ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/2220-6469-2019-13-4-22-30
УДК 338.14+004.056.5(045)
JEL L86

Современные тренды экономической кибербезопасности

Ю.Ю. Шитова
Российский государственный гуманитарный университет, Москва, Россия;
Университет «Дубна», Дубна, Россия
https://orcid.org/0000-0001-6885-9047

Ю.А. Шитов
Объединенный институт ядерных исследований, Дубна, Россия
https://orcid.org/0000-0002-0184-418X

АННОТАЦИЯ

Настоящая работа посвящена анализу современных трендов экономической кибербезопасности. В работе проанализирована динамика кибератак за последние пять лет, показаны основные тренды ушедшего 2018 г. Анализ показал большую вариативность и разнообразие подходов со стороны киберкриминала: глобальный шпионаж, финансовые атаки, мошенничество с картами, кража информации и фишинг, сетевые атаки и перехват трафика, криптоджекинг. На основании систематизации данных от фирм, занимающихся кибербезопасностью, предпринята попытка предсказать киберугрозы, ожидающие нас в ближайшем будущем. Проведенное исследование показало, что основные проблемы стоит ожидать от умных кибератак, построенных на новейших технологиях искусственного интеллекта (ИИ) и машинного обучения (МО), а также использовании уязвимостей интернета вещей. Индустрия киберпреступности будет все более консолидироваться, основное направление — автоматизация и постановка на поток преступной кибердеятельности, новые технологии будут дальше снижать себестоимость поиска уязвимостей и разработки средств взлома при ускорении скорости и масштаба атак. Для эффективной борьбы с новыми вызовами необходим комплексный эшелонированный подход с использованием тех же инновационных технологий ИИ и МО, которые применяются хакерами. Мелкий и средний бизнес получит возможность покупки сервиса кибезащиты. По-прежнему ключевым вопросом и вечным трендом остается необходимость повышения внутренней ИТ-культуры внутри компании.

Ключевые слова: кибербезопасность; цифровая экономика; фишинг; вирусное ПО; компрометация данных; интернет вещей; искусственный интеллект; машинное обучение

Для цитирования: **Шитова Ю.Ю., Шитов Ю.А. Современные тренды экономической кибербезопасности. *Мир новой экономики*. 2019;13(3):22-30. DOI: 10.26794/2220-6469-2019-13-4-22-30**

ORIGINAL PAPER

Contemporary Trends in Economic Cybersecurity

Yu. Yu. Shitova
Russian State Humanitarian University, Moscow, Russia;
The University "Dubna", Dubna, Russia
https://orcid.org/0000-0001-6885-9047

Yu.A. Shitov
Institute for Nuclear Research, Dubna, Russia
https://orcid.org/0000-0002-0184-418X

ABSTRACT

This paper is devoted to the analysis of modern trends in economic cybersecurity. We analysed the dynamics of cyber-attacks over the past five years and, particularly, pointed on the main trends of 2018 year. Our analysis

showed great diversity and variety of cyber-criminal actions: global espionage, financial attacks, card fraud, information theft and phishing, network attacks and traffic interception, cryptographers and extortionists, cryptojacking. Further, we attempted to predict cyber threats that await us soon. We expected the main problems come from smart cyber-attacks, based on the latest technologies of artificial intelligence (AI) and machine learning (ML), as well as exploiting the vulnerabilities of the Internet of Things. Therefore, we ought to apply integrated approaches using the same innovative technologies. The cyber-crime industry will increasingly consolidate — the efforts will be focused on automating and streaming criminal cyber activities, and new technologies will further reduce the cost of searching for vulnerabilities. It means development of hacking tools while accelerating the speed and scale of attacks. We must implement an integrated, echeloned approach with the same innovative technologies of AI and MO used by hackers, to fight effectively with future cyber threats. Small and medium businesses will have the opportunity to purchase a cyber-defence service. An improvement of the internal IT culture in the company remains the critical issue, which is still a weak link in the chain and the target of cyber-attacks. We discuss the measures of legislative state support in Europe and Russia against cybercrime in the final section of the paper, followed by conclusion.
Keywords: cybersecurity; digital economy; phishing; virus software; data compromise; Internet of Things; artificial intelligence; machine learning

For citation: **Shitova Yu. Yu., Shitov Yu.A. Contemporary trends in economic cybersecurity.** ***Mir novoj ekonomiki = World of the New Economy*****. 2019;13(4):22-30. DOI: 10.26794/2220-6469-2019-13-4-22-30**

ВВЕДЕНИЕ

Основным глобальным трендом жизни современного человека и общества был и остается все больший и больший уход в область онлайн-существования. Этому объективному революционному изменению жизни невозможно и бессмысленно сопротивляться. Но возможно и крайне необходимо учитывать возникающие в связи с онлайн-существованием новые возможности в бизнесе и новые угрозы во всех аспектах общественной жизни: политических, личных, экономических.

