Nr. 1 (3) 2021

CZU 338:004
DOI 10.5281/zenodo.5236346

ТОВАРЫ И УСЛУГИ В ТЕНЕВОЙ ЦИФРОВОЙ ЭКОНОМИКЕ[1]

Сергей ОХРИМЕНКО
Республика Молдова, Кишинёв
Молдавская экономическая академия, Лаборатория информационной безопасности
доктор экономических наук, профессор
e-mail: osa@ase.md

Григорий БОРТЭ
Республика Молдова, Кишинёв
FusionWorks
кандидат экономических наук
e-mail: grigori.borta@gmail.com

Сергей БАЖЕНОВ
Россия, Москва
Science Horizons Foundation
кандидат философских наук
e-mail: sbazhenov@mail.ru

Елена БАЖЕНОВА
Россия, Ростов-на-Дону
Южный федеральный университет, Институт социологии и регионоведения
кандидат экономических наук, доцент
e-mail: ebazhenova@mail.ru

Дмитрий АБРОСИМОВ
Россия, Ростов-на-Дону
Южный федеральный университет, Институт философии и социально-политических наук кандидат политических наук, доцент
e-mail: dabrosimov@mail.ru

В условиях бурной цифровизации всех аспектов жизни человека и общества недостаточно внимания уделяется вопросам формирования латентных негативных тенденций, в которых особая роль принадлежит теневой цифровой экономике. Мы применили системный подход[2] и рассмотрели проектную природу осуществления хозяйственной деятельности в рамках теневой цифровой экономики. В итоге, мы определили базовую структуру «теневого» проекта по созданию продукта или услуги в сфере теневой цифровой экономики, организованного преступной группой. Также мы определили потенциальные угрозы и инциденты информационной безопасности, порождаемые в рамках теневой цифровой экономики.

[1] Статья подготовлена в рамках договора о сотрудничестве и совместной деятельности между Молдавской экономической академией (Республика Молдова, Кишинёв) и Южным федеральным университетом (Россия, Ростов-на-Дону) № 3/06.01.2021.

[2] КЛЕЙНЕР, Г. *Экосистема предприятия в свете системной экономической теории*. В: КЛЕЙНЕР, Г. Б., (ред.) *Стратегическое планирование и развитие предприятий*: материалы Девятнадцатого всероссийского симпозиума Москва, 10–11 апреля 2018, ЦЭМИ РАН, 2018, с. 88–97.

***Ключевые слова**: цифровая экономика, теневая цифровая экономика, информационная безопасность, угрозы информационной безопасности, кибербезопасность.*

MĂRFURI ȘI SERVICII ÎN ECONOMIA DIGITALĂ TENEBRĂ

În contextul digitalizării rapide a tuturor aspectelor vieții și societății umane, nu se acordă suficientă atenție formării tendințelor negative latente, în care economia digitală subterană joacă un rol special. În acest articol ne propunem o abordare sistematică a temei respective și am luat în considerare natura proiectării desfășurării activităților economice în cadrul economiei digitale subterane. Prin urmare, am identificat structura de bază a unui proiect „privind abordarea tenebră (subterană)" pentru a crea un produs sau serviciu în economia digitală subterană, organizat de un grup infracțional și am identificat, de asemenea, potențiale amenințări și incidente de securitate a informațiilor generate în economia digitală subterană..

***Cuvinte-cheie**: economie digitală, economie digitală tenebră; securitatea informațiilor, amenințări la adresa securității informațiilor; securitate cibernetică.*

GOODS AND SERVICES IN THE SHADOW DIGITAL ECONOMY

In the context of rapid digitalization of all aspects of human life and society, not enough attention is paid to the formation of latent negative trends, in which the shadow digital economy plays a special role. We applied a systematic approach and considered the design nature of carrying out economic activities within the shadow digital economy. As a result, we have identified the basic structure of a "shadow" project to create a product or service in the shadow digital economy organized by a criminal group. We also identified potential threats and information security incidents generated by the shadow digital economy.

***Keywords:** digital economy, shadow digital economy, information security, threats to information security, cybersecurity.*

BIENS ET SERVICES DANS L'ECONOMIE NUMERIQUE DE L'OMBRE

Dans le contexte de la numérisation rapide de tous les aspects de la vie humaine et celle de la société, on n'accorde pas suffisamment d'attention à la formation des tendances négatives latentes, dans lesquelles l'économie numérique parallèle joue un rôle particulier. Nous avons examiné des activités de l'économie numérique parallèle en appliquant l'approche systémique. Cela nous a permis d'identifier la structure de base du projet de la création d'un produit ou d'un service, élaboré par un groupe criminel au sein de l'économie numérique parallèle, et également identifier des menaces potentielles et les incidents de sécurité informatique générés dans le cadre de l'économie numérique parallèle.

***Mots clés**: économie numérique, économie numérique parallèle, sécurité de l'information, menaces à la sécurité de l'information, la cyber-sécurité.*

Введение

В основе любой деятельности человека лежит информация, характеризующая многие стороны творческих, производственных и сбытовых процессов. Именно поэтому, с широким внедрением в жизнь общества новейших информационных технологий, зародилась новая отрасль знаний – *теневая цифровая экономика* (ТЦЭ), которая объединяет деятельность по продвижению продуктов и услуг «теневой» направленности. Она представляет собой специфическую сферу экономической деятельности, с присущими ей структурой и системой экономических

отношений. «Теневая» специфичность задаётся нелегальностью, неофициальностью, а также криминальным характером экономичес-кой деятельности и сокрытием доходов.

С экономической точки зрения ТЦЭ — это сектор экономических отношений, охватывающий все виды производственно-хозяйственной деятельности, которые по своей направленности, содержанию, характеру и форме противоречат требованиям существующего законодательства и осуществляются вопреки государственному регулированию экономики и в обход контроля над ней.

С технологической точки зрения ТЦЭ — это индивидуальная и коллективная деятельность, являющаяся незаконной, связанная с проектированием, разработкой, распространением, поддержкой и использованием компонента информационных и коммуникационных технологий, скрываемая от общества.

Мы предлагаем определять теневую цифровую экономику как «*все незаконные и скрываемые продукты и услуги, использующие информационные технологии. В качестве наиболее важных экономических элементов данной сферы выделяются следующие: незаконные экономические взаимоотношения, незаконная деятельность, связанная с производством, распространением и использованием запрещённых продуктов и услуг*»[1].

Основу ТЦЭ составляет теневая предпринимательская деятельность, общими чертами которой являются: (1) скрытый, латентный (тайный) характер, то есть та деятельность, которая не регистрируется государственными органами и не находит отражение в официальной отчётности; (2) охват всех фаз процесса общественного воспроизводства (производство, распределение, обмен и потребление); (3) паразитический характер всех процессов, от раскрытия исходного кода программного продукта до монетизации сдачи в аренду ботнетов.

Известный специалист по информационной безопасности А. Лукацкий подчёркивает: «*Мы отмечаем переход киберпреступности на качественно новый уровень, заключающийся в превращении теневого рынка киберкриминала в хорошо отлаженную индустрию, которая полностью повторяет законы мира обычного. Своя разработка, своя поддержка, возврат средств в случае недовольства купленным товаром, сдача в аренду технологий и оборудования, услуги посредников, неотслеживаемые платёжные системы расчётов, партнёрские программы, обналичивание денежных средств и многое другое. Не случайно появляется термин Crime-as-a-Service, означающий превращение рынка киберпреступности в хорошо налаженную машину, работающую со знаком минус*»[2].

