Романов Александр Олегович,
студент, ФВУНЦ ВВС «ВВА»,
РФ, г. Челябинск
Romanov Alexander Olegovich
student, FVUNTS VVS " VVA "
of the Russian Federation, Chelyabinsk

Научный руководитель:
Клепиковский Алексей Александрович
доцент 1-й кафедры
"Кафедра тактики и общевоенных дисциплин"
РФ, г. Челябинск
Klepikovsky Alexey Alexandrovich
Associate Professor of the first department
"Department of Tactics and General Military Disciplines"
Russian Federation, Chelyabinsk

НОВЫЕ ТРЕНДЫ И ТЕХНОЛОГИИ В СФЕРЕ МОШЕННИЧЕСТВА
NEW TRENDS AND TECHNOLOGIES IN THE FIELD OF FRAUD

Аннотация: Целью исследования является анализ и систематизация информации о новых и перспективных трендах и технологиях, используемых в мошенничестве, чтобы спрогнозировать будущие векторы развития мошеннических схем и выявить потенциальные уязвимости, требующие внимания со стороны экспертов в области кибербезопасности, финансовых институтов и правоохранительных органов.

Материалы и методы. Использованы следующие методы: теоретический анализ и обобщение литературных источников, математические и статические обработки результатов исследования.

Abstract: The aim of the study is to analyze and systematize information about new and promising trends and technologies used in fraud, in order to predict the future development vectors of fraudulent schemes and identify potential vulnerabilities that require attention from experts in the field of cybersecurity, financial institutions and law enforcement agencies.

Materials and methods. The following methods were used: theoretical analysis and generalization of literature sources, mathematical and static processing of research results.

Ключевые слова: технологии, мошенничество, кибербезопасность, векторы развития.
Keywords: technologies, fraud, cybersecurity, development vectors.

Современный мир характеризуется повсеместным переходом в онлайн-пространство, что создает как новые возможности для бизнеса, так и новые угрозы для общества в целом. Сопротивляться этому объективному процессу бессмысленно, однако необходимо учитывать возникающие риски, особенно в экономической сфере. В данной статье акцент сделан на экономические аспекты киберугроз, с которыми сталкиваются частные лица, компании и государства. Для понимания текущей ситуации проводится ретроспективный анализ. Следует отметить, что вопросы экономики спама, как одного из видов нелегитимной киберактивности, уже рассматривались ранее [1, 2].

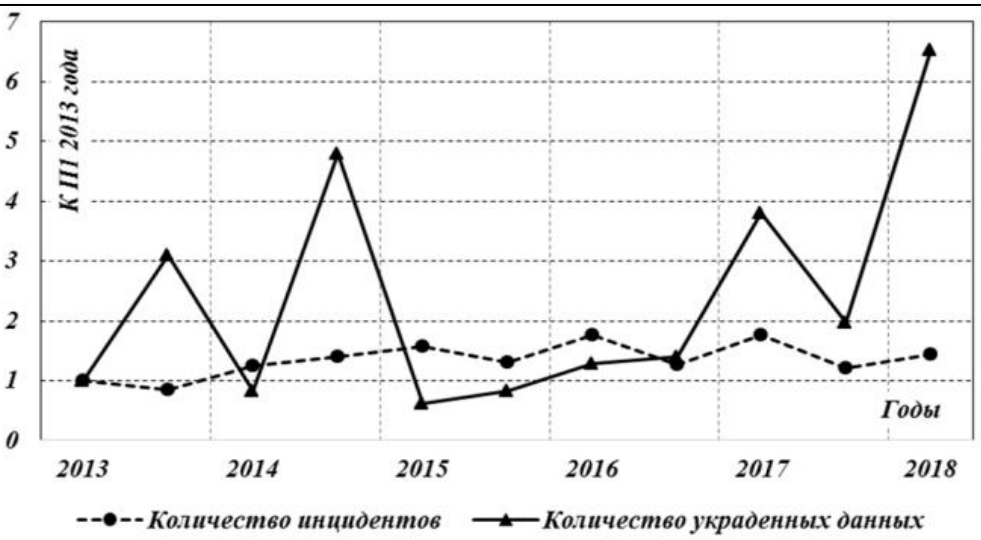

Рис. 1 / Fig. 1. **Динамика успешных кибератак, приведших к компрометации данных* / The dynamics of successful cyber-attacks leading to data compromise**

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.