В данной работе упор делается на экономические аспекты киберугроз — проблемы, возникающие у людей, компаний и целых стран в связи онлайн-преступностью различного рода. Основные усилия будут направлены на ретроспективную оценку текущего состояния дел.

Прежде чем приступить к изложению материала, отметим, что ровно 15 лет назад мы подробно анализировали экономику спама, которая является одним из направлений нелегитимной киберактивности [0, 2]. Настоящее исследование можно условно назвать «***Экономика спама v.2.0***» (следуя модному тренду нумерации версий). В его рамках очень интересно сравнение той и сегодняшней ситуации с киберпреступностью в историческом аспекте. С одной стороны, можно удивиться, насколько далеко шагнули современные кибертехнологии. С другой стороны, не менее удивительно, что многие человеческие слабости, используемые при помощи социальной инженерии, остаются все теми же и через 15 лет…

ДИНАМИКА ХАКЕРСКОЙ АКТИВНОСТИ

Промчалися красные грозы,
Победа настала кругом,
Утрите суровые слезы
Пробитым в боях рукавом.

Песня из кинофильма «Собачье сердце».

Несмотря на большое количество публикаций о противоправной деятельности в интернете, отслеживать динамику событий во времени (по годам) представляется достаточно сложной задачей. И этому есть несколько причин.

Во-первых, вся хакерская среда априори старается максимально скрыть и замаскировать следы своей деятельности. Во-вторых, большинство субъектов, пострадавших от этой деятельности (люди, фирмы, государство), предпочитают скрывать события (инциденты) компрометации своих ИТ-ресурсов для сохранения репутации. В-третьих, не существует единых стандартов оценки деятельности в этой сфере — универсальных методик классификации действий, расчета причиненного ущерба и т.д. Поэтому фирмы, занимающиеся бизнесом по кибербезопасности, делают анализ и мониторинг ситуации по собственным различающимся методикам, тонкости которых зачастую не раскрываются, а в пресс-релизах выдаются только конечные цифры, которые невозможно проверить. В итоге это приводит к сильному разбросу при оценке одной и той же деятельности разными фирмами.

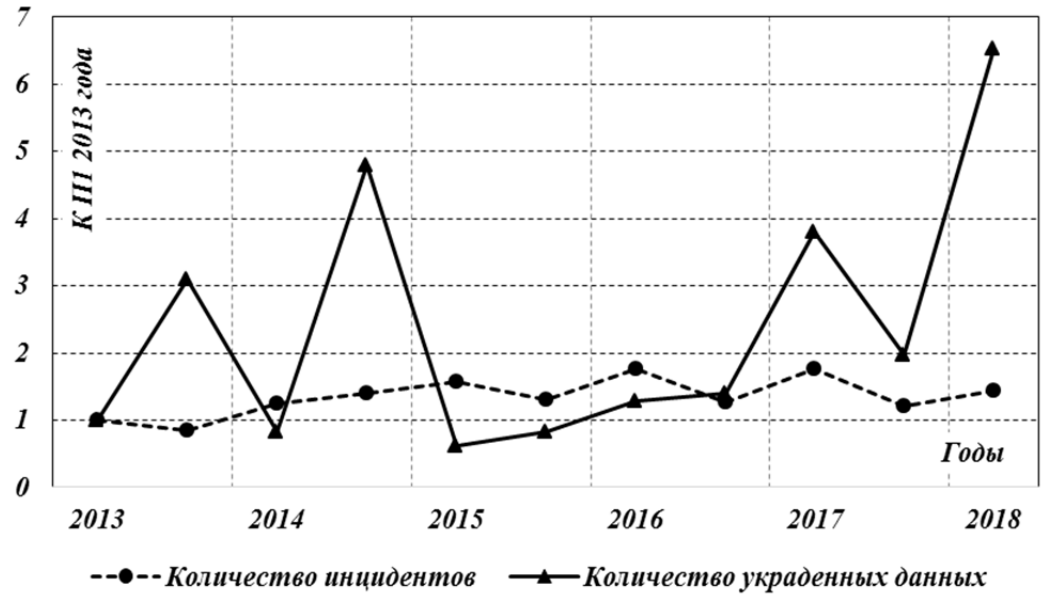

Рис. 1 / Fig. 1. **Динамика успешных кибератак, приведших к компрометации данных* / The dynamics of successful cyber-attacks leading to data compromise**

Источник / Source: Gemalto.