Специалисты ведущей информационной фирмы в области противостояния теневой цифровой экономике Digital Shadows определили основные категории

[1] BORTA, G. *The Dark Side of Information Economics*. В: Economica, № XXIII (2 (92), 2015, с. 97–102; ОХРИМЕНКО, С., БОРТЭ, Г. *Новое наполнение науки секьюритологии*. В: Kozera A, Sadowska E (editors), *Nauka i praktyka bezpieczeństwa : księga pamiątkowa Leszka Fryderyka Korzeniowskiego profesora Uniwersytetu Pedagogicznego im Komisji Edukacji Narodowej w Krakowie*. Krakow: Wydawnictwo EAS; 2019, с. 112–47; ОХРИМЕНКО, С., БОРТЭ, Г. *Тень цифровой экономики*. Годишник на Стопанска Академия «ДА Ценов». 2018; БОРТЭ, Г. *Теневая информационная экономика*. Годишен Алманах «Научни Изследвания на Докторанта» Стопанска Академия «ДА Ценов», 2012, с 5; БОРТЭ, Г. Р. *Исторические предпосылки развития теневой информационной экономики.* В: Системи Обробки Інформації, № 4(102), 2012, с. 12–4.

[2] ЛУКАЦКИЙ, А. *Будущее российского рынка информационной безопасности*. В: Век качества., 2015, 2:5 с. 8–9. https://cyberleninka.ru/article/n/buduschee-rossiyskogo-rynka-informatsionnoy-bezopasnosti (дата обращения 04.03.2021).

злоумышленников, у которых есть мотив для злоупотреблений и использования труда удалённых сотрудников[1]. К ним относятся: - *организованная преступность*: группы, занимающиеся киберпреступностью, обладают возможностями и навыками для проведения целевых атак на конечных удалённо работающих сотрудников. Использование личных устройств с меньшим количеством мер безопасности и контроля делает пользовательские приложения более привлекательными для таких операций. Доступ к корпоративным услугам и ресурсам, даже с собственных устройств конечного пользователя, делает цель более привлекательной, поскольку вероятность получения несанкционированного доступа значительно увеличивается;

- *мошенники*: ожидается рост числа попыток мошенничества из-за вспышки COVID-19. Они, вероятно, будут особенно эффективны против сотрудников, которые не привыкли работать на личных и / или мобильных устройствах;
- *злонамеренные инсайдеры*: те пользователи, кто не привык к удалённой работе, могут столкнуться с проблемами из-за случайного раскрытия конфиденциальных данных, ошибок при обмене файлами и т. д.;
- *хактивисты*: фишинговые атаки будут развиваться, особенно сейчас, когда конечный пользователь более уязвим в интернете.

Директор BI.ZONE Д. Самарцев отмечает: «*Сегодня все мы стоим на пороге новой эры киберпреступности, которая будет с каждым годом усиливаться благодаря постоянно эволюционирующим технологиям. Находясь на страже бизнеса и регулярно сталкиваясь с киберугрозами, мы видим, как этот „снежный ком“ уже вырос и разогнался. Мы искренне рады, что такие крупные организации, как ВЭФ, придают большое значение проблеме кибербезопасности, и на сегодняшний день плодотворно сотрудничаем с ними в данной сфере. Ведь только коллаборация усилий на международном уровне позволит гораздо эффективнее выстраивать киберзащиту будущего уже сегодня*»[2].

У. Диксон, глава операционной деятельности Центра кибербезопасности Всемирного экономического форума отмечает: «*Мир лишь начинает свой путь кибербезопасности, и хотя технологии четвёртой промышленной революции несомненно породят новые препятствия, у нас есть много вариантов для инноваций и новых моделей сотрудничества в борьбе с существующими и новыми угрозами*»[3].

Председатель Европейской комиссии У. фон дер Ляйен на выступлении в январе 2021 года на Всемирном экономическом форуме в Давосе, рассказывая о существующих проблемах, от изменения климата до высоких технологий и

[1] FUENTES, M. *Trading in the Dark: An Investigation into the Current Condition of Underground Markets and Cybercriminal Forums*, 2020. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/trading-in-the-dark (дата обращения 04.03.2021); KROPOTOV, V., MCARDLE, R., YAROCHKIN, F. *Commodified Cybercrime Infrastructure: Exploring the Underground Services Market for Cybercriminals*, 2020. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/commodified-cybercrime-infrastructure-exploring-the-underground-services-market-for-cybercriminals (дата обращения 04.03.2021); KROPOTOV, V., MCARDLE, R., YAROCHKIN, F. T*he Hacker Infrastructure and Underground Hosting: Services Used by Criminals*, 2020. https://documents.trendmicro.com/assets/white_papers/wp-the-hacker-infrastructure-and-underground-hosting-services-used-by-criminals.pdf (дата обращения 04.03.2021).

[2] DIXON, W., SAMARTSEV, D. *Three technologies that could define the next decade of cybersecurity*. В: Annual Meeting of the New Champions, 2019. World Economic Forum, 2019.

[3] *Ibidem.*

воздействия COVID-19, напомнила, что год назад в Давосе интенсивно обсуждали процессы цифровизации, но пандемия ускорила эти процессы и для того, чтобы быть успешным, необходимо обратить внимание на «тёмные стороны» цифрового мира[1].

2. Проектный характер ТЦЭ

Как и в реальной экономике, все виды товаров и услуг в теневой цифровой экономике производятся с правильным экономическим подходом к организации их производства. Современные реалии осуществления хозяйственной деятельности в рамках ТЦЭ доказывают необходимость проектного подхода в организации бизнеса. По мнению К. Хелдмана, большинство подобного рода «теневых» проектов вытекают из стратегической необходимости преодолевать сложности внешней среды и трудности в управлении проектом как динамической системой[2]. С точки зрения системного подхода[3], проектная деятельность заключается в управлении отношениями между элементами проекта, для обеспечения достижения цели, поставленной в его рамках.

На рисунке 1 показана базовая структура «теневого» проекта по созданию продукта или услуги в сфере ТЦЭ, организованного преступной группой. Участники проекта – это стороны (физические лица или сформировавшиеся структуры), которые непосредственно вовлечены в реализацию проекта, либо чьи интересы могут быть затронуты при осуществлении проекта.

Рис. 1. *Базовая структура «теневого» проекта по созданию продукта или услуги в сфере теневой цифровой экономики, организованного преступной группой*

Источник: Project Management Institute. A guide to the project management body of knowledge (PMBOK® guide). Project Management Journal. 2008.; ROSE, K., A Guide to the Project Management Body of Knowledge (PMBOK Guide)-Fifth Edition. Proj Manag J. 2013.

По степени вовлеченности в «теневой» проект можно выделить четыре основные группы участников:

1. *Заинтересованные стороны* – стороны, преследующие свои интересы и оказывающие определённое влияние на членов основной команды и команды поддержки, а также на ход работ по проекту, но не вступающие с этими командами в непос-

[1] Von der Leyen U., *Ursula von der Leyen's message to Davos Agenda:* Full transcript, 2021. 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 04.03.2021).

[2] ХЕЛДМАН, К. *Профессиональное управление проектом*: пер. с англ. 7th ed. Москва: БИНОМ, Лаборатория знаний, 2016.

[3] КЛЕЙНЕР, Г. *Экосистема предприятия в свете системной экономической теории*. В: КЛЕЙНЕР, Г. (ред.) *Стратегическое планирование и развитие предприятий: материалы Девятнадцатого всероссийского симпозиума Москва*, 10–11 апреля 2018 г. ЦЭМИ РАН, 2018, с. 88–97.

