef Baddi, Mamoun Alazab, Loai Tawalbeh, Imed Romdhani (2021). Artificial Intelligence and Blockchain for Future Cybersecurity Applications. — URL: https://doi.org/10.1007/978–3–030–74575–2 (дата обращения: 03.06.2022).
117. Under the Hood of Cyber Crime. The Rise of Stealthy and Targeted Cyber Attacks. 2019 Security Report. Volume 02. Check Point Research. — URL: https://bezpecneit.cz/wp-content/uploads/2019/03/SR2019_Single-Pages_Vol-2_R2.pdf (дата обращения: 03.06.2022).
118. Dhanya Thakkar. Preventing Digital Extortion. Mitigate ransomware, DDoS, and other cyber-extortion Attacks // 2017 Packt Publishing. — P. 334.
119. Вавренюк А.Б., Васильев Н.П., Вельмякина Е.В., Гуров Д.В., Иванов М.А., Матвейчиков И.В., Мацук И.А., Михайлов Д.М., Шустова Л.И. Разрушающие программные воздействия. — М.: НИЯУ МИФИ, 2011. — 328 с.
120. The Underground Hacker Markets are Booming with Counterfeit Documents, Premiere Credit Cards, Hacker Tutorials and 100% Satisfaction Guarantees. DELL Secureworks, 12.2014. — URL: http://www.secureworks.com/assets/pdf-store/white-papers/wp-underground-hacking-report.pdf (дата обращения: 03.06.2022).
121. The Internet Organised Crime Threat Assessment (IOCTA) 2016. Europol. — URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 (дата обращения: 03.06.2022).
122. The Cost of Cybercrime. Detica. — URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf (дата обращения: 03.06.2022).

123. A Cyberworm That Knows No Boundaries. RAND Corporation. — URL: https://www.rand.org/content/dam/rand/pubs/occasional_papers/2011/RAND_OP342.sum.pdf (дата обращения: 03.06.2022).
124. Lillian Ablon, Martin C. Libicki, Andrea A. Golay. Markets for Cybercrime Tools and Stolen Data. — URL: https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf (дата обращения: 03.06.2022).
125. Охрименко С., Борта Г. Тень цифровой экономики. Годишник на СА “Д.А. Ценов”. — Свищов. 2018. — С. 79–134.
126. Банковский Android-троян Cerberus выставлен на аукцион. — URL: https://www.securitylab.ru/news/510564.php
127. Cyber Capabilities and National Power: A Net Assessment. — URL: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power (дата обращения: 03.06.2022).
128. Что такое целевая атака: признаки, объекты и последствия. — URL: https://www.ptsecurity.com/ru-ru/research/knowledge-base/chto-takoe-celevaya-ataka-priznaki-obekty-i-posledstviya/ (дата обращения: 03.06.2022).
129. Report: Cryptocurrency Exchanges Lost $882 Million to Hackers. — URL: https://www.bankinfosecurity.com/cryptocurrency-exchanges-lost-882-million-to-hackers-a-11624 (дата обращения: 03.06.2022).
130. Hosuk Lee-Makiyama. Stealing Thunder. ECIPE, № 2/18 — URL: https://ecipe.org/wp-content/uploads/2018/02/ECIPE_Occasional0218_HLM_V7.pdf (дата обращения: 03.06.2022).
131. General Data Protection Regulation GDPR. — URL: https://gdpr-info.eu, https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1–0.pdf (дата обращения: 03.06.2022).
132. Stephen Willis. Is GDPR the new hacker scare tactic? — URL: https://betanews.com/2019/03/29/is-gdpr-the-new-hacker-scare-tactic (дата обращения: 03.06.2022).
133. DLA Piper GDPR data breach survey: January 2020. — URL: https://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020/ (дата обращения: 03.06.2022).
134. 2017 Data Breach Investigation Report. 10th Edition. — URL: https://enterprise.verizon.com/resources/reports/2017/2017_dbir.pdf (дата обращения: 03.06.2022).

135. Колобова. Эфир и ум: в 2022-м капитализация крипторынка достигнет $4 трлн. Почему Ethereum станет лучшим активом для инвестиций, чем биткоин. — URL: https://iz.ru/1270357/mariia-kolobova/efir-i-um-v-2022-m-kapitalizatciia-kriptorynka-dostignet-4-trln (дата обращения: 03.06.2022).
136. 2018 Криптовалютные биржи. Анализ утечек учетных записей пользователей. — URL: https://www.group-ib.ru/resources/threat-research/cryptocurrency-exchanges.html (дата обращения: 03.06.2022).
137. Хакеры похитили более 7 тысяч биткойнов с криптобиржи Binance — URL: https://www.kommersant.ru/doc/3965956?from=four_mir (дата обращения: 25.05.2022).
138. Crypto Crime Report. Decoding increasingly sophisticated hacks, darknet markets, and scams. — URL: January 2019. — URL: https://uploads-ssl.webflow.com/5a9360f88433cb00018022c2/5c4f67ee7deb5948e2941fda_Chainalysis%20January%202019 %20Crypto%20Crime%20Report.pdf (дата обращения: 15.03.2022).
139. На постсоветском пространстве нейтрализована банда, отмывшая десятки миллионов долларов от кибервымогательства. URL: https://safe.cnews.ru/news/top/2020–08–20_na_postsovetskom_prostranstve (дата обращения: 02.06.2022).
140. The Global Risks Report 2022, 17th Edition, is published by the World Economic Forum. — URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf (дата обращения: 02.06.2022).