* Данные показаны в отношении к первому полугодию 2013 г., в котором было зарегистрировано 659 атак и скомпрометировано данных в размере 513 млн записей.

Однако в этом хаосе и разнобое информации ценными являются редкие попытки расчета системных индикаторов, основанных на публичной и прозрачной методике оценки. Анализ временных рядов таких показателей представляет собой интерес с точки зрения научного подхода к анализу временной динамики противоправной деятельности в киберпространстве.

Один из таких примеров — **Индекс уровня компрометации** (**Breach Level Index**, **BLI**), расчет которого предложен и осуществляется компанией Gemalto с 2013 г. [3] раз в полгода (https://www.gemalto.com/). Компания ведет подсчет количества успешных атак (инцидентов), приведших к компрометации данных, которые анализируются в разрезе ряда показателей: количества украденных данных (записей), типов атак, пострадавших отраслей бизнеса, географии и др. Динамика BLI будет нами представлена в данном разделе.

Количество атак в динамике с 2013 г. показано на *рис. 1*. Из него видно, что общее количество атакующих действий не сильно изменялось в течение исследуемого периода. Однако количество скомпрометированных данных серьезно увеличилось в последние годы. Особый прорыв случился в первой половине 2018 г., когда количество украденных данных выросло в 6,5 раза по сравнению с первым полугодием 2013 г. О причинах такой ситуации речь пойдет далее, когда будет обсуждаться текущее положение дел в отрасли.

Типы атак на ИТ-ресурсы во временной динамике показаны на *рис. 2*. Как видно из графиков, лидирующими инцидентами являются кражи личных данных. На втором месте — доступ к финансовым ресурсам жертв (см. *рис. 2, слева*). При этом по объему украденных данных (см. *рис. 2, справа*) эти два основных типа атак соревнуются между собой, сменяя лидерство во времени. Периодически в этот процесс вмешиваются и другие типы, к примеру половина украденных данных в 2017 г.— это ценная информация (ноу-хау и чувствительные бизнес-данные).

Изменяющаяся картинка по доле компрометированных данных (колебания графиков на *рис. 2, справа*) говорит нам о динамике хакерской активности, которая активно видоизменяется, ищет и пробует разные виды атакующих усилий, что будет подробно обсуждаться далее.

Динамика **атак по источникам** показана на *рис. 3*. Из него видно, что главную угрозу по-прежнему несут атаки извне. Количество атак изнутри неуклонно снижается, оставаясь небольшим по

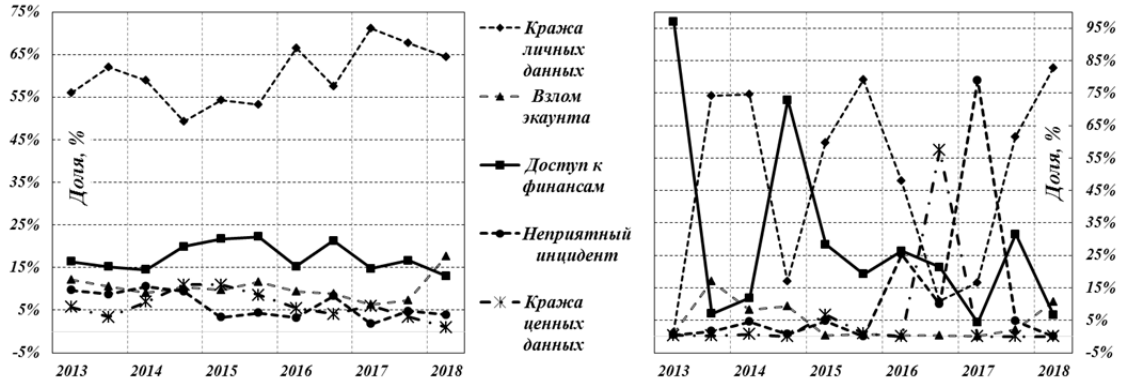

Рис. 2 / Fig. 2. **Динамика успешных кибератак по их типам в долях от общего количества инцидентов (слева) и объема компрометированных данных (справа) / The dynamics of successful cyber-attacks by their types in shares of the total number of incidents (left) and the amount of compromised data records (right)**

Источник / Source: Gemalto.

