Московский экономический журнал. № 4. 2022
Moscow economic journal. № 4. 2022
Научная статья
Original article
УДК 33
doi: 10.55186/2413046X_2022_7_4_247

РИСКИ КИБЕРАТАК НА ПРЕДПРИЯТИЯ, ВХОДЯЩИЕ В РЕАЛЬНЫЙ СЕКТОР ЭКОНОМИКИ СТРАН

THE RISKS OF CYBER ATTACKS ON ENTERPRISES BELONGING TO THE REAL SECTOR OF THE ECONOMY OF COUNTRIES

Бекишев Юрий Алексеевич, соискатель на кандидатскую степень, Санкт-Петербургский государственный университет, Санкт-Петербург, Россия, Langaron@yandex.ru

Куликов Денис Алексеевич, аспирант, Санкт-Петербургский государственный университет, Санкт-Петербург, Россия, denisk7873@gmail.com

Писаренко Жанна Викторовна, доктор экономических наук, профессор кафедры управления рисками и страхования, Санкт-Петербургский государственный университет, Санкт-Петербург, Россия, janna12000@yandex.ru

Bekishev Yuri Alekseevich, Candidate for a PhD, St. Petersburg State University, St. Petersburg, Russia, Langaron@yandex.ru

Kulikov Denis Alekseyevich, Postgraduate Student, Saint Petersburg State University, Saint Petersburg, Russia, denisk7873@gmail.com

Pisarenko Zhanna Viktorovna, Doctor of Economics, Professor of Risk Management and Insurance Department, Saint Petersburg State University, Saint Petersburg, Russia, janna12000@yandex.ru

Аннотация. За прошедшие двадцать лет в сфере кибербезопасности наблюдается необычайный рост финансовых и капитальных вложений. Только за последние четыре года инвестиции в сектор информационных технологий, занимающийся защитой данных и устройств, выросли практически в два раза. По данным аналитических агентств, основными инвесторами в этой области, в связи с высоким уровнем потребности в защите технологий автоматизации производства, интеллектуальной собственности, информационных ресурсов и пр., остаются компании, входящие в реальный сектор экономики. В настоящей работе рассмотрены основные уязвимости предприятий в разрезе цифровой безопасности, определены основные типы угроз и методы воздействия злоумышленников на организацию. В качестве аргументации проводятся примеры кейсов из истории новейшего времени. Надеемся, что данная статья поможет лучше понять виды нападений на предприятия со стороны так называемых «хакерских группировок» и реальные механизмы защиты.

Abstract. Over the past twenty years, there has been an extraordinary increase in financial and capital investments in the field of cybersecurity. Over the past four years alone, investments in the information technology sector dealing with data and device protection have almost doubled. According to analytical agencies, the main investors in this area, due to the high level of need for the protection of production automation technologies, intellectual property, information resources, etc., remain companies belonging to the real sector of the economy. In this paper, the main vulnerabilities of enterprises in the context of digital security are considered, the main types of threats and methods of influence of intruders on the organization are determined. As an argument, examples of cases from the history of modern times are given. We hope that this article will help to better understand the types of attacks on enterprises by so-called "hacker groups" and the real protection mechanisms.

Ключевые слова: кибербезопасность, кибератаки, цифровые угрозы, риски, экономика, IT

Keywords: cybersecurity, cyberattacks, digital threats, risks, economy, IT

Введение. Чем больше развиваются информационные технологии, тем больше появляется угроз, связанных с их эволюцией. Данную зависимость можно проследить, рассмотрев количество финансовых потерь мира, связанных с кибератаками, а также объем случаев утечки информации на одном из самых развитых экономических рынков, а именно Соединенных Штатов Америки (Рисунок 1):