редственное прямое взаимодействие;
2. *Основная команда* – группа специалистов, непосредственно работающих над осуществлением проекта в тесном контакте друг с другом;
3. *Команда поддержки* – более обширная, чем основная группа, объединяет специалистов и структуры, оказывающие опосредованное содействие членам основной группы, но не участвующие напрямую в осуществлении проекта и достижении его целей;
4. *Конечные потребители* – физические лица и неформальные структуры, использующие созданный в результате проекта продукт или услугу в сфере ТЦЭ в своих целях в соответствии с её назначением и технико-экономическими параметрами.

Как правило, главными участниками «теневого» проекта являются представители заинтересованных сторон:

Инициатор проекта – сторона, заинтересованная в успешном осуществлении проекта и достижении его основных целей, будущий владелец результатов проекта. Инициатор определяет основные требования к результатам проекта, обеспечивает финансирование проекта за счет своих или привлекаемых средств инвестора, может заключать контракты с основными исполнителями проекта.

Куратор проекта – представитель высшего звена организационной структуры, реализующей проект, который курирует проект со стороны инициатора, обеспечивает общий контроль и операционную поддержку проекта в виде финансовых, материальных, человеческих и иных ресурсов. Куратор проекта отвечает за достижение проектом конечных целей непосредственно перед инициатором.

Инвестор – сторона, инвестирующая проект, например, посредством кредитных или заёмных денежных средств. Если инвестор и инициатор не являются одним и тем же лицом, то в качестве инвесторов обычно выступают различные криминальные структуры.

В рамках сформированного «теневого» проектного офиса можно выделить следующих участников проекта:

Руководитель службы безопасности проекта – лицо, курирующее в проекте выполнение всего комплекса охранных функций. Он пресекает несанкционированный сбор и обработку актуальной информации о проекте; изобличает агентуру, осведомителей, а также сотрудников правоохранительных органов; предупреждает и пресекает попытки инфильтрации и вербовки агентуры; контролирует лояльность сотрудников проекта в сочетании с применением мер по их прикрытию от действий правоохранителей.

М*енеджер проекта / Контрактор* – конкретное лицо, ответственное за управление проектом в рамках проектного офиса. Менеджер проекта несет ответственность перед куратором за достижение целей проекта в рамках бюджета, в срок и с заданным уровнем качества, обеспечивает ежедневное управление основной командой проекта, в разрезе всех основных управленческих функций (управление по срокам, затратам, рискам и др.). Менеджер проекта берёт на себя ответственность за выполнение всех работ и услуг по контракту.

Аналитик данных – универсальный специалист, обладающий знаниями в математике, статистике, информатике, компьютерных науках, бизнесе и экономике и занимающийся проведением описательного (дескриптивного) анализа данных и их интерпретацией для нужд проекта.

Мошенники – эксперты-аналитики, создающие новые схемы мошенничества и манипулирования потенциальными жертвами.

Хакеры – эксперты в компьютерной безопасности, осуществляющие поиск и

отработку уязвимостей в информационных системах, приложениях, сетях и т. д.

ИТ-специалисты – специалисты, создающие, поддерживающие и наращивающие технологическую инфраструктуру проекта (сети, серверы, базы данных и т. д.).

Программисты – специалисты, занимающиеся разработкой алгоритмов и кода компьютерных вредоносных программ различной ориентации для нужд проекта.

Аналитик внедрения – специалист, оказывающий конечному потребителю сервис внедрения: подготовку проектной документации, работу с требованиями заказчика, непосредственную тонкую настройку внедряемого продукта.

Вспомогательными участниками «теневого» проекта являются представители команды поддержки:

Субконтрактор – лицо или структура, вступающая в договорные отношения с контрактором и несущая ответственность за выполнение определённых работ и услуг в соответствии с контрактом.

Поставщик – субконтрактор, осуществляющий разные виды поставок товаров и услуг в рамках проекта на контрактной основе – материалы, оборудование, нематериальные активы и др. Типичным примером может служить «теневой» сервис, предоставляющий услуги хостинга, как части преступной инфраструктуры.

Последним звеном в структуре «теневого» проекта, организованного преступной группой, являются:

Торговцы – лица и структуры, перепродающие созданный продукт или услугу в сфере теневой цифровой экономики представителям организованных преступных групп. Одновременно, торговцы через аналитика внедрения обеспечивают обратную связь с проектным офисом в целях повышения качества разработки и сервиса поддержки.

Организованная преступная группа – устойчивая группа лиц, заранее объединившихся для совершения одного или нескольких преступлений, использующая продукт или услугу в сфере теневой цифровой экономики для повышения качества и эффективности своего преступления.

Именно проектный характер всех «теневых» процессов по созданию продуктов и услуг в сфере теневой цифровой экономики позволяет осуществлять их эффективно, надёжно и подконтрольно на протяжении всего жизненного цикла проекта[1].

3. Товары и услуги

Далее мы рассмотрим товары и услуги в теневой цифровой экономике. Быстрое развитие новых технологий обеспечивает достаточно быструю сменяемость аппаратной и программной платформ, придавая товарам и услугам характер постоянной изменчивости. Как только производители выводят на рынок новый продукт или услугу, они сразу становятся объектом пристального внимания представителей криминального мира на предмет их использования для совершения преступления. В силу своей специфики, в цифровой экономике материальные товары крайне малочисленны и обычно относятся к аппаратному обеспечению, в то время как большая часть товаров представляет собой нематериальное программное обеспечение.

3.1. Потенциальные угрозы.

Будем использовать следующие определения:

Потенциальная угроза (Potential Threat): возможная опасность совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю,

[1] *Project Management Institute. A guide to the project management body of knowledge* (PMBOK® guide). Project Management Journal. 2008.

проявляющегося в опасности искажения и потери информации[1].

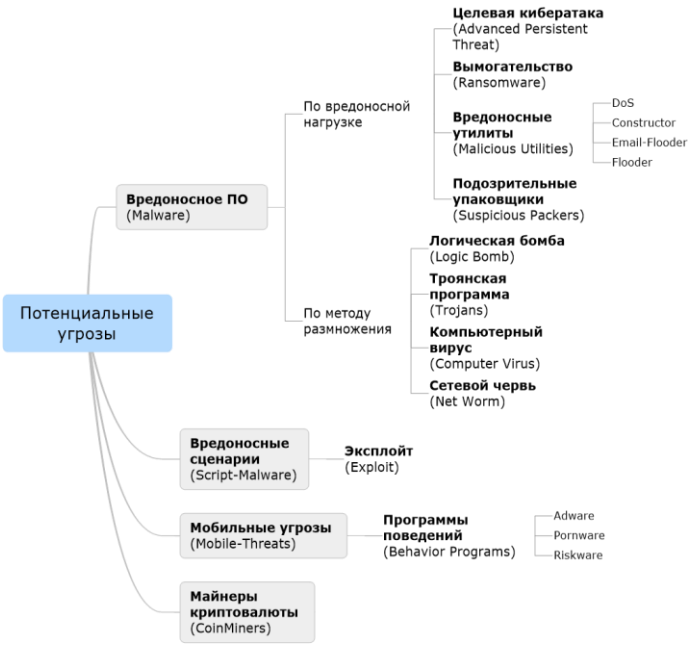

Рис. 2. *Потенциальные угрозы, порождаемые в рамках теневой цифровой экономики.*

Источник: ВИХОРЕВ, С. Классификация угроз информационной безопасности. CNews. 2001. https://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml?print (дата обращения 04.03.2021); Check Point Software. 2021 Cyber Security Report. 2021. https://pages.checkpoint.com/cyber-security-report-2021.html (дата обращения 04.03.2021); Skybox Security. 2021 Vulnerability and Threat Trends Report. 2021. https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox-Security-vulnerability-and-threat-trends-report-2021.pdf (дата обращения 04.03.2021); Verizon. 2020 Data Breach Investigations Report. 2021. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf (дата обращения 04.03.2021); Bremmer I., Kupchan C., Top Risks for 2021. 2021. https://www.eurasiagroup.net/files/upload/top-risks-2021-full-report.pdf (дата обращения 04.03.2021).