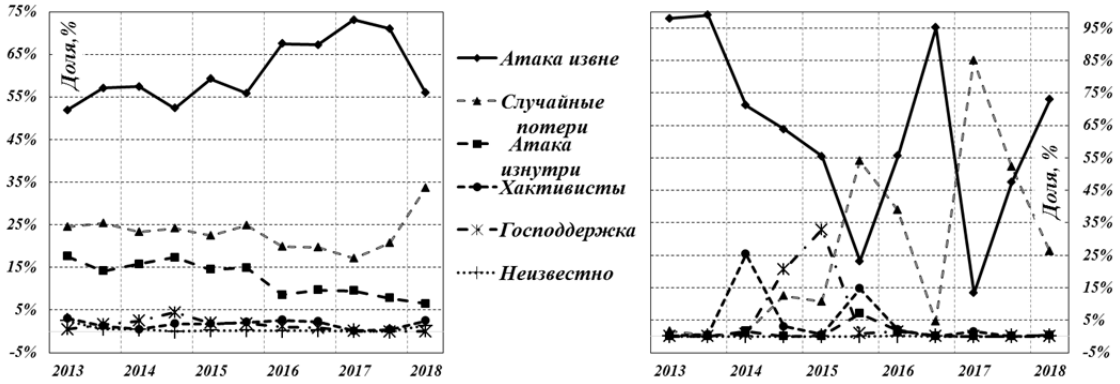

Рис. 3 / Fig. 3. **Динамика успешных кибератак по источникам в долях от общего количества инцидентов (слева) и объема компрометированных данных (справа) / The dynamics of successful cyber-attacks by sources in shares of the total number of incidents (left) and the amount of compromised data records (right)**

Источник / Source: Gemalto.

доле (за исследуемый период уменьшилось с 15 до 5%). Неожиданно большое количество проходит по типу «случайные потери», причем в 2018 г. объем случайных потерь достиг уровня 35%. На наш взгляд, это опять-таки следствие замалчивания фирмами деталей компрометации с целью сохранения репутации. Возможно, часть данных по этой категории на самом деле связана с другими источниками атак.

Динамика атак по географии (континентам) показана на *рис. 4*. Очевидно, что наиболее привлекательным регионом для кибератак является Северная Америка. Однако в 2018 г. деятельность хакеров резко (до 35%) выросла в Азии и Тихоокеанском регионе. Это подтверждает тот факт, что этот регион начинает претендовать на лидерство в цифровой экономике.

Наконец, динамика **атак по направлениям бизнеса** показана в *таблице*. Неожиданно лидером атак оказалась медицина, что связано с высокой степенью ее интернетизации в Северной Америке, являющейся главным объектом хакерских атак, как обсуждалось выше. Традиционно высок уровень атак на финансы (деньги), государственный сектор (секреты), технологические компании (ноу-хау в области ИТ). Большое количество инцидентов в сфере образования, по-видимому, связано с практикой обучения хакеров, заметную долю которых составляют студенты. Высока доля атак на ритейлеров при неочевидных причинах. В последнее время объектами атак стали промышленность, сервисные услуги, отели, индустрия развлечений. Тем самым, география атакуемого бизнеса неуклонно расширяется.

Подводя итоги анализа динамики киберугроз, стоит отметить, что хакерская активность увеличи-

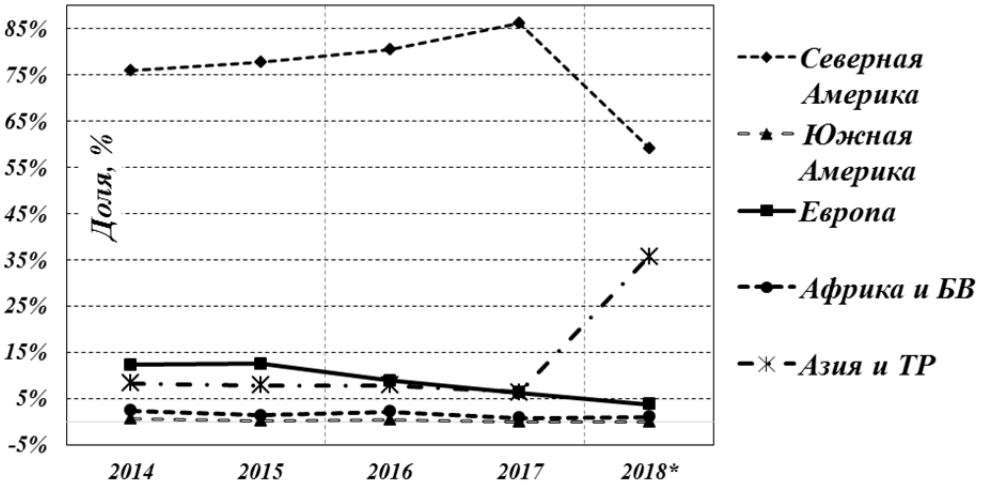

Рис. 4 / Fig. 4. **Динамика успешных кибератак по географии (континентам) / The dynamics of successful cyber-attacks by geography (continents)**

Источник / Source: Gemalto.