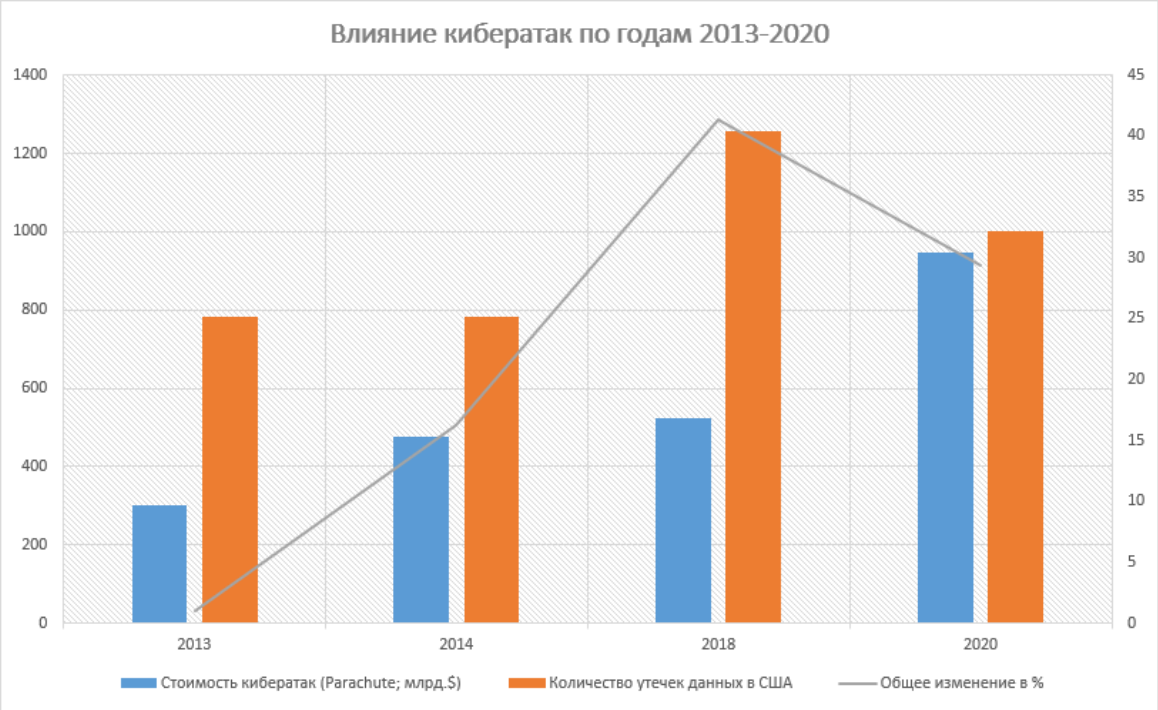

Рис.1 «Влияние кибератак на экономические рынки мира и США с 2013 по 2020 гг.»

Источник: IT агентство Parachute & Statista [19]

Отчет компании «Positive Technologies», являющейся ведущим мировым поставщиком решений в области корпоративной цифровой безопасности, показал, на какие сектора в настоящее время приходится больше всего атак (Рисунок 2):

Рис.2 «Категории жертв среди организаций»

Источник: Positive Technologies [17]

Из этого же отчета следует, что 49% из них приходится на реальный сектор экономики, что в целом не удивительно, так как в рыночно-хозяйственной системе именно они приносят больше всего ресурсов и инвестиций в развитие цифровой отрасли. Это обусловлено их постоянной потребностью в обновлении и расширении парка технологической инфраструктуры, без которой в мире неугасающей конкуренции они просто не смогут выжить. Только за 2020 год вследствие таких вливаний, а также при денежной поддержке со стороны финансового сектора (который если не делит с ними первое место, то является вторым по величине объема вложений), компании инвестировали в рынок кибербезопасности около 157 миллиардов долларов США, а по данным экспертов из «Тинькофф» банка, к 2026 году эта отметка может достигнуть величины в 352 миллиарда долларов США [6]. Ввиду такого стремительного роста сферы кибербезопасности, а также развития технологического мира с каждым временным периодом, будь то месяц или год, потребность в цифровой защите у организаций будет только увеличиваться. Отсюда цель данной работы – рассмотреть наиболее подверженные к кибератакам ресурсы на типичном предприятии реального сектора экономики.

Теоретико-методологическую основу исследования составляют книги, научные работы и статьи экспертов в области экономики и кибербезопасности. Основными источниками информации являются: Роберт Слейд и его работа под названием «Computer Viruses», опубликованная в «Encyclopedia of Information Systems»; научная команда Сваруп Бхуния, Майкл Сяо, Майнак Банга и Ситарам Нарасимхан с работой под названием «Hardware Trojan Attacks: Threat Analysis and Countermeasures», опубликованной в сборнике Proceedings of the IEEE; Эрик Филиол и его работа «Computer viruses: from theory to applications»; а также Николай Безруков и его труд под названием «Классификация компьютерных вирусов MS-DOS и методы защиты от них».

