KEY SEGMENTS OF THE DIGITAL SHADOW ECONOMICS

ОСНОВНЫЕ СЕГМЕНТЫ ТЕНЕВОЙ ЦИФРОВОЙ ЭКОНОМИКИ

Охрименко Сергей
Доктор экономических наук, профессор
Академия Экономичексих Знаний Молдовы
e-mail: osa@ase.md

Бортэ Григорий
Кандидат экономических наук, доцент
Академия Экономичексих Знаний Молдовы
e-mail: grigori.borta@gmail.com

Abstract
This article highlights and discusses new segments of the shadow digital economy. Among them, such as cyber weapons, as the concentration of all the achievements of information and communication technologies at the level of counteraction between states; targeted attacks and ATR groups; attack on cryptocurrency exchanges; identity theft. Statistical data characterizing these segments of the shadow digital economy is analyzed.

Keywords: *shadow digital economics, information security, threats in information security, cryptocurrencies, cryptoexchanges.*

JEL Classification: *E26 F52 J46 H56*

ВВЕДЕНИЕ

Настоящая работа является логическим продолжением исследований теневой цифровой экономики (ТЦЭ), нашедших отражение в ряде публикаций авторов, в частности таких, как [2], [6], [7]. Одной из важных задач выступает не только определение категории ТЦЭ, но и ландшафта современных угроз. В частности, процессы цифровой трансформации экономики (например, реализация концепции «Индустрия 4.0») породили новые угрозы [4]:

- атаки становятся все более изощренными за счет автоматизации и использования методов искусственного интеллекта и машинного обучения;
- подключение огромного количества новых незащищенных устройств (промышленный интернет или интернет вещей, как сеть передачи данных между физическими объектами, которые оснащены встроенными средствами и технологиями взаимодействия друг с другом или с внешней средой). Хакеры используют для входа в сеть такие устройства как, видеокамеры, кофемашины и др.;
- в результате резко возрастает количество целей для атак.

Авторы изучили состав основных продуктов и услуг криминальной направленности, относящихся к ТЦЭ. Но их спектр постоянно изменяется, появляются новые сегменты, требующие исследования и описания. В данной статье будет рассмотрены следующие сегменты: кибероружие, как сосредоточение всех достижений информационных и коммуникационных технологий на уровне противодействия между государствами; целенаправленные атаки и АТР-группы; нападение на криптобиржи, кража личных данных.

КИБЕРОРУЖИЕ

Под кибероружием понимается вредоносное программное обеспечение, используемое в военных или разведывательных целях. В последнее время всплывает всё 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 кибероборoной, но и кибератаками, являются следующие: США, Великобритания, Российская Федерация, Франция, Германия, Эстония, Иран, Израиль, Южная и Северная Корея, Китай. Австралия и др.

Основными событиями выступают следующие [5]:

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 авиа-ударов 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) 2014 – 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.

С ростом киберугроз расходы в области кибербезопасности постоянно растут (в том числе расходы на брандмауэры и анализ угроз) со стороны правительств и частного сектора неуклонно растут, и по оценкам [1], стоимость приближается к 0,1% мирового ВВП. Некоторые исследователи утверждают, что существующую риски и издержки, связанные с облачными технологиями и 5G, перевешивают выгоды от цифровизации [9], [15].

Еще одним немаловажным аспектом является стоимость потерь от кибершпионажа. Например, по данным Центра стратегических и международных исследований (CSIS, https://www.csis.org), в 2014 году глобальные затраты на кибербезопасность составили до 575 млрд. дол. (или 0,8% от мирового ВВП). Для Европейского Союза стоимость оценивается в 0,41% ВВП или 55 млрд. дол. в год. По расчетам страховой компании Lloyd's срыв облачного сервиса может привести к значительным экономическим потерям, которые могут варьироваться от 4,6 млрд. дол. До 53,1 млрд. дол. Или 0,07% мирового ВВП [10]. Кибершпионаж очень дорого обходится Европейскому Союзу – как результат подобных действий - ежегодно теряются 55 млрд евро, 289000 рабочих мест находятся в опасности. Подобные существенные потери будут возрастать с расширением процессов цифровизации

(поколение 5G, Индустрия 4.0), по прогнозам ожидается появление в сети 26 000 000 000 новых устройств. Естественно можно предположить, что возрастут атаки на информационные системы и ресурсы, изменится их состав и количество.