Таблица / Table

Динамика успешных кибератак по направлениям бизнеса (единицы — количество подтвержденных успешных случаев) / The dynamics of successful cyber-attacks by businesses (units are the number of confirmed successful cases)

Отрасль	Годы										
	2013		2014		2015		2016		2017		2018
	П1	П2	П1	П2	П1	П2	П1	П2	П1	П2	П1
Медицина	176	170	242	209	239	215	301	236	305	223	256
Другие отрасли	152	111	138	137	176	140	116	46	59	27	159
Финансы	80	85	87	126	154	122	145	97	156	87	134
Образование	8	30	86	88	102	64	108	58	136	78	86
Сервис	0	0	0	1	0	0	0	1	17	88	68
Государство	131	65	114	180	161	138	162	127	118	89	60
Ритейл	56	41	82	115	132	109	122	126	147	75	55
Технология	55	57	73	67	61	63	121	84	85	59	37
Промышленность	0	0	0	0	0	0	20	12	41	24	31
Отели	1	0	0	1	2	0	15	15	26	15	15
Страхование	0	0	0	0	1	1	9	6	11	14	15
Развлечение	0	0	0	0	3	2	20	10	37	9	11
НКО	0	0	0	0	0	0	17	11	18	7	11
Социальные медиа	0	0	0	1	1	1	1	1	6	3	6
Всего	**659**	**559**	**822**	**925**	**1032**	**855**	**1157**	**830**	**1162**	**798**	**944**

Источник / Source: Gemalto.

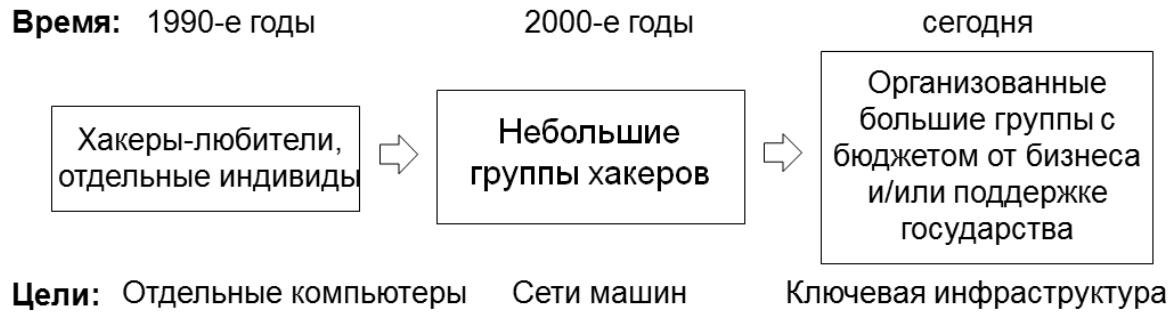

Рис. 5 / Fig. 5. **Динамика организации хакерских угроз / The dynamics of the organization of hacker threats**
Источник / Source: составлено авторами / prepared by the authors.

вается, она активно пульсирует и видоизменяется, варьирует типы и направления атак, географию применения. В следующем разделе мы попытаемся проанализировать основные тренды в этом живом, постоянно изменяющемся и совершенствующемся киберорганизме.

ТЕКУЩИЕ ТРЕНДЫ

Суровые годы уходят
Борьбы за свободу страны…
Песня из кинофильма «Собачье сердце».

Анализ событий 2018 г. позволяет нам оценить главные тренды в киберпреступности, что дает серьезную пищу для размышлений о будущих угрозах. Уровень развития и организации киберугроз уже показывает, что реагирование по факту — это проигрышная стратегия, уже сейчас стратегии безопасности должны строиться по принципу предугадывания и защиты от будущих действий киберпреступников. И это возможно при детальном анализе текущей ситуации, основные моменты которой изложены в настоящем разделе.

ГЛОБАЛИЗАЦИЯ ХАКЕРСКИХ УГРОЗ

Один из самых заметных трендов современности — повышение уровня организации киберпреступников и глобализация решаемых ими задач (*рис. 5*).