Эмпирическую основу исследования составляют данные аналитических и технических агентств, таких, как Positive Technologies, Parachute, Statista, PWC, BI.ZONE, СБЕРБАНК, Kaspersky и PandaLabs, а также данные следующих СМИ: Tadviser, Россельхознадзор новости, Рамблер, EXPRESS NEWS и Anti-malware.

Основные сектора предприятия, которые могут быть подвержены кибератакам

В настоящее время на различных производствах существует множество систем, которые могут быть подвержены разного рода взломам, начиная с сайта организации и заканчивая автоматическим производственным оборудованием. Для наглядности нами была составлена небольшая карта основных механизмов, которые присутствуют на множестве предприятий производственного комплекса (Рисунок 3):

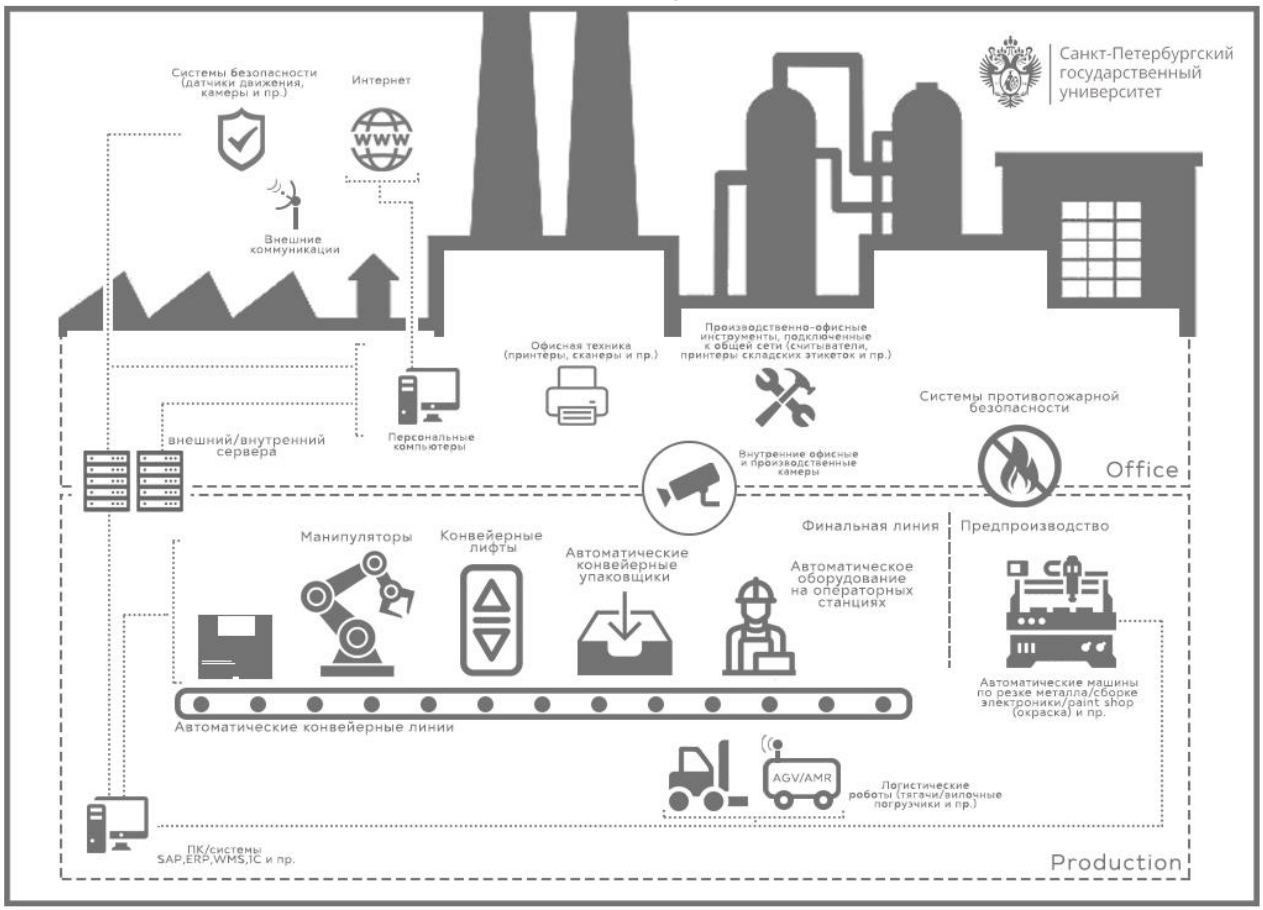

Рис.3 «Карта цифровых технологий на предприятии»

Источник: составлено авторами работы

Конечно, это далеко не полный список средств цифровизации и автоматизации фабрики, однако, это те виды технологий, которые уже не являются чем-то новым в рабочей среде. Кроме того, перечисленные инструменты присутствуют практически во всех видах компаний реального сектора.

Так как каждый вид специального оборудования имеет своё назначение и структуру, подход и цели мошенничества по отношению к ним различаются. Ниже выделены две основные группы технологий, наиболее подверженные нападениям со стороны хакеров, а также определены способы и методы кибератак, которые могут быть использованы.

Интернет-ресурсы предприятия (почта, интернет-сайт, внутренняя среда)

Самыми легкими и наиболее склонными к киберугрозам являются те технологии, которые напрямую размещены в глобальной сети «Интернет». К ним относятся сайты компании, цифровая среда организации (библиотеки, магазины, инфраструктура отделов и пр., привязанные к системе интернета) корпоративная почта сотрудников, а также мобильные приложения. Именно они наиболее уязвимы для:

1) Фишинга – атака типа «социальная инженерия», чаще всего направленная не на взлом каких-либо систем компании, а на самих сотрудников. Данное направление основывается на незнании простейших правил сетевой безопасности пользователей. Хотя видов фишинговых атак на данный момент существует целое множество, общий механизм остается без существенных изменений. Происходит это следующим образом: пользователю на определенный ресурс компании (почта, приложение, аккаунт сайта, СМС на корпоративный номер) приходит письмо с содержанием, направленным на определенное действие. Цель этого действия может быть разной: ввод собственного пароля, отправка средств или личных документов и т.