Анализ динамики кибератак с 2013 года (рис. 1) показывает, что общее количество атак относительно стабильно. Однако, наблюдается значительный рост объема скомпрометированных данных в последние годы. В частности, в первой половине 2018 года количество украденных данных увеличилось в 6,5 раз по сравнению с аналогичным периодом 2013 года. Причины такого резкого скачка будут рассмотрены далее.

Глобализация хакерских угроз: от любителей до государственных операций. Современный мир сталкивается с растущей организацией киберпреступности и глобализацией хакерских атак. Эта эволюция прошла долгий путь:

1990-е: Одиночные хакеры-любители, взламывающие отдельные компьютеры.

2000-е: Формирование хакерских групп, нацеленных на компьютерные сети и системы.

Настоящее время: Крупные хакерские организации, финансируемые криминальными структурами, нелегальным бизнесом и даже правительствами различных стран. Целью этих организаций является не только финансовая выгода, но и шпионаж, саботаж и долгосрочное внедрение в критическую инфраструктуру крупных государственных и частных компаний (энергетика, ядерная отрасль, транспорт и др.). По данным Group IB, в 2018 году насчитывалось около 40 активных хакерских групп, спонсируемых государствами, включая Северную Корею, Пакистан, Китай, США, Россию, Иран и Украину. Происхождение некоторых групп остается неизвестным. Хотя атаки на критическую инфраструктуру пока редки (например, перехват трафика британской компании, разрабатывающей ядерное оружие), ожидается их рост.

Ключевые направления кибератак, спонсируемых Китаем, Северной Кореей и Ираном:

Шпионаж.

Азиатско-Тихоокеанский регион (АТ) является наиболее атакуемым. В 2017-2018 годах здесь действовали более 20 хакерских групп (больше, чем в США и Европе). В 2018 году 35% мировых кибератак были направлены на АТ. Взлом домашних и персональных устройств крупных должностных лиц государства и бизнеса

Финансовые атаки на банки и коммерческие компании с целью кражи денежных средств остаются важным направлением деятельности хакерских групп.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, 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 – уникальны. Теперь на сайте специалиста по кибербезопасности и волонтера Троя Ханта, 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 [8] 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.

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 [8]. 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 интернетбанеров

действительно были увидены реальными пользователями. 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. 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 расшифровку 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 [8]. 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. 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 [8] 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. 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. 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 [8].

Список литературы:

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.) (дата обращения 10.05.2025)

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.) (дата обращения 10.05.2025)

3. Stiennon R. Categorizing data breach severity with a breach level index. URL: https://breachlevelindex.com/ pdf/Breach-Level-Index-WP.pdf (дата обращения 10.05.2025)

4. Madory D. UK traffic diverted through Ukraine. Research. 13.05.2015. URL: https://dyn.com/blog/uk-trafficdiverted-ukraine/ (дата обращения 10.05.2025)

5. Madory D. BGP hijack of Amazon DNS to steal crypto currency. URL: https://dyn.com/blog/bgp-hijack-ofamazon-dns-to-steal-crypto-currency/ (дата обращения 10.05.2025)

6. Toonk A. Case AS 12389. URL: https://bgpmon.net/bgpstream-and-the-curious-case-of-as12389/ (дата обращения 10.05.2025).

7. Jarvis J. Ransomware: Are you paying attention? fortintet blog. URL: https://www.fortinet.com/blog/industrytrends/ransomware-are-you-paying-attention.html (дата обращения 10.05.2025)

8. 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 (дата обращения 10.05.2025)