Если в начале развития интернета (1990-е гг.) были обособленные хакеры-любители, взламывающие одиночные компьютеры, то в 2000-х гг. стали формироваться хакерские группы, нацелившиеся на атаки компьютеров и компьютерные сети. В настоящее время развитие этого процесса привело к формированию крупных хакерских организаций, финансируемых и поддерживаемых крупными игроками на уровне фигур, близких к криминалу, нелегальному бизнесу, и, самое опасное — правительственным кругам ряда стран. При этом повысился и уровень задач, например хакерские атаки и долгосрочное внедрение в объекты критической инфраструктуры крупных государственных и частных компаний. Целью является шпионаж, саботаж на энергетических и ядерных объектах, транспорте и др. По данным Group IB (https://www.group-ib.ru/resources/threat-research/2018-report.html), в 2018 г. в мире насчитывалось около 40 активных групп, спонсируемых рядом государств, среди которых Северная Корея, Пакистан, Китай, США, Россия, Иран, Украина. Происхождение ряда групп при этом неизвестно.

Пока хакерские атаки на объекты критической инфраструктуры носят единичный характер, к примеру перехват трафика британской фирмы, занимающейся разработкой ядерного оружия [4], но ожидается рост подобных атак.

Шпионаж — одно из ключевых направлений кибератак, спонсируемых Китаем, Северной Кореей и Ираном (основная тройка). Наиболее атакуемый регион — Азиатско-Тихоокеанский (АТ). В 2017–2018 гг. тут были активны более 20 хакерских групп — больше, чем в США и Европе. Это подтверждалось и динамикой атак по географии (см. *рис. 4*), где АТ попал в зону особого интереса в 2018 г. (35% мировых кибератак). Еще один из актуальных трендов глобального уровня — взлом домашних и персональных устройств крупных должностных лиц государства и бизнеса.

Финансовые атаки на финансово-коммерческие фирмы с целью кражи денег, очевидно, остаются в тренде как основной способ заработка хакерских групп. Самыми опасными для банков являются группы Silenc, MoneyTaker, Lazarus и Cobalt. Они способны взломать многостороннюю и хорошо

изолированную банковскую онлайн-систему и снять деньги. Три группы из четырех — русскоязычные.

По данным Group IB (https://www.group-ib.ru/resources/threat-research/2018-report.html), в среднем в России взламывается 1–2 банка в месяц, со средним ущербом около 2 млн долл. США. Количество атак в 2018 г. выросло в 3 раза по сравнению с предыдущим годом, а скорость вывода денег наличными — всего 8 минут. Несмотря на аресты, продолжается процесс консолидации и роста хакерских групп, появляются новые, еще более изощренные методы, происходит быстрый «обмен опытом» и совместные координированные действия различных группировок, что затрудняет процесс их идентификации.

Кража персональной информации — еще один тренд, который остается в силе. Речь идет о взломе и воровстве персональных данных у крупных держателей — социальных сетей, мобильных операторов, интернет-магазинов и т.п. Совсем недавно в сеть попал крупнейший в истории дамп (база данных), содержащий информацию о 2,7 млрд аккаунтов (!), из которых 773 млн — уникальные (https://habr.com/ru/post/436420/). Теперь на сайте специалиста по кибербезопасности и волонтера Троя Ханта (https://haveibeenpwned.com/), **где каждый обязан проверить свой адрес почты на предмет компрометации пароля**, содержится информация о более чем 6,5 млрд паролей, украденных у самых различных сайтов и фирм (Myspace, Linkedin, NetEase и др.).

Мошенничество с банковскими картами остается в числе наиболее опасных угроз для физических лиц. Данные карт продолжают утекать преступникам по разным каналам. К сожалению, чаще всего утечка информации по картам происходит в онлайн-фирмах, интернет-магазинах и т.п., где иногда карточные данные пользователей могут храниться в открытом виде и даже индексироваться поисковыми системами (!). Это связано с экономией средних и мелких фирм на программистах и дырах в коде. Поэтому рынок **кардинга** — воровства денег с украденного «картона» (пластиковых карт) — продолжает существовать. В 2018 г. таким образом было украдено 663 млрд долл. США (https://www.group-ib.ru/resources/threat-research/2018-report.html). Интересен тот факт, что уровень защиты в российских интернет-компаниях намного выше, чем на Западе. Поэтому **кардеры** практически всегда обналичивают деньги с ворованных карт через иностранные онлайн-фирмы, прежде всего США и Великобритании.

Веб-фишинг — метод хищений через поддельные веб-сайты известных брендов — еще один тренд, который показывает устойчивый рост во всем мире. Подделки под российские бренды осуществляют 26 групп, а общее количество успешных фишинговых атак в 2018 г. составило 1274 в день (против 950 в день годом ранее). В целом в России в 2018 г. при помощи веб-фишинга было похищено более 250 млн руб. (https://www.group-ib.ru/resources/threat-research/2018-report.html).