д. Различается также и метод принуждения к выполнению этого действия – это может быть как прямая угроза, шантаж, так и простейший обман через подставные сайты, обещания дохода или запроса документов от соответствующих ведомств. Примеров фишинговых атак на данный момент существует множество: атака на пользователей компании Malwaretising, реализованная хакерской группировкой eGobbler [3], где, путем показа всплывающей рекламы, пользователей переводили на сайт, собирающий личные данные; фишинговая компания 2019 года, распространяющая PDF документы с VBS-скриптом, направленная на кражу личных данных пользователей, которая затронула сотрудников более 200 компаний [3].

2) Троянов – программ, предназначенных для определенного воздействия на операционную систему компьютера с разными целями: сбор/разрушение информации на накопителе, нарушение работы операционной системы

компьютера, использование его мощностей в своих целях и т.д. [12]. Видов троянских программ на данный момент существует множество:

a. Клавиатурные шпионы (или Trojan-SPY): программа копирует все команды, которые были отправлены с клавиатуры (или аналогичного устройства ввода), затем передавая её злоумышленнику. Часто используется для сбора паролей.

b. Анонимные smtp-сервера и прокси (или Trojan-Proxy): программы, которые используются либо как отдельные сервера, либо как прокси. Часто используются для спам-рассылок.

c. Похитители паролей (или Trojan-PSW): в отличии от Trojan-SPY, данная утилита забирает данные по паролям из мест их хранения (файловой системы, архивов).

d. Инсталляторы прочих вредоносных программ (Trojan-Dropper): трояны, которые, внедрившись в компьютерную систему, дают возможность отправителю устанавливать определенные вредоносные программы.

e. Модификаторы настроек браузера (или Trojan-Cliker): программа, которая меняет стартовую страницу браузера пользователя для несанкционированного обращения последнего к нему.

f. Архивные бомбы (ARCBomb): троян, оформленный в виде архива, который при распаковке полностью заполняет пространство хранилища на компьютере, вызывая замедление работы операционной системы, вплоть до разрушения файловой системы на ПК [14].