ЦЕЛЕВЫЕ (ЦЕЛЕНАПРАВЛЕННЫЕ) 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 [22].

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

Таблица 1. Список целевых кибератак, нацеленных на интересы ЕС

Инцидент, угроза	*Предполагаемый правительственный спонсор*	*Год*	*Затрагиваемые интересы ЕС*	*Примечания*
APT 10	Китай	2017	Великобритания, Франция, Швеция, Финляндия	Китайская группа ATP 10 (или Red Apollo) осуществляет кражу информации, характеризующую интеллектуальную собственность и других конфиденциальных данных из нескольких информационных систем сервис-провайдеров относительно энергетических, финасовых, 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

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 науелена 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
CROUCHING 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
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 THYSSENKRUPP	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 [1]

ATP-команды по странам:
Китай: ATP41, ATP40, ATP31, ATP30, ATP27, ATP25, ATP24, ATP23, ATP22, ATP21, ATP20, ATP19, ATP18, ATP17, ATP16, ATP15, ATP14, ATP12, ATP10, ATP9, ATP8, ATP7, ATP6, ATP4, ATP3, ATP2, ATP1.
Северная Корея: ATP38, ATP37.
Россия: ATP29, ATP28.
Вьетнам: ATP32.
Неопределенные: ATP5.

Приведенные примеры нелегальных действий и продуктов далеко не исчерпывают всего многообразия. Данный набор постоянно совершенствуется и обновляется с завидной скоростью. В связи с этим, разработка реестра подобных продуктов является весьма актуальной и окажет существенную помощь разработчикам программного обеспечения, персоналу, отвечающему за поддержку информационных систем.

Следует отметить многообразие атак, направленных на разные информационные объекты. В качестве основного объекта следует рассматривать организации кредитно-финансовой сферы. Основной тренд последних лет – использование для компрометации информационных систем и сетей инструментов, предназначенных для проведения тестирования на проникновение. В качестве такого инструмента использовался прежде всего набор программ Cobalt Strike, разработанный американской компанией Strategic Cyber, LLC. В то же время, анализируя способы совершения различных атак, специалисты ФинЦЕРТ обоснованно предполагают наличие иных преступных групп, использующих похожие инструменты. Большинство атак с использованием Cobalt Strike, наблюдавшихся в 2016 – 2017 гг., реализовали одну из двух схем: конечной целью были либо банкоматы, либо процессинг платежных карт.

Типовая схема целевой атаки на кредитную организацию выглядит следующим образом:

1. Производится массовая рассылка электронных писем, содержащих вредоносные вложения, на адреса организаций кредитно-финансовой сферы.
2. В случае запуска вредоносного вложения из письма на компьютере получателя, проявившего неосторожность, происходит скрытное внедрение программ, чаще всего – загрузчика.
3. После скачивания загрузчика на компьютере устанавливается компонент Beacon – основной инструмент из набора Cobalt Strike. Атакующий получает возможность удаленного доступа к зараженному компьютеру.

4. Атакующий проводит исследование доступных с зараженного компьютера сегментов сети и пытается установить доступ к контроллеру домена сети с целью последующего получения паролей администраторов. Для получения пароля могут быть использованы возможности специальных инструментов (Mimikatz и другие).

5. После получения доступа к контроллеру домена и администраторских паролей атакующий проводит поиск в сети интересующих серверов и компьютеров. Прежде всего ищется компьютер или сервер, с которого есть доступ в подсеть, где находятся банкоматы или иные сегменты сети, например, в сегмент процессинга платежных карт.