Товары и услуги в теневой цифровой экономике являются преимущественно вредоносными, поэтому *первоначально* мы классифицируем их через потенциальные угрозы, которые они непосредственно порождают в рамках ТЦЭ (см. рис. 2).

Вторично, товары и услуги в теневой экономике мы классифицируем и опишем через инциденты информационной безопасности. Для этого мы выделим наиболее авторитетные экспертные подходы и затем сформируем из них авторскую категорию событий.

3.2. Инциденты информационной безопасности.

Будем использовать следующие определения:

1. *Инцидент информационной безопасности* (Information Security Incident): событие безопасности, которое ставит под угрозу целостность, конфиденциальность или доступность информационного актива.
2. *Нарушение* (Breach): инцидент, который приводит не только к потенциальному, но и к подтверждённому раскрытию данных неавторизованной стороне[2].

Рассмотрим базовые категории и типы событий, классифицируемые как компьютерный инцидент, и их международное обозначение. Практически все классификаторы отвечают международным стандартам, таким как ISO/IEC

[1] ВИХОРЕВ, С. *Классификация угроз информационной безопасности*. CNews, 2001. https://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml?print (дата обращения 04.03.2021).

[2] *AT&T Cybersecurity. Chapter Three. Security Incidents: Types of Attacks and Triage Options. In: AlienVault's Insider's Guide to Incident Response*. 2021, с. 48. https://learn-cybersecurity.att.com/c/alien-vault-incident?x=5v9G6V&utm_internal=soc-irlookbook&xs=1248 (дата обращения 04.03.2021).

27035-1:2016 «Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management» и ISO/IEC 27035-2:2016 «Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response».

Эксперты компании Verizon для обеспечения согласованного и недвусмысленного сбора сведений об инцидентах компьютерной безопасности используют словарь для записи событий и обмена инцидентами (VERIS), в котором классифицированы семь основных категорий угрожающих действий: (1) применение вредоносного ПО; (2) взлом; (3) атака через социальные сети; (4) получение инсайдерской информации и неправомерное использование привилегий; (5) физическая кража и потеря ценного актива; (6) ошибка и (7) вредоносная окружающая среда[1].

Агентство Европейского Союза по сетевой и информационной безопасности (The European Union Agency for Network and Information Security) публикует справочную таксономию классификации инцидентов, которая стала результатом совместных инициатив между агентством, группами реагирования на инциденты компьютерной безопасности (CSIRT) и правоохранительными органами ЕС[2].

Лаборатория информационных технологий при Национальном институте стандартов и технологий США (The Information Technology Laboratory at the National Institute of Standards and Technology) рекомендует использовать руководство по обработке инцидентов компьютерной безопасности[3].

Рис. 3. *Потенциальные инциденты информационной безопасности, порождаемые в рамках теневой цифровой экономики.*

Источник: НКЦКИ. Состав технических параметров компьютерного инцидента, указываемых при представлении информации в ГосСОПКА, и форматы представления информации о компьютерных инцидентах. Безопасность пользователей в сети интернет. 2019. https://safe-surf.ru/specialists/article/5252/638030/ (дата обращения 04.03.2021).

На наш взгляд, наиболее полную и непротиворечивую категоризацию инцидентов компьютерной безопасности даёт Национальный координационный центр по компьютерным инцидентам России (НКЦКИ) (см. рис. 3): (1) Заражение вредоносным ПО (Malware); (2) Распространение вредоносного ПО (Malware

[1] *Verizon. 2020 Data Breach Investigations Report*. 2021. Available from: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf (дата обращения 04.03.2021).

[2] ENISA. *Reference Incident Classification Taxonomy. Task Force Status and Way Forward*. 2018. https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy (дата обращения 04.03.2021).

[3] CICHONSKI, P., MILLAR, T., GRANCE, T., SCARFONE, K. *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*. NIST Special Publication, 2012.

Distribution); (3) Нарушение или замедление работы контролируемого информационного ресурса (Availability); (4) Несанкционированный доступ в систему (Intrusion); (5) Попытки несанкционированного доступа в систему или к информации (Intrusion Attempt); (6) Сбор сведений с использованием ИКТ (Information Gathering); (7) Нарушение безопасности информации (Information Content Security); (8) Распространение информации с неприемлемым содержимым (Abusive Content); (9) Мошенничество с использованием ИКТ (Fraud); (10) Уязвимость (Vulnerability)[1]. Далее рассмотрим каждый инцидент информационной безопасности более подробно.

3.2.1. Заражение вредоносным ПО.

Будем использовать следующие определения:

Вредоносное ПО (Malware): (1) любая программа, созданная для выполнения любого несанкционированного, как правило, вредоносного действия на устройстве пользователя; (2) приложение или код, которые ставят под угрозу безопасность пользователя[2].

Каждый день Институт AV-TEST регистрирует более 350 000 новых вредоносных программ и потенциально нежелательных приложений (PUA). Они исследуются и классифицируются в соответствии с их характеристиками и сохраняются (см. рис 4).

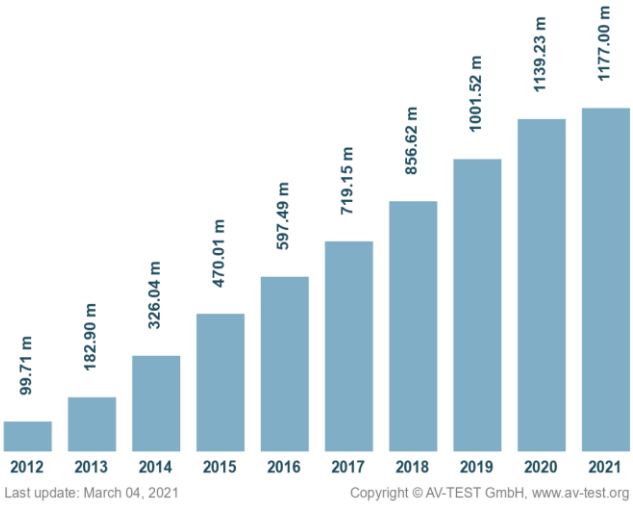

Рис. 4. *Общее количество вредоносного ПО в мире (на 04 марта 2021 года).*
Источник: AV-TEST. Malware. AV-TEST - The Independent IT-Security Institute. 2021. https://www.av-test.org/en/statistics/malware/ (дата обращения 04.03.2021.)

Список вредоносных программ обширен и постоянно пополняется:

Компьютерные вирусы — это вредоносные программы, которые могут воспроизводить сами себя и заражать файл за файлом на компьютере, а также могут распространяться с одного компьютера на другой. Обычно компьютерные вирусы запрограммированы на выполнение разрушающих действий, таких как повреждение или удаление данных. Подвидом данного вида вирусов являются *макровирусы* для Word и Excel, *загрузочные* вирусы; *скрипт-вирусы*, включая batch-вирусы, заражающие оболочку ОС Windows, Java-приложения и т. д.