Особенно яркий пример использования троянского вируса можно наблюдать при атаке на компании из агропромышленного холдинга «Мираторг», где при помощи трояна Win32:Bitlocker/l!rsm были атакованы информационные ресурсы компании, нарушив деятельность некоторых её предприятий [7].

3) Технического флуда – атака при помощи большого количества запросов или действий: обращений к сайту/приложению, отправкой форм, комментариев, сообщений в чатах и пр. на ресурсы предприятия, приводящая

к остановке его работы. Самая известная форма такого инструмента – DoS и DDoS-атаки, где при помощи множества зараженных вирусами (к примеру, троянами) устройств (ботнет (Botnet) сети) производится атака на различные ресурсы организаций. Самым ярким примером такой атаки служит компания Google, которую атаковали в 2017 году с мощностью запросов 2.54 Тбит/с [11]. На данный момент это самое крупное DDoS нападение в истории.

Стоит отметить, что, во-первых, после заражения или получения доступа к информационному ресурсу/приложению/почте, злоумышленник часто оставляет за собой вирусную программу типа «Backdoor», которая в будущем позволяет ему заново получить доступ к системе без ввода пароля. Во-вторых, необходимо упомянуть, что часто вместе с вирусными программами используют Руткит (Rootkit) - набор программ, которые используют технологии сокрытия системных объектов (файлов, процессов, драйверов, сервисов, ключей реестра, открытых портов, соединений и пр.) посредством обхода механизмов системы. В-третьих, все перечисленные методы атак зачастую используются в связке, разрабатываются целые хакерские компании, в котором используются как методы, описанные в этой части работы, так и те, о которых будет написано далее.

Сервера компаний, хранилища информации, системы SAP,1C, WMS, ERP и др.

Одними из самых опасных для предприятия являются атаки на их внутренние сервера, имеющие доступ как к хранилищу данных организации, так и к её технологическому функционалу. В отличии от предыдущей группы, здесь все осложняется масштабом и возможным ущербом, а также тем, что, в отличии от ресурсов сети интернет (где зачастую нападение осуществляется на арендованные под них сервера, не принадлежащие компании), здесь уже участвуют имущество и внутренняя структура самой организации.

Для получения доступа к компьютерам/серверам/специальным производственным программам также, как и к информационным ресурсам,

используют трояны или сетевые черви (различаются они между собой способом распространения, а также стелс-режимом и полиморфизмом, присущем сетевому червю), а для их распространения применяют инструменты фишинга, о которых говорилось ранее. Далее, уже после получения доступа к устройству, в ход идут несколько популярных на данный момент сценариев:

1) Использование вирусов-вымогателей (шифровальщиков; ransomware): в данном случае все жизненно важные (и не только) файлы наиболее распространённых форматов на сервере/компьютере шифруются, тем самым становясь недоступными для пользователей. После этого злоумышленники, как правило, просят выкуп, угрожая полным их удалением. Если требование не выполняется, то, кроме реализации прямой угрозы, как правило, в вирус закладывают команду к изменению главной загрузочной записи, выводя систему из строя. Для компании это страшно не только финансовыми потерями, но и остановкой рабочей деятельности, часто на довольно продолжительное время. Так как по аналитическим данным многих уважаемых изданий [8] на сегодняшний день это самый частый исход событий при кибератаках на предприятие, то и примеров таких сценариев множество: атака на компанию ASCO Industries (являющийся одним из крупнейших в мире поставщиков запчастей для авиационной техники) в марте 2019 года, в результате которой было остановлено производство на заводах сразу в четырёх странах из-за вируса-вымогателя, появившегося на производственной площадке в Завентеме [10]; атака при помощи вируса-вымогателя на аэропорт Бристоля в середине сентября 2018 года, из-за которой на два дня отключились все информационные табло аэровокзала [16]; хакерская атака на южнокорейскую компанию «Nayana» в июне 2017 года, в результате чего были зашифрованы и недоступны более трех тысяч клиентских веб-сайтов [18].