6. На банкоматах устанавливается программное обеспечение, взаимодействующее, предположительно, через программный интерфейс XFS и обеспечивающее выдачу денежных средств по команде, подаваемой удаленно. После получения контроля над банкоматами к процессу привлекаются соучастники, занимающиеся получением денежных средств. Их задача – обеспечить присутствие около банкоматов в условленное время для получения денег. После успешной выдачи денежных средств программное обеспечение с банкоматов, как правило, удаляется.

7. В случае получения доступа к процессингу платежных карт привлекаются соучастники, занимающиеся оформлением на подставных лиц платежных карт атакованной организации. Данные карты консолидируются в руках лиц, занимающихся получением денежных средств. Их задача – обеспечить снятие денежных средств в банкоматах непосредственно после того, как балансы и лимиты карт будут повышены в системе процессинга. В процессе получения денег соучастниками оператор может при необходимости продолжать поднимать лимиты по снятию или балансы карт.

8. В случае получения доступа к компьютерным средствам сегмента платежной системы Банка России (АРМ КБР) или системы переводов SWIFT производятся платежи на заранее подготовленные счета, с которых денежные средства далее переводятся и обналичиваются по стандартным для компьютерной преступности схемам.

НАПАДЕНИЕ НА КРИПТОБИРЖИ

Относительно новым направлением является атака на криптобиржи, кража криптовалют и отмывание денежных средств. Высокая рыночная капитализация отдельных криптовалют привлекает хакеров. В качестве примера используем данные, приведенные в таблице 2.

Таблица 2. Криптовалюты по состоянию на 8 мая 2018 года

№ п\п	*Наименование криптовалюты*	*Стоимость (в млрд. дол.)*
1.	Bitcoin	160
2.	Ethereum	75
3.	Ripple	32
4.	Bitcoin Cash	28
5.	EOS	15
6.	Litecoin	9
7.	Cardano	8
8.	Stellar	7,4
9.	IOTA	6,6
10.	TRON	5,5
11.	NEO	5,1
12.	Dash	3,7
13.	Monero	3,6
14.	Ethereum Classic	2,3
15.	Verge	1,1
16.	Zcash	1,1
17.	Decred	0,62

Источник: CoinMarketCap website (https://coinmarketcap.com/)

По состоянию на 23 декабря 2020, года лидерами являются следующие криптовалюты, таблица 3.

Таблица 3. Текущие данные о стоимости основных криптовалют

Название	*Тикер*	*Цена (USD)*	*Рын.кап.*
Биткоин	BTC	23.570	439,57B$
Эфириум	ETH	609,25	69,76B$
Tether	USDT	0,9997	20,47B$
Рипл	XRP	0,31428	14,57B$
Лайткоин	LTC	105,212	7,07B$
Bitcoin Cash	BCH	291,12	5,46B$
Chainlink	LINK	11,82	4,74B$

Источник: Ведущие криптовалюты. https://ru.investing.com/crypto/

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.

ТОП 10 КРИПТОВАЛЮТ ПО КАПИТАЛИЗАЦИИ

Капитализация рынка криптовалют превысила $400 млрд. [18]. Наибольшее внимание инвесторов и трейдеров приковано к тем криптовалютам, которые имеют самую высокую капитализацию. Несмотря на то, что сравнение криптовалют по данному показателю некоторые считают не полностью объективным, именно капитализация является главным фактором, определяющим интерес к отдельной монете со стороны не только покупателей, но и кибермошенников. Для сравнения

приведем данные по 10 криптовалютам по капитализации на начало октября 2020 г., которые представлены в следующей таблице.

Таблица 4. 10 ведущих криптовалют по капитализации на октябрь 2020 г.