Компьютерный червь – это вредоносная программа, которая многократно копирует сама себя, но не наносит прямого вреда безопасности. Червь, однажды попавший на компьютер, будет искать способы распространения на другие компьютеры и носители. Если вирус является фрагментом программного кода, добавляющимся к обычным файлам, червь – это самостоятельная программа.

[1] *НКЦКИ. Состав технических параметров компьютерного инцидента, указываемых при представлении информации в ГосСОПКА, и форматы представления информации о компьютерных инцидентах. Безопасность пользователей в сети Интернет*, 2019. https://safe-surf.ru/specialists/article/5252/638030/ (дата обращения 04.03.2021).

[2] *Microsoft. Understanding malware & other threats*. Technical documentation. 2021. https://docs.microsoft.com/ru-ru/windows/security/threat-protection/intelligence/understanding-malware (дата обращения 04.03.2021).

Троянская программа – разновидность вредоносного ПО, проникающая в компьютер под видом легального программного обеспечения и после своего запуска выполняющая вредоносные действия. В отличие от вирусов и червей, троянские программы не умеют распространяться самостоятельно. Как правило, троянцы тайно загружаются в компьютер пользователя и начинают осуществлять несанкционированные им вредоносные действия.

Киберпреступники используют множество троянских программ разных типов, каждый из которых предназначен для выполнения особой вредоносной функции. Наиболее распространены: (1) *бэкдоры* (в их состав часто входят программы-кейлоггеры); (2) *шпионские программы*; (3) *программы для кражи паролей*; (4) *прокси-серверы*, которые преобразуют ваш компьютер в средство распространение спама.

Crimeware – вредоносные программы, созданные для автоматизации совершения финансовых преступлений.

Adware – программы принудительного показа рекламы, воплощающие собой принцип неявной формы оплаты за использование программного обеспечения, осуществляемые за счёт показа пользователю рекламной информации.

3.2.2. Распространение вредоносного ПО.

Будем использовать следующие определения:

Распространение вредоносного ПО (Malware Distribution): передача кому-либо вредоносного программного кода или носителя с таким кодом безвозмездно или за определённую плату электронным или иным способом без раскрытия информации о потенциальной вредоносности данного кода.

Управление и контроль вредоносного ПО (Malware Command and Control), также называемое *C&C* или *C2* относится к тому, как злоумышленники общаются и демонстрируют контроль над заражённой системой. После заражения системы большинство вредоносных программ связывается с сервером, контролируемым злоумышленником (сервером C2), либо для выполнения команд, загрузки дополнительных компонентов или для эксфильтрации информации[1].

3.2.3. Нарушение или замедление работы контролируемого информационного ресурса.

Будем использовать следующие определения:

Нарушение или замедление работы контролируемого информационного ресурса (Availability): злонамеренное или случайное нарушение доступности отдельных сервисов и систем в целом[2].

Основным инцидентом данного вида является *атака типа отказ в обслуживании* (Denial-of-Service, DoS), которая затрудняет или прекращает нормальное функционирование веб-сайта, сервера или другого сетевого ресурса. Это достигается несколькими способами, например, отправлением серверу большого количество запросов, которые он не в состоянии обработать. Работа сервера будет замедлена, веб-страницы будут открываться намного дольше, и сервер может совсем выйти из строя, в результате чего все веб-сайты на сервере будут недоступны.

Другим инцидентом является *распределённая атака типа отказ в обслуживании* (Distributed-Denial-of-Service, DDoS), которая действует аналогично обычной атаке типа «отказ в обслуживании». Однако распределённая атака типа «отказ в обслу-

[1] MONNAPPA, K. Malware *Command and Control (C2). Learning Malware Analysis*, 2018. https://www.oreilly.com/library/view/learning-malware-analysis/9781788392501/17a1735d-9583-4d86-9d1e-8b2735af5168.xhtml (дата обращения 04.03.2021).

[2] SecurityLab. *Глубины SIEM: корреляции «из коробки»*. Часть 3.1. Категоризация событий. SecurityLab by Positive Technologies. 2018. https://www.securitylab.ru/blog/company/pt/345302.php (дата обращения 04.03.2021).

живании» осуществляется с использованием большого количества компьютеров. Обычно для распределённой атаки типа «отказ в обслуживании» хакеры используют один взломанный компьютер в качестве «главного» компьютера, который координирует атаку со стороны других зомби-компьютеров. Как правило, кибер-преступник взламывает главный компьютер и все зомби-компьютеры, используя уязвимость в приложениях для установки троянской программы или другого компонента вредоносного кода.

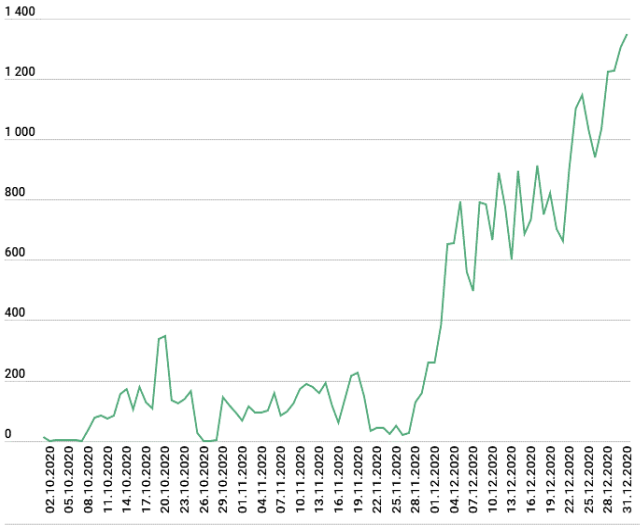

Рисунок 5. *Динамика числа DDoS-атак, Q4 2020 г.*

Источник: SecureList. DDoS-атаки в IV квартале 2020 года. SecureList by Kaspersky. 2021. https://securelist.ru/ddos-attacks-in-q4-2020/100469/ (Просмотрен 04.03.2021).

Существенными инцидентами являются *вывод объекта из строя* (Sabotage) и непреднамеренное *отключение объекта* (Outage).

Ещё одним инцидентом считается *флуд* (Flood) – однотипные нетематические сообщения в интернет-форумах и чатах, зачастую занимающие большие объёмы, которые при определённых условиях также могут приводить к отказу в обслуживании.

3.2.4. Несанкционированный доступ в систему.

Будем использовать следующие определения:

Несанкционированный доступ в систему (Intrusion): (1) доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации; (2) получение доступа к информации лицом, имеющим право на доступ к этой информации в объёме, превышающем необходимый для выполнения служебных обязанностей.

На том или ином этапе совершения преступления выделяют следующие приёмы и методы: (1) *тактические* — предназначенные для достижения ближайших целей (например, для получения паролей) и (2) *стратегические* — направленные на реализацию далеко идущих целей и связанные с большими финансовыми потерями для автоматизированных информационных систем[1].

По методам использования преступником тех или иных действий, направленных на получение несанкционированного доступа к средствам компьютерной техники, можно выделить следующие: (1) перехват информации; (2) неавторизованный доступ; (3) манипуляция; (4) комплексный метод.

Основными способами получения несанкционированного доступа являются: (1) взлом информационных ресурсов (корпоративных сетей, веб-сайтов, облачных сервисов, отдельных компьютеров и мобильных устройств); (2) перехват сообщений (электронная почта, мессенджеры, SMS и пр.); (3) сбор данных (законный или незаконный); (4)

[1] ОХРИМЕНКО, С., ЧЕРНЕЙ, Г. *Угрозы безопасности автоматизированным информационным системам (программные злоупотребления).* НТИ, Серия 1, Организация и методика информационной работы. 1996; 5: с. 5–13.