2) Промышленный шпионаж, а также кража интеллектуальной собственности: в данном сценарии при помощи уже внедренных

вышеупомянутых программ похищается интеллектуальная собственность компании (чертежи, технологии, методы производства и пр.). Одним из примеров такой кражи является инцидент с нападением на компанию Volvo Cars в декабре 2021 года, где, по признанию самой компании, хакерам удалось похитить исследования и разработки организации [4].

3) Снижение качества выпускаемой продукции или техническая остановка предприятия: в данном случае целью злоумышленников является инфраструктура предприятия, а именно системообразующие программы (типа SAP, 1C, WMS, ERP и др.), роботизированные системы (AGV/AMR, манипуляторы, краны), действующие как на самостоятельных площадках, так и в системах SAP/WMS, автоматические конвейера, а также системы безопасности. Первая кибератака подобного рода произошла еще до появления глобальной системы «Интернет» в 1982 году при помощи внедрения трояна в SCADA-систему, контролирующую сибирский нефтепровод, что привело к мощному взрыву; также интересен инцидент в Maroochy Water System, в котором бывший сотрудник взломал системы управления водоснабжением, в результате чего миллионы литров сточных вод попали в ближайшую реку, что послужило затоплению местной гостиницы [9]; на форуме «Positive Hack Days» в 2018 году провели кибербитву «The Standoff», где команды атакующих, защитников и «Security Operations Centers» боролись за контроль над масштабной эмуляцией автоматизированной городской инфраструктуры [5].

Используя весь этот инструментарий, а также прорехи в системах безопасности объекта нападения, злоумышленники на сегодняшний день могут наводить хаос среди организаций, обогащаться, а также выполнять свои или чужие цели разного рода. Таким образом, с каждым новым месяцем/кварталом/годом перед организациями стоит необходимость в увеличении инвестиций для защиты своих активов и выстраивания стратегии сетевой обороны. Однако в данной закономерности есть и плюсы: во-первых, такая борьба дает толчок развитию отрасли программирования, во-вторых,

эта борьба, ввиду инвестиций в данный сектор, формирует целый рынок компаний, предлагающих свои методы сетевой защиты, что означает как рост специалистов в данной области, так и появление для них новых рабочих мест.

Заключение. Как говорилось ранее, с развитием цифровых технологий будет расти и количество преступлений, связанных с ними. Каждой компании в настоящем и будущем следует обращать на это внимание и позаботиться как об информировании своих сотрудников о базовых мерах безопасности в интернете, так и об достаточно хорошей сетевой защите своих информационных и интеллектуальных ресурсов.

Сегодня мы уже можем наблюдать стандартные меры по построению такой защиты. Многие организации проводят тренинги среди своих сотрудников, нанимают агентов по цифровой безопасности, подключают свое высокотехнологическое оборудование к закрытой сети и пр. Все это позволяет им минимизировать риски атак со стороны злоумышленников. Однако следует помнить, что никакая защита не дает 100% гарантии и только бдительность и осторожность каждого сотрудника организации, будь то IT специалист, оператор станции или директор, поможет избежать опасной ситуации, а также, по возможности, предотвратить последствия хакерской атаки.

Список источников

1. Безруков Н. "Классификация компьютерных вирусов MS-DOS и методы защиты от них" // Вычислительные машины электронные персональные - Обеспечение сохранности данных. - Б-ка "МИР ПК", 2010
2. Атака на Мираторг, АПХ // TADVISER URL: https://www.tadviser.ru/index.php/Компания:Мираторг,_АПХ#.2A2022:_.D0.A5.D0.B0.D0.BA.D0.B5.D1.80.D1.81.D0.BA.D0.B0.D1.8F_.D0.B0.D1.82.D0.B0.D0.BA.D0.B0 (дата обращения: 03.04.2022).
3. Анализ «громких» инцидентов в сфере информационной безопасности в 2019 году // TADVISER URL:

https://www.tadviser.ru/index.php/Статья:Анализ_громких_инцидентов_в_сфере_информационной_безопасности_в_2019_году#.D0.A4.D0.B8.D1.88.D0.B8.D0.BD.D0.B3 (дата обращения: 03.04.2022)

4. Группа Snatch взломала Volvo Cars и украла внутренние документы компании // Anti-malware URL: https://www.anti-malware.ru/news/2021-12-13-111332/37723 (дата обращения: 04.04.2022).