Название криптовалюты	*Тиккер*	*Текущая рыночная стоимость*	*Капитализация*
Bitcoin	BTC	$10 610	$196,4 млрд
Ethereum	ETH	$340	$38,3 млрд
Tether	USDT	$1,00	$15,6 млрд
Ripple	XRP	$0,24	$11,1 млрд
Bitcoin Cash	BCH	$219,01	$4,05 млрд
Binance Coin	BNB	$27,45	$3,9 млрд
Polkadot	DOT	$3,81	$3,2 млрд
Chainlink	LINK	$8,80	$3,08 млрд
Crypto.com Coin	CRO	$0,14	$3,02 млрд
Litecoin	LTC	$45,89	$3,01 млрд

Источник: Капитализация криптовалют: Особенности и как влияет на трейдинг [17]

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 5. Примеры успешных атак на криптообменники в 2017-2018 г.г

Дата	*Наименование проекта*	*Страна*	*Группа*	*Потери в криптовалюте*	*Потери в млн $*
Февраль 2017 г.	Bithumb	Южная Корея	-	-	7
Апрель 2017 г.	YouBit	Южная Корея	-	-	5,6
Апрель 2017 г.	Yapizon	Южная Корея	Lazarus	3,816 BTC	5,3
Апрель 2017 г.	Ether Delta	-	Неизвестна	-	0,225
Август 2017 г.	OKEx	Гонконг	Неизвестна	-	3
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
Январь 2018 г.	Coincheck	Япония	Lazarus	532.000.000 NEM	534
Февраль 2018 г.	Bitgrail	Италия	Неизвестна	17.000.000 NANO	170
Июнь 2018 г.	Bithumb	Южная Корея	Lazarus	-	32
Июнь 2018 г.	Coinrail	Южная Корея	Неизвестна	-	37
Июнь 2018 г.	Bancor	-	Неизвестна	-	23
Сентябрь 2018 г.	Zaif	Япония	Неизвестна	-	60
				Итого	882

Источник: Report: Cryptocurrency Exchanges Lost $882 Million to Hackers [14]

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 коммерческие 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. 26 января 2018 года японская криптобиржа Coincheck стала жертвой крупной хакерской атаки взлома, 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 (табл.6).

Таблица 6. 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% [21]

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» [8] указано, что по меньшей мере 5 из 19 криптобирж стали жертвами целенаправленных атак: Bitfinex, Bithumb, HitBTC, Huobi (табл.7).

Таблица 7. 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 980277	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: Short Guide on Shadow it Digital Footprinting, Continuous Monitoring & Digital Risk Protection [16]

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 млню – 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 трансакцию 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 [20].

Хакерские атаки на криптобиржи превращаются в норму. Так, по данным отчета аналитической компании Chainalysis [11], 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 млн.дол. 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» [19]. Киберполицейские Украины при поддержке операторов криптобиржи Binance нейтрализовали банду кибермошенников, которые за два года отмыли около $42 млн через два десятка криминальных «обменников» – точек обналичивания криптовалют. Киберполицейские Украины 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.

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. Это своеобразная подушка безопасности для задержанных.

КРАЖА ЛИЧНЫХ 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) [13]. 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 [3].

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 может быть банковское учреждение, страховая компания, инвестиционная служба или медицинское учреждение. 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 (это относилось к необходимости в дополнительном персонале для защиты данных за пределами обычной ИТ-команды).

Продолжаются между специалистами в печати дискуссии относительно возможности создания адекватной системы информационной безопасности на базе минимальных стандартов, отвечающей требованиям GDPR. Высказываются мнения,

что хакеры продолжат поиск возможностей вторжения в сеть, используя технологии искусственного интеллекта для поиска уязвимых точек, а также анализ и отслеживание их на предмет возможных кибератак. Нет никаких сомнений, что хакеры пристально изучают новый регламент на предмет поиска «узких» мест и готовят «сюрпризы» службе информационной безопасности. В частности [3], предлагается проанализировать возможные действия хакеров, получивших название «обратного вымогательства». В основе данной схемы лежит использование механизма шифрования данных у пользователя (программа-шифровальщик) и вымогательства денежных средств (в различных криптовалютах, в основном в биткойнах) для восстановления данных. Подобные действия подробно описаны в специальной литературе. Но последовательность действий несколько другая, отличная от технологии вымогательства.