шантаж, вымогательство, дача взятки; (5) кража информации.

3.2.5. Попытки несанкционированного доступа в систему или к информации.

Будем использовать следующее определение:

Попытка несанкционированного доступа в систему или к информации (Intrusion Attempt): последовательность из нескольких запросов или проб доступа, передаваемых по каналу связи в процессе взаимодействия абонента с системой связи с целью получения разрешения на обмен информацией при отсутствии на это у абонента необходимых прав. Попытка несанкционированного доступа заканчивается как в случае успеха, так и отказа в доступе.

Для отслеживания несанкционированных попыток получения доступа к защищаемым ресурсам организации, используют *мониторинг управления доступом* с помощью систем обнаружения вторжений (Intrusion Detection Systems, IDS) и систем предотвращения вторжений (Intrusion Prevention Systems, IPS). Они нацелены на выявление и регистрацию недостатков в безопасности внутренней инфраструктуры – сетевые атаки, попытки несанкционированного доступа или повышения привилегий, работа вредоносного программного обеспечения и т.д. Различия между ними заключаются лишь в том, что одна может автоматически блокировать атаки, а другая просто предупреждает об этом.

В настоящий момент также применяют межсетевой экран нового поколения (NGFW, Next Generation Firewall), который использует параллельный анализ одного и того же трафика всеми средствами защиты, разбор трафика для проверки антивирусом в памяти, анализ протоколов 7 уровня OSI, который позволяет анализировать работу конкретных приложений, а также облачный анализ угроз[1].

3.2.6. Сбор сведений с использованием ИКТ.

Будем использовать следующее определение:

Сбор сведений с использованием ИКТ (Information Gathering): сбор данных об объекте защиты из открытых и закрытых источников информации при помощи активных и пассивных методов сбора[2].

Прослушивание (захват) сетевого трафика (Traffic Hijacking) – Разновидность атаки «Человек посередине» (Man-In-The-Middle), когда атакующий способен просматривать пакеты участников сети и посылать свои собственные пакеты в сеть. Атака использует особенности установления соединения в протоколе TCP, и может осуществляться как во время «тройного рукопожатия», так и при установленном соединении.

Социальная инженерия (Social Engineering) – это метод манипулирования мыслями и поступками людей. Он базируется на психологических особенностях личности и закономерностях человеческого мышления. В социальной инженерии есть несколько техник, используемых для достижения поставленных задач. Все они основаны на ошибках, допускаемых человеком в поведении.

Например, *фишинг* применяется для сбора логинов и паролей пользователей путем рассылки писем и сообщений, побуждающих жертву сообщить интересующую злоумышленника информацию. *Претекстинг* состоит в выдаче себя за другого человека для получения жела-

[1] *Cisco Systems. What Is a Next-Generation Firewall?* Cisco Systems. 2021. https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html (дата обращения 04.03.2021).

[2] *SecurityLab. Глубины SIEM: корреляции «из коробки». Часть 3.1. Категоризация событий. SecurityLab by Positive Technologies*, 2018. https://www.securitylab.ru/blog/company/pt/345302.php (дата обращения 04.03.2021).

емых данных. Такая атака выполняется по телефону или почте. К ней предварительно готовятся, чтобы вызвать доверие пользователя.

Получить информацию о человеке можно через источники с открытым доступом, в основном — из социальных сетей. Одной из техник социальной инженерии является «*плечевой серфинг*», который применяется в транспорте, в кафе и других общественных местах, позволяющих через плечо жертвы наблюдать за компьютерными устройствами и телефонами.

Бывают ситуации, в которых пользователь сам предлагает мошеннику необходимую информацию, будучи уверенным в порядочности человека. В таком случае говорят об *обратной социальной инженерии*.

Шпионские программы предназначены для сбора данных и их отправки стороннему лицу без уведомления или согласия пользователя. Как правило, шпионские программы: (1) отслеживают, какие клавиши пользователь нажимает на клавиатуре; (2) собирают конфиденциальную информацию, такую как пароли, номера кредитных карт, номера PIN и т.д.; (3) собирают адреса электронной почты с компьютера пользователя; (4) запоминают наиболее посещаемые вами веб-страницы.

Клавиатурный шпион (кейлоггер) — это программа, которая записывает все нажатия клавиш на клавиатуре заражённого компьютера. Киберпреступники используют клавиатурные шпионы для кражи конфиденциальных данных, например имён пользователей, паролей, номеров и PIN-кодов кредитных карт, а также прочих сведений. Как правило, кейлоггеры входят в состав бэкдоров.

3.2.7. Нарушение безопасности информации.

Будем использовать следующее определение:

Нарушение безопасности информации (Information Content Security) – это целенаправленные попытки обхода механизма обеспечения безопасности для защиты от атак с внедрением контента, например, межсайтового скриптинга (XSS, cross site scripting). Для предотвращения подобных атак механизм обеспечения безопасности описывает безопасные источники загрузки ресурсов, устанавливает правила использования встроенных стилей, скриптов, а также динамической оценки JavaScript. Загрузка с ресурсов, не входящих в «белый список», блокируется.

Несанкционированное разглашение обрабатываемой информации (Unauthorised Access) напрямую относится к лицам, получающим доступ к данным, сетям, конечным точкам, приложениям или устройствам организации без разрешения. Это тесно связано с аутентификацией – процессом, который проверяет личность пользователя, когда он обращается к системе. Сломанные или неправильно настроенные механизмы аутентификации являются основной причиной доступа неавторизованных сторон.

Несанкционированное изменение обрабатываемой информации (Unauthorised Modification) – это любое несанкционированное изменение данных, хранящихся на компьютере, с целью нарушения доступа или нанесения ущерба надёжности, безопасности или работе любых данных, хранящихся на компьютере.

3.2.8. Распространение информации с неприемлемым содержимым.

Будем использовать следующие определения:

Распространение информации с неприемлемым содержимым (Abusive Content) – доставка легальным образом до конечного пользователя контента, побуждающего к противоправным действиям (умышленным или

неумышленным) или содержащего зловредные/мусорные данные[1].

Рассылка спам-сообщений (Spam) – это массовая рассылка корреспонденции рекламного характера лицам, не выражавшим желания её получить, а также рассылка массовых сообщений.

Публикация запрещённой законодательством информации (Prohibited Content) – предоставление доступа к контенту, который нарушает закон, продаёт нелегальные продукты или услуги, или имеет откровенно сексуальный характер.

3.2.9. Мошенничество с использованием ИКТ.

Будем использовать следующие определения:

Мошенничество с использованием ИКТ (Fraud – вид незаконного использования информационных технологий в различных областях бизнеса, от телекоммуникаций до банковского сектора, цель которого обычно состоит в том, чтобы присвоить денежные средства жертвы[2].

Фишинг — это особый вид компьютерных преступлений, который заключается в том, чтобы обманом заставить пользователя раскрыть ценную информацию, например личные данные, логины и пароли, сведения о банковском счёте или кредитных картах. Мошенники создают поддельные сайты, внешне неотличимые от настоящих, с похожими доменными именами, чтобы пользователь поверил в их подлинность и попытался пройти авторизацию со своим логином и паролем, после чего учётные данные окажутся у злоумышленников. Также фишинг может быть реализован в виде электронных писем и других подобных сообщений, в которых мошенники от имени компании (банка, социальной сети и т.п.) запрашивают у пользователя сведения для входа в аккаунт или его личные данные (номера кредитных карт, копии документов).