5. Ежегодный форум "Positive Hack Days" // Positive Hack Days URL: https://www.phdays.com/ru/ (дата обращения: 04.04.2022).

6. Инвестиции в кибербезопасность: 6 крупнейших компаний // Тинькофф журнал URL: https://journal.tinkoff.ru/short/cybersecurity-stocks/ (дата обращения: 05.04.2022).

7. Относительно оформления электронных ветеринарных сертификатов компаниями из холдинга «Мираторг» после хакерской атаки на их информационные ресурсы // Россельхознадзор URL: https://fsvps.gov.ru/fsvps/news/48103.html (дата обращения: 03.04.2022)

8. Отчет PWC: "Цифровое сообщество готовится отражать кибератаки" // PWC. – 2018 & Threat Zone 2020: Аналитическое исследование основных трендов кибератак от BI.ZONE // BI.ZONE & СБЕРБАНК. – 2020

9. Отчет PandaLabs: "Критическая инфраструктура" // PandaLabs URL: https://www.cloudav.ru/upload/iblock/447/PAD_PAD360%20-%20Whitepaper%20-%20Критические%20инфраструктуры.pdf (дата обращения: 04.04.2022).

10. Программа-вымогатель приостановила производство на четырех заводах ASCO Industries // Kaspersky ICS CERT URL: https://ics-cert.kaspersky.ru/publications/news/2019/06/14/asco-ransomware/ (дата обращения: 04.04.2022).

11. Google: В 2017 году мы отразили самую мощную DDoS-атаку (2.54 Tbps) Об этом сообщает "Рамблер" // Рамблер URL: https://news.rambler.ru/internet/45042637-google-v-2017-godu-my-otrazili-samuyu-moschnuyu-ddos-ataku-2-54-tbps/ (дата обращения: 03.04.2022).

12. Swarup B., Mainak B., Michael H., Seetharam N. Hardware Trojan Attacks: Threat Analysis and Countermeasures // Proceedings of the IEEE. - 2014. - №8. - С. 1229-1247.
13. Filiol E. "Computer viruses: from theory to applications" // France: Springer-Verlag France, 2005. - С. 405 с.
14. Robert M.Slade Computer Viruses // Encyclopedia of Information Systems. - 2003. - №California State University, Academic Press. - С. 255-265.
15. Annual number of data breaches and exposed records in the United States from 2005 to 2020 // statista.com URL: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (дата обращения: 01.04.2022).
16. Bristol Airport CYBER ATTACK: Flight information screens go BLANK in shock hacking // EXPRESS NEWS URL: https://translated.turbopages.org/proxy_u/en-ru.ru.a01e4958-624b2d68-30797bc6-74722d776562/https/www.express.co.uk/news/uk/1018377/bristol-airport-flights-information-hacking-cyber-attack (дата обращения: 04.04.2022).
17. Cybersecurity threatscape // "Positive Technologies" company URL: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2020-q1/ (дата обращения: 01.04.2022).
18. Ransomware attack costs South Korean company $1M, largest payment ever // FoxNews URL: https://translated.turbopages.org/proxy_u/en-ru.ru.b9c9453d-624b2e6b-be1bef52-74722d776562/https/www.foxnews.com/tech/ransomware-attack-costs-south-korean-company-1m-largest-payment-ever (дата обращения: 04.04.2022).
19. 2022 Cyber Attack Statistics, Data, and Trends // Global IT agency "Parachute" URL: https://parachute.cloud/2022-cyber-attack-statistics-data-and-trends/ (дата обращения: 01.04.2022)