Суть данного действия заключается в следующем:

- хакер проникает в сеть любыми доступными средствами для получения и сбора информации о списках клиентов, которые обеспечены защитой новыми правилами GDPR;
- полученные данные обещают опубликовать публично, что приведет к нарушению регламента GDPR и сделает ответственной организацию за нарушение данного регламента. Соответственно, организацию ждет огромный штраф, который значительно превышает требуемый выкуп.

Второе действие сводится к массовой рассылке фишинговых писем, в которых предлагаются услуги бесплатных консультаций для объяснения GDPR, треннингов и разработку политики безопасности. В случае, если пользователь проходит по указанной ссылке, не исключено, что сайт заражен шпионским программным обеспечением или содержание письма автоматически рассылается коллегам абонента. Невнимательность пользователя может быть самой большой угрозой кибербезопасности.

В январе 2020 года юридическая фирма DLA Piper опубликовала обзор данных о нарушениях, связанных с реализацией GDPR в части утечки персональных данных [12] в 28 странах-членах ЕС, а также Норвегии, Исландия и Лихтенштейна. Приведем основные положения данного отчета.

С 25 мая 2018 года (время ввода GDPR в действие) по 20 января 2020 года в общей сложности было отмечено 160921 случай нарушения данного закона, получивших уведомление надзорными огранами по заащите 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%. Отмечается четкая тенденция роста, хотя подробная информация об утечках не публикуется. Лидерами утечек персональных данных признаны Нидерланды, Германия и Великобритания. Общее количество нарушений персональных данных приведено в следующей таблице.

Таблица 8. Общее количество нарушений персональных данных

№ п\п	Страна	Общее количество нарушений персональных данных, зарегистрированных по юрисдикции за период с 25 мая 2018 года по 27 января 2020 года	Количество нарушений персональных данных, уведомленных по юрисдикции с 28 января 2019 года по 27	Количество нарушений персональных данных, уведомленных по юрисдикции с 25 мая 2018 года по 27	Рейтинг уведомлений о нарушениях в расчете на душу населения	Общая стоимость штрафов GDPR, наложенных с 25 мая 2018 года на 17 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
16	Венгрия	749	479	270	4,87	198 000
17	Чехия	720	430	290	4,03	291 717
18	Румыния	668	408	260	1,9	329 500
19	Люксембург	545	345	200	56,97	-
20	Исландия	338	313	25	91,15	-
21	Мальта	239	139	100	31	35 500
22	Греция	232	162	70	1,5	550 000
23	Литва	222	118	105	4,18	67 500
24	Эстония	188	121	67	9,74	-
25	Латвия	173	117	55	6,13	168 930
26	Кипр	94	59	35	4,8	151 900
27	Лихтенштейн	30	15	15	39,18	-
28	Болгария	-	-	-	-	3 156 500
29	Португалия	-	-	-	-	424 000
30	Словакия	-	-	-	-	132 600

Рассчитано по DLA Piper GDPR data breach survey: January 2020 [12].

ЗАКЛЮЧЕНИЕ

За последние несколько лет киберпреступность перешагнула через многие технические и программные преграды и перешла из узкоспециализированной ниши в один из наиболее значительных стратегических рисков, стоящих сегодня перед всем миром. Развитие цифровых форм мошенничества (криптовалюты и ICO, заражение вирусом-вымогателем, установка приложения на смартфон, фишинг и др) во многом способствует развитие технического прогресса.

Какие прогнозы представляют ведущие исследовательские и консалтинговые компании в области теневых ИТ [16]?

По прогнозам исследовательской и консалтинговой компании, Gartner к 2020 году 30% нарушений в информационной сфере будет вызвано теневыми ИТ.