Кража личности — преступление, при котором один человек выдаёт себя за другого. Мошенники могут делать это, например, для того чтобы удалённо получить кредит на чужое имя.

Кардинг — это кража данных о пластиковых картах и их владельцах (адрес, ответы на секретные вопросы, дата рождения, имя) для последующей оплаты товара в интернет-магазинах или продажи этих данных на чёрном рынке. Для получения данных мошенники применяют фишинг, социальную инженерию, скимминг, специальные устройства, особые виды вредоносных программ. Также они могут получать сведения после взлома интернет-магазинов или банков.

Внутренний фрод – это внутренние хищения, совершаемые сотрудниками компании с использованием служебного положения и доступа к информационным системам.

3.2.10. Уязвимость.

Будем использовать следующие определения:

Уязвимость (Vulnerability): (1) присущие объекту информатизации причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации[3]; (2) ошибка в

[1] SecurityLab. *Глубины SIEM: корреляции «из коробки»*, Часть 3.1. Категоризация событий. SecurityLab by Positive Technologies, 2018. https://www.securitylab.ru/blog/company/pt/345302.php (дата обращения 04.03.2021).

[2] *Anti-Malware.ru. Мошенничество* (фрод). Anti-Malware.ru, 2021. https://www.anti-malware.ru/threats/fraud (дата обращения 04.03.2021).

[3] ВИХОРЕВ, С. *Классификация угроз информационной безопасности*, CNews, 2001. https://www.cnews.ru/reviews/free/oldcom/securit

программном, микропрограммном обеспечении, оборудовании или сервисном компоненте, возникшая в результате слабого места, которая может быть использована, оказывая негативное влияние на конфиденциальность, целостность или доступность затронутого компонента или компонентов[1].

Для обнаружения возможных проблем в системе безопасности, оценки ущерба и устранения уязвимости применяют *сканеры уязвимостей* – программные или аппаратные средства, служащие для осуществления диагностики и мониторинга сетевых компьютеров, позволяющее сканировать сети, компьютеры и приложения[2].

Полученные результаты оперативно размещаются в авторитетных базах данных общеизвестных уязвимостей информационной безопасности, например, в CVE (Common Vulnerabilities and Exposures). Каждой уязвимости присваивается идентификационный номер вида CVE-год-номер, описание и ряд общедоступных ссылок с описанием.

Другими примерами авторитетных баз уязвимостей информационной безопасности могут служить американская NVD (National Vulnerability Database), поддерживаемая Лабораторией информационных технологий при Национальном институте стандартов и технологий[3]. Также стоит отметить Банк данных угроз безопасности информации (БДУ) ФСТЭК России[4].

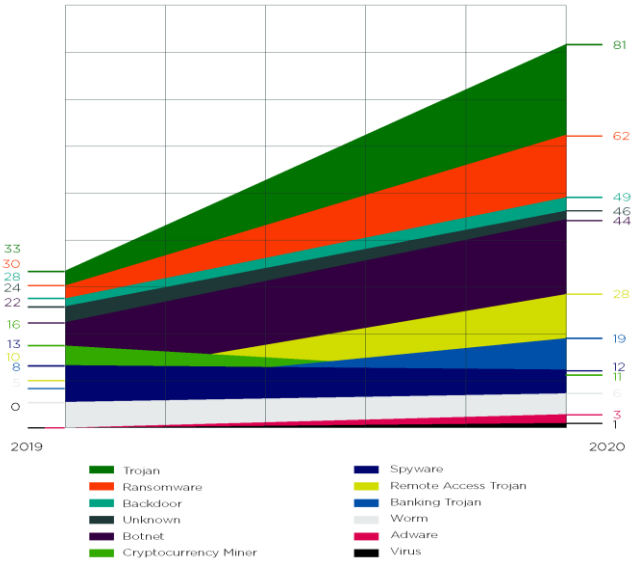

Рис. 6. *Динамика выявленных общеизвестных уязвимостей информационной безопасности (2019 – 2020 годы).*

Источник: Skybox Security. 2021 Vulnerability and Threat Trends Report. 2021. https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox-Security-vulnerability-and-threat-trends-report-2021.pdf (Просмотрен 04.03.2021).

За 2020 год в базе данных NVD фактически впервые появились 1628 новых уязвимостей. Динамика роста числа новых сообщений об уязвимостях (см. рис. 6) вызывает беспокойство у экспертов информационной безопасности: рост числа уязвимостей является верным признаком будущих атак. Высокие показатели уязвимости также усложняют процессы определения приоритетов и устранения недостатков[5].

y/elvis_class.shtml?print (дата обращения 04.03.2021).

1 *MITRE Corporation. Vulnerability. Terminology*. A glossary of terms used by the CVE Program, 2020. https://cve.mitre.org/about/terminology.html#cve_record (дата обращения 04.03.2021).

2 RAAM, G. *10 Best Vulnerability Scanning Tools for Penetration Testing*, 2020. В: GBHackers on Security, 2020. https://gbhackers.com/best-vulnerability-scanner/ (дата обращения 04.03.2021).

3 *Information Technology Laboratory. National Vulnerability Database. National Vulnerability Database*, 2021. https://nvd.nist.gov/ (дата обращения 04.03.2021).

4 *ФСТЭК России. Банк данных угроз безопасности информации*. ФСТЭК России, 2021. https://bdu.fstec.ru/threat (дата обращения 04.03.2021).

5 *Skybox Security. Vulnerability and Threat Trends Report, 2021*. https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox-Security-vulnerability-and-threat-trends-report-2021.pdf (дата обращения 04.03.2021).

Заключение

Каждый день сообщество специалистов по информационной безопасности решает непростую задачу по защите распределённых, разнородных и становящихся всё более сложными, систем и объектов критической инфраструктуры государства от злонамеренных действий участников теневой цифровой экономики.

Пандемия COVID-19 ускорила в большинстве стран внедрение облачных технологий, оптимизировала дистанционную работу, изменила домашний офис, резко повысила системные риски и обострила проблемы кибербезопасности.

В ближайшее время, с развитием и внедрением новых информационных технологий – квантовых вычислений, алгоритмов искусственного интеллекта и систем идентификации, с повышением сложности сетевых инфраструктур и взаимозависимости секторов, резко повысятся риски и угрозы, которые несёт в себе теневая цифровая экономика.

Для решения этой проблемы потребуется *моделирование системных рисков и угроз теневой цифровой экономики* в рамках единого подхода, учитывающее новейшие системные проблемы и риски, международные законы и стандарты и требующее согласованного взаимодействия на межгосударственном уровне.

Выводы

В заключении, считаем необходимым предложить разработку целостной стратегии противодействия теневой цифровой экономике. Основополагающими принципами этой стратегии должны являться:

– Совершенствование законодательной базы экономического регулирования, нацеленного на создание условий, при которых сокрытие определённых видов деятельности или их элементов, как и любая незаконная деятельность станут невыгодными.
– Развитие сотрудничества на государственном, региональном и международном уровнях с целью понижения уровня теневой цифровой экономики.