References

1. Bezrukov N. "Classification of MS-DOS computer viruses and methods of protection against them" // Personal electronic computing machines - Ensuring data security. - B-ka "PC WORLD", 2010
2. Attack on Miratorg, APX // TADVISER URL: https://www.tadviser.ru/index.php/Компания:Miratorg,_APH#.2A2022:_.D0.A5.D0.B0.D0.BA.D0.B5.D1.80.D1.81.D0.BA.D0.B0.D1.8F_.D0.B0.D1.82.D0.B0.D0.BA.D0.B0 (date of application: 03.04.2022).
3. Analysis of "high-profile" incidents in the field of information security in 2019 // TADVISER URL: https://www.tadviser.ru/index.php/Статья:Analysis of rare incidents in the Information Security Sphere In2019_year#.D0.A4.D0.B8.D1.88.D0.B8.D0.BD.D0.B3 (accessed 03.04.2022)
4. The Snatch group hacked Volvo Cars and stole the company's internal documents // Anti-malware URL: https://www.anti-malware.ru/news/2021-12-13-111332/37723 (accessed: 04.04.2022).
5. Annual Forum "Positive Hack Days" // Positive Hack Days URL: https://www.phdays.com/ru / (accessed 04.04.2022).
6. Investments in cybersecurity: 6 largest companies // Tinkoff Magazine URL: https://journal.tinkoff.ru/short/cybersecurity-stocks / (date of application: 05.04.2022).
7. Regarding the registration of electronic veterinary certificates by companies from Miratorg Holding after a hacker attack on their information resources // Rosselkhoznadzor URL: https://fsvps.gov.ru/fsvps/news/48103.html (accessed: 04/03/2022)
8. PWC Report: "The digital community is preparing to repel cyber attacks" // PWC. – 2018 & Threat Zone 2020: Analytical study of the main trends of cyber attacks from BI.ZONE // BI.ZONE & SBERBANK. – 2020
9. PandaLabs Report: "Critical Infrastructure" // PandaLabs URL: https://www.cloudav.ru/upload/iblock/447/PAD_PAD360%20-%20Whitepaper%20-%20Критические%20инфраструктуры.pdf (accessed: 04.04.2022).

10. The ransomware program suspended production at four ASCO Industries plants // Kaspersky ICS CERT URL: https://ics-cert .kaspersky.ru/publications/news/2019/06/14/asco-ransomware / (accessed 04.04.2022).
11. Google: In 2017, we repelled the most powerful DDoS attack (2.54 Tbps) This is reported by Rambler // Rambler URL: https://news.rambler.ru/internet/45042637-google-v-2017-godu-my-otrazili-samuyu-moschnuyu-ddos-ataku-2-54-tbps / (accessed 03.04.2022).
12. Swarup B., Mainak B., Michael H., Seetharam N. Hardware Trojan Attacks: Threat Analysis and Countermeasures // Proceedings of the IEEE. - 2014. - No.8. - pp. 1229-1247.
13. Filiol E. "Computer viruses: from theory to applications" // France: Springer-Verlag France, 2005. - p. 405 p.
14. Robert M.Slade Computer Viruses // Encyclopedia of Information Systems. - 2003. - No. California State University, Academic Press. - pp. 255-265.
15. Annual number of data breaches and exposed records in the United States from 2005 to 2020 // statista.com URL: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed / (accessed: 01.04.2022).
16. Bristol Airport CYBER ATTACK: Flight information screens go BLANK in shock hacking // EXPRESS NEWS URL: https://translated.turbopages.org/proxy_u/en-ru.ru.a01e4958-624b2d68-30797bc6-74722d776562/https/www.express.co.uk/news/uk/1018377/bristol-airport-flights-information-hacking-cyber-attack (accessed: 04.04.2022).
17. Cybersecurity threatscape // "Positive Technologies" company URL: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2020-q1 / (accessed: 01.04.2022).
18. Ransomware attack costs South Korean company $1M, largest payment ever // FoxNews URL: https://translated.turbopages.org/proxy_u/en-ru.ru.b9c9453d-624b2e6b-be1bef52-74722d776562/https/www.foxnews.com/tech/ransomware-

attack-costs-south-korean-company-1m-largest-payment-ever (accessed: 04.04.2022).

19. 2022 Cyber Attack Statistics, Data, and Trends // Global IT agency "Parachute" URL: https://parachute.cloud/2022-cyber-attack-statistics-data-and-trends / (accessed: 01.04.2022)

Для цитирования: Бекишев Ю.А., Куликов Д.А., Писаренко Ж.В. Риски кибератак на предприятия, входящие в реальный сектор экономики стран // Московский экономический журнал. 2022. № 4. URL: https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-4-2022-49/