В отчете консалтинговой компании Frost & Sullivan говорится, что более 80% респондентов признают, что используют неутвержденные (теневые) приложения в своей работе.

Исследования, проведенные компанией IDG, свидетельствуют что распространение теневых ИТ ежегодно увеличивается на 5% и составляют около 30% ИТ-бюджетов предприятий.

Исследователи Gartner показали, что Shadow IT составляют от 30 до 40% расходов на ИТ в целом.

Исследования Everest Group зафиксировали, что доля теневых ИТ составляет 50% и более в расходах на ИТ в целом.

БИБЛИОГРАФИЯ

9. Lee-Makiyama H. *Stealing Thunder.* ECIPE, No. 2/18. https://bit.ly/38FuJvs
10. Ohrimenco S., Borta G. *Chapter 8. Challenges for Digital Transformation in the Manufacturing Industry.* Socio-Economic Development. Interdisciplinary Ecosystems Perspective. The Jubilee Book Dedicated to Professor Kazimierz Zielinski. Cracow University of Economics, 2020, Poland, Cracow. – 330 p. ISBN 978-83-8175-233-6.
11. Willis S. *Is GDPR the new hacker scare tactic?* https://bit.ly/3rxcelw
12. Батранков Д. *Первый NGFW с машинным обучением.* https://bit.ly/3mKIjCY
13. Овчинский В., Ларина Е. *Кибервойны XXI века. О чем умолчал Эдвард Сноуден.* https://bit.ly/3mQ45Ft
14. Охрименко С., Бортэ Г. *Новое наполнение науки секьюритологии.* Nauka i praktyka bezpieczeństwa, Wydawnictwo EAS, Kraków, Poland. 2019. P. 112-147. ISBN 978-83-61645-34-4.
15. Охрименко С., Бортэ Г. *Тень цифровой экономики.* Годишник, Том CXXI, Академично Издателство „Ценов", Стопанска Академия "Д. А. Ценов". № 121, 2018. С.79-131. ISSN 0861-8054.
16. Юсуфов Р. *2018 Криптовалютные биржи. Анализ утечек учетных записей пользователей.* https://bit.ly/3poQ9nt
17. *2017 Data Breach Investigations Report.* https://vz.to/3aKNi4q
18. *A Lloyd's emerging risk report.* https://bit.ly/3rtjizK
19. *Crypto Crime Report. Decoding increasingly sophisticated hacks, darknet markets, and scams. January 2019.* https://bit.ly/34LqPQL
20. *DLA Piper GDPR data breach survey: January 2020.* https://bit.ly/3rw67hC
21. *General Data Protection Regulation. GDPR.* https://bit.ly/37RkaGs, https://bit.ly/3pjaQkG
22. *Report: Cryptocurrency Exchanges Lost $882 Million to Hackers.* https://bit.ly/37QWoKV
23. *Risk Nexus. Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Futures.* https://bit.ly/3nSl0bF
24. *Short Guide on Shadow it Digital Footprinting, Continuous Monitoring & digital risk protection.* https://bit.ly/2WOrRqW
25. *Капитализация криптовалют: Особенности и как влияет на трейдинг.* https://bit.ly/3rtjkaQ
26. *Капитализация рынка криптовалют превысила $400 млрд, но этого все равно мало.* https://bit.ly/34IEw2I

27. *На постсоветском пространстве нейтрализована банда, отмывшая десятки миллионов долларов от кибервымогательства.* https://bit.ly/2KTYrVE
28. *Хакеры похитили более 7 тысяч биткойнов с криптобиржи Binance.* https://bit.ly/38yA8Vq
29. *Число взломанных аккаунтов на биткоинбиржах в начале 2018 года выросло на 689%.* https://bit.ly/2WOud8Z
30. *Что такое целевая атака: признаки, объекты и последствия.* https://bit.ly/3aIp8aw