БИБЛИОГРАФИЯ

1. *Anti-Malware.ru. Мошенничество (фрод).* Anti-Malware.ru. 2021. https://www.anti-malware.ru/threats/fraud (дата обращения 04.03.2021).
2. *AT&T Cybersecurity*. Chapter Three. Security Incidents: Types of Attacks and Triage Options. In: AlienVault's Insider's Guide to Incident Response. 2021. p. 48. https://learn-cybersecurity.att.com/c/alien-vault-incident?x=5v9G6V&utm_internal=soc-irlookbook&xs=1248 (дата обращения 04.03.2021).
3. AV-TEST. Malware. *AV-TEST - The Independent IT-Security Institute*. 2021. https://www.av-test.org/en/statistics/malware/ (дата обращения 04.03.2021).
4. BORTA, G. *The Dark Side of Information Economics*. В: Economica, № XXIII (2 (92)2015, с. 97–102.
5. BREMMER, I., KUPCHAN, C. *Top Risks for 2021*. 2021. https://www.eurasiagroup.net/files/upload/top-risks-2021-full-report.pdf (дата обращения 04.03.2021).
6. *Check Point Software,* Cyber Security Report, 2021. https://pages.checkpoint.com/cyber-security-report-2021.html (дата обращения 04.03.2021).
7. CICHONSKI, P., MILLAR, T., GRANCE, T., SCARFONE, K. *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*. NIST Special Publication, 2012.
8. *Cisco Systems. What Is a Next-Generation Firewall?* Cisco Systems. 2021. https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html (дата обращения 04.03.2021).
9. DIXON, W., SAMARTSEV, D. *Three technologies that could define the next*

decade of cybersecurity. B: Annual Meeting of the New Champions 2019 (1-3 July 2019, Dalian, People's Republic of China). World Economic Forum, 2019.
10. *ENISA. Reference Incident Classification Taxonomy. Task Force Status and Way Forward. 2018.* https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy (дата обращения 04.03.2021).
11. FUENTES, M. *Trading in the Dark: An Investigation into the Current Condition of Underground Markets and Cybercriminal Forums*, 2020. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/trading-in-the-dark (дата обращения 04.03.2021).
12. *Information Technology Laboratory. National Vulnerability Database.* National Vulnerability Database, 2021. https://nvd.nist.gov/ (дата обращения 04.03.2021).
13. KROPOTOV, V., MCARDLE, R., YAROCHKIN, F. *Commodified Cybercrime Infrastructure: Exploring the Underground Services Market for Cybercriminals*, 2020. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/commodified-cybercrime-infrastructure-exploring-the-underground-services-market-for-cybercriminals (дата обращения 04.03.2021).
14. KROPOTOV, V., MCARDLE, R., YAROCHKIN, F. *The Hacker Infrastructure and Underground Hosting: Services Used by Criminals*, 2020. https://documents.trendmicro.com/assets/white_papers/wp-the-hacker-infrastructure-and-underground-hosting-services-used-by-criminals.pdf (дата обращения 04.03.2021).
15. *Microsoft. Understanding malware & other threats. Technical documentation*, 2021. https://docs.microsoft.com/ru-ru/windows/security/threat-protection/intelligence/understanding-malware (дата обращения 04.03.2021).
16. *MITRE Corporation. Vulnerability. Terminology. A glossary of terms used by the CVE Program. 2020.* https://cve.mitre.org/about/terminology.html#cve_record (дата обращения 04.03.2021).
17. MONNAPPA, K. 1.5 *Malware Command and Control (C2). Learning Malware Analysis*. 2018. https://www.oreilly.com/library/view/learning-malware-analysis/9781788392501/17a1735d-9583-4d86-9d1e-8b2735af5168.xhtml (дата обращения 04.03.2021).
18. *Project Management Institute. A guide to the project management body of knowledge (PMBOK® guide).* Project Management Journal. 2008.
19. RAAM, G. *Ten best vulnerability scanning tools for penetration testing*, 2020. GBHackers on Security, 2020. https://gbhackers.com/best-vulnerability-scanner/ (дата обращения 04.03.2021).
20. ROSE, K. A *Guide to the Project Management Body of Knowledge* (PMBOK® Guide)-Fifth Edition. Proj Manag J. 2013.
21. *SecureList. DDoS-атаки в IV квартале 2020 года.* SecureList by KASPERSKY, 2021. https://securelist.ru/ddos-attacks-in-q4-2020/100469/ (дата обращения 04.03.2021).
22. *SecurityLab. Глубины SIEM: корреляции «из коробки».* Часть 3.1. Категоризация событий. SecurityLab by Positive Technologies. 2018. https://www.securitylab.ru/blog/company/pt/345302.php (дата обращения 04.03.2021).
23. *Skybox Security, 2021 Vulnerability and Threat Trends Report*, 2021. https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox-Security-vulnerability-and-threat-trends-report-2021.pdf (дата обращения 04.03.2021).
24. Verizon, 2020. Data Breach Investigations Report, 2021. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf (дата обращения 04.03.2021).
25. Von der Leyen U., *Ursula von der Leyen's message to Davos Agenda: Full transcript. 2021.* 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 04.03.2021).
26. БОРТЭ, Г. Р. *Исторические предпосылки развития теневой информационной экономики*. Системи Обробки Інформації, № 4, 2012, с. 12–4.
27. БОРТЭ, Г. *Теневая информационная экономика*. Годишен Алманах «Научни Изследвания на Докторанта» Стопанска Академия «ДА Ценов», 2012, с. 5.
28. ВИХОРЕВ, С. Классификация угроз информационной безопасности, CNews, 2001. https://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml?print (дата обращения 04.03.2021).
29. КЛЕЙНЕР, Г. *Экосистема предприятия в свете системной экономической теории*. В: КЛЕЙНЕР, Г.Б. (ред.) *Стратегическое планирование и развитие предприятий: материалы* Девятнадцатого всероссийского симпозиума Москва, 10–11 апреля 2018 г., ЦЭМИ РАН, 2018, с. 88–97.
30. ЛУКАЦКИЙ, А. *Будущее российского рынка информационной безопасности*. *Век качества*, 2015, с. 8–9. https://cyberleninka.ru/article/n/buduschee-rossiyskogo-rynka-informatsionnoy-bezopasnosti (дата обращения 04.03.2021).
31. *НКЦКИ. Состав технических параметров компьютерного инцидента, указываемых при представлении информации в ГосСОПКА, и форматы представления информации о компьютерных инцидентах. Безопасность пользователей в сети Интернет*, 2019. https://safe-surf.ru/specialists/article/5252/638030/ (дата обращения 04.03.2021).
32. ОХРИМЕНКО, С., БОРТЭ, Г. *Новое наполнение науки секьюритологии*. В: KOZERA A, SADOWSKA, E. editors. Nauka i prak-tyka bezpieczeństwa : księga pamiątkowa Leszka Fryderyka Korzeniowskiego profesora Uniwersytetu Pedagog-icznego im Komisji Edukacji Narodowej w Krakowie. Krakow: Wydawnictwo EAS; 2019, с. 112–47.
33. ОХРИМЕНКО, С., БОРТЭ, Г., Тень цифровой экономики. Годишник на Стопанска Академия «ДА Ценов», 2018, с. 121.
34. ОХРИМЕНКО, С., ЧЕРНЕЙ, Г. *Угрозы безопасности автоматизированным информационным системам (программные злоупотребления).* НТИ, Серия 1. Организация и методика информационной работы, № 5, 1996, с. 5–13.
35. ФСТЭК России. *Банк данных угроз безопасности информации*, 2021. https://bdu.fstec.ru/threat (дата обращения 04.03.2021).
36. ХЕЛДМАН, К. *Профессиональное управление проектом*: пер. с англ. 7th ed. Москва: БИНОМ, Лаборатория знаний; 2016.

11.05.2021