Атака сетевых устройств и перехват трафика — самый свежий тренд развития киберпреступности, заключающийся во взломе не конечных компьютеров, а сетевых устройств, управляющих сетевым трафиком. Взламывая их операционные системы или подменяя физически (просто заменой узла), преступники получают огромные возможности. Дополнительный момент тут — **уязвимость протоколов маршрутизации** (управление потоками данных согласно адресам). В сочетании эти два фактора позволяют осуществлять как простое воровство траффика (анализ и кража данных, проходящих по узлу), так и сложные комбинации с подменой сетевых адресов, позволяющих перенаправлять траффик с настоящих на фейковые фишинговые сайты. Наиболее заметные атаки уходящего года — перехват трафика 1300 адресов Amazon с целью маскировки под криптобиржу MyEtherWallet с последующей кражей криптовалюты на сумму 150 тыс. долл. [5], перехват трафика двух десятков финансовых организаций, включая MasterCard, Visa, Symantec, Verisign [6]. Но самая нетривиальная схема была реализована осенью 2018 г., когда операция злоумышленников, названная ***3ve***, позволила перехватить трафик более 1,5 млн IP-адресов и заставить рекламные компании поверить, что миллиарды показов интернет-банеров действительно были увидены реальными пользователями (https://www.us-cert.gov/ncas/alerts/TA18–331A). Для рекламных компаний эта атака обошлась в 29 млн долл.

В дальнейшем нас ждет расширение вариантов атак на сетевую инфраструктуру, и этот тренд заставляет производителей и пользователей сетевого оборудования совершенствовать свою защиту (https://habr.com/ru/company/cisco/blog/434250/).

Шифровщики и вымогатели (**ransomware**) — отдельный тип вирусного ПО, являющегося особо опасным в экономическом плане. Проникая на машины, вредоносный код данного типа шифрует данные и требует денежный выкуп за расшиф-

ровку с владельцев компьютеров. Судьбоносным в этом отношении стал 2017 г., ознаменовавшийся эпидемией вируса WannaCry. С сотнями тысяч зараженных и ставших непригодными для использования компьютеров, которые оказались шантажированными киберпреступниками, WannaCry в буквальном смысле «заставил рыдать» множество компаний и частных лиц по всему миру. За WannaCry появились множество других последователей: Petya, NotPetya, Goldeneye, BadRabbit, Reyptson, Leakerlocker, Osiris, WYSIWYE и др.

В 2017 г. количество атак с помощью вымогателей выросло в 35 раз по сравнению с предыдущим годом. Ежедневно происходило более 4000 атак вымогателей, заражающих от 30 до 500 тыс. устройств в месяц. Финансовый ущерб стремительно растет: выплаты по выкупу увеличились с 24 млн долл. в 2015 г. до более 850 млн долл. в 2016 г., а в 2017 г. эта цифра превысила 1 млрд долл. Увеличивается сумма, которую преступники требуют на каждую атаку — с 294 долл. в 2015 г. до 619 долл. в 2016 г. [7].

Тем не менее самая большая опасность — не в сумме денег, а в угрозе бизнесу. Каждая пятая компания, подвергшаяся атаке вымогателей, была вынуждена закрыть свой бизнес, еще 63% организаций ощутили вред, угрожающий существованию бизнеса. В 48% произошла потеря данных или оборудования, а из 42%, заплативших выкуп, четверть были обмануты. Кроме того, из-за атак на критическую инфраструктуру (например, здравоохранения), в 3,5% случаев была угроза жизни [7].

Несмотря на то что 2018 г. оказался более спокойным, расслабляться не стоит. Практически все фирмы, занимающиеся кибербезопасностью, уверены, что кража данных с требованием выкупа остается важным направлением кибератак как один из основных каналов заработка преступников. Поэтому следует быть готовым к новым угрозам на качественно новом уровне, что будет обсуждаться в следующем разделе.

Атаки на мобильные телефоны. Прошедший год выдался относительно спокойным в России. Количество хищений с помощью Android-троянов в России снизилось почти в три раза. Сократился и средний размер хищений: 7 тыс. руб. в 2018 г. против 11 тыс. руб. в 2017 г. (https://www.group-ib.ru/resources/threat-research/2018-report.html). На международном рынке ситуация противоположная: наблюдается рост атак. В 2018 г. было выявлено 6 новых троянов для ПК (IcedID, BackSwap, DanaBot, MnuBot, Osiris и Xbot). Выложены либо проданы исходные коды еще 5 троянов. Зараженные мобильные гаджеты (прежде всего, смартфоны и планшеты) рассматриваются хакерами как способ проникновения в закрытые корпоративные сети, куда входят владельцы инфицированных устройств.

Аппаратные уязвимости. Еще один серьезный источник современных угроз. Речь идет о поисках брешей и уязвимостей в аппаратном обеспечении ИТ-ресурсов: микропроцессорах, чипах, роутерах и т.д. Уязвимости такого рода очень тяжело обнаружить и устранить методами программного обеспечения. Ранее поиск такого рода уязвимостей был очень трудной задачей, требующей высококвалифицированного труда. Однако сегодня есть предпосылки к облегчению и ускорению процесса поисков, которые будут обсуждаться в следующем разделе. В прошлом году был обнаружен целый ряд критических аппаратных уязвимостей: Meltdown, Specter, AMD. Появление таких угроз, которые не устраняются стандартными методами, представляет серьезную опасность. Похожая ситуация с вредоносным кодом для виртуальных сред, гипервизоров, единого расширяемого интерфейса прошивки (BIOS/UEFI). Для всех трех уже обнаружены пилотные версии вирусов, а группа HackingTeam еще в 2014 г. даже показала руткит (набор хакерских инструментов) для UEFI. Хотя вирусных эпидемий по этим каналам еще не было, но они очень вероятны в будущем (https://habr.com/ru/post/436420/).

Криптовалюты и майнинг. Несмотря на заявления о надежности криптовалюты, в 2017–2018 гг. было ограблено 14 криптовалютных бирж при общем ущербе 882 млн долл. Отдельным направлением является **криптоджекинг** (скрытый майнинг криптовалют), на зараженных машинах сумма прямого ущерба оценена от 0,5 до 18 млн долл. (https://www.group-ib.ru/resources/threat-research/2018-report.html). Такой огромный разброс еще раз показывает нам, как сложно вести количественные оценки в данной сфере. И еще один момент. На наш взгляд, из-за сильного падения цен на биткоины интерес к этим махинациям должен пойти на убыль, как предсказывает большинство фирм, занимающихся кибербезопасностью.

В следующей работе будет предпринята попытка предсказать тренды недалекого будущего в сфере экономической кибербезопасности, показать основные средства защиты и меры государственной поддержки в борьбе с киберкриминалом.

СПИСОК ИСТОЧНИКОВ/REFERENCES

1. Шитов Ю. Экономика спама: Компьютерра онлайн. Коммерческая подноготная спамерства. URL: https://old.computerra.ru/hitech/spam/206281/.
   Shitov Yu. The Economics of spam: Computerra online. Commercial background of spamming. URL: https://old.computerra.ru/hitech/spam/206281/. (In Russ.).
2. Шитов Ю. Эскалация конфликта. URL: https://old.computerra.ru/hitech/spam/206294/.
   Shitov Yu. Escalation of the conflict. URL: https://old.computerra.ru/hitech/spam/206294/. (In Russ.).
3. Stiennon R. Categorizing data breach severity with a breach level index. URL: https://breachlevelindex.com/pdf/Breach-Level-Index-WP.pdf.
4. Madory D. UK traffic diverted through Ukraine. Research. 13.05.2015. URL: https://dyn.com/blog/uk-traffic-diverted-ukraine/.
5. Madory D. BGP hijack of Amazon DNS to steal crypto currency. URL: https://dyn.com/blog/bgp-hijack-of-amazon-dns-to-steal-crypto-currency/.
6. Toonk A. Case AS 12389. URL: https://bgpmon.net/bgpstream-and-the-curious-case-of-as12389/.
7. Jarvis J. Ransomware: Are you paying attention? fortintet blog. URL: https://www.fortinet.com/blog/industry-trends/ransomware-are-you-paying-attention.html.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Юлия Юрьевна Шитова — доктор экономических наук, доцент, профессор кафедры маркетинга и рекламы, Российский государственный гуманитарный университет, Москва, Россия; профессор кафедры экономики, Университет «Дубна», Дубна, Россия
yu_shitova@mail.ru
Юрий Александрович Шитов — кандидат физико-математических наук, старший научный сотрудник, Объединенный институт ядерных исследований, Дубна, Россия
shitov@jinr.ru

ABOUT THE AUTHORS

Julia Y. Shitova — Doctor of Economics, Professor of the Department of Marketing and Advertising of the Russian State Humanitarian University, Professor of the Department of Economics of the University “Dubna”, Dubna, Russia
yu_shitova@mail.ru
Yury A. Shitov — Ph.D. (Math.), Senior researcher of the Joint Institute for Nuclear Research, Dubna, Russia
shitov@jinr.ru

Статья поступила 08.07.2019; принята к публикации 30.07.2019.
Авторы прочитали и одобрили окончательный вариант рукописи.
The article received on 08.07.2019; accepted for publication on 30.07.2019.
The authors read and approved the final version of the manuscript.