УДК 004.056 **DOI: 10.18413/2518-1092-2022-8-2-0-2**

Кузьминых Е.С.
Маслова М.А.

АНАЛИЗ РОСТА КИБЕРАТАК И РЫНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ

Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия

e-mail: egor2014ru@mail.ru, mashechka-81@mail.ru

Аннотация
Сфера IT прогрессирует без остановки, из-за чего сотрудникам информационной безопасности приходится регулярно прогрессировать вместе со всеми обновлениями программного обеспечения для максимальной результативности обеспечения безопасности компании, в которой они работают. Для этого компаниям необходимо нанимать квалифицированного сотрудника информационной безопасности, который будет обучать персонал «правильно» обращаться с компьютером, будет регулярно обновлять программное обеспечение, устанавливать новое и сможет в режиме реального времени противостоять атакам злоумышленников. В 2022 году на российский сегмент обрушились нападения зарубежных хакеров, что привело к большим проблемам для всех отраслей страны. Компаниям и государственным структурам пришлось противостоять постоянным атакам. В настоящее время происходит переход на отечественное ПО, что облегчает ситуацию. Также в 2022-2023 годах было выделено большое количество средств на разработку нового ПО и борьбу со злоумышленниками. В данной статье были рассмотрены некоторые виды атак на компании, самая актуальная, 0-day, какая информация больше интересует злоумышленников, какие отрасли подверглись атакам и каким образом. Как все эти изменения повиляли на российский рынок ИБ и прогнозы на будущее.
Ключевые слова: кибератаки; атаки; хакеры; злоумышленники; атака нулевого дня; 0-day; отечественное ПО; рынок; информационная безопасность; ИБ; антивирусы; безопасность; российские сегменты; бюджет; бюджет ИБ; импортозамещение
Для цитирования: Кузьминых Е.С., Маслова М.А. Анализ роста кибератак и рынка информационной безопасности РФ // Научный результат. Информационные технологии. – Т.8, №2, 2023. – С. 11-18. DOI: 10.18413/2518-1092-2022-8-2-0-2

Kuzminykh E.S.
Maslova M.A.

ANALYSIS OF THE GROWTH OF CYBERATTACKS OF THE INFORMATION SECURITY MARKET OF THE RUSSIAN FEDERATION

Sevastopol state University, 33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: egor2014ru@mail.ru, mashechka-81@mail.ru

Abstract
The IT sphere is progressing without stopping, which is why information security employees have to regularly progress along with all software updates to maximize the effectiveness of ensuring the security of the company in which they work. To do this, companies need to hire a qualified information security officer who will train staff to "properly" use a computer, will regularly update software, install new ones and will be able to withstand attacks by intruders in real time. In 2022, the Russian segment was attacked by foreign hackers, which led to big problems for all sectors of the country. Companies and even government agencies had to resist constant attacks. Currently, there is a transition to domestic software, which makes the situation easier. Also, in 2022-2023, a large amount of funds was allocated for the development of new software and the fight against intruders. In this article, some types of attacks on companies were considered, the most relevant, 0-day, which information is more interested in attackers, which

industries were attacked and how. How all these changes affected the Russian information security market and forecasts for the future.
Keywords: cyber-attacks; attacks; hackers; intruders; zero-day attack; 0-day; domestic software; market; information security; IB; antiviruses; security; Russian segments; budget; IB budget; import substitution
For citation: Kuzminykh E.S., Maslova M.A. Analysis of the growth of cyberattacks of the information security market of the Russian Federation. – Т.8, №2, 2023. – P. 11-18. DOI: 10.18413/2518-1092-2022-8-2-0-2

ВВЕДЕНИЕ

В век развития информационных технологий сфера IT развивается достаточно быстро, появляются новые технологии, программное обеспечение и постоянное обновление ранее созданного, что приводит к появлению новых проблем и ошибок в работе той, или иной системы. На фоне этого актуален вопрос, как же защищать все эти технологии, чтобы хоть немного обезопасить себя, или компанию от злоумышленников. Данный вопрос решает сфера Информационной безопасности, сотрудники которой регулярно развивают себя, следят за новинками, обновлениями и создающимися новыми угрозами со стороны злоумышленников.

В последние годы идёт развитие отечественного программного обеспечения, заменяют иностранное ПО на российское и поддерживают любых разработчиков в грамотных идеях по разработке. Благодаря чему появляется всё больше самостоятельных и новых компаний, которые развивают новое ПО. Сотрудники IT получают множество бонусов от правительства и чувствуют себя как «рыба в воде», благодаря чему рынок информационной безопасности начал расти с каждым годом.

ОСНОВНАЯ ЧАСТЬ

Существует множество проблем информационной безопасности, как и различное ПО для атак на компании. В основном злоумышленники пользуются уязвимостью нулевого дня. 0-day — обозначает, что существуют уязвимости, для которых не нашли способа устранения, или вредоносное ПО, против которых не разработали защитные методы. Сложно предсказать, где именно в коде будет ошибка, из-за которой злоумышленник сможет проникнуть в систему. В настоящее время многие создатели вирусов фокусируются именно на неизвестных уязвимостях, т.к. компания может быть не готова к такой атаке и даже не знать про проблему, через которую проберётся злоумышленник [1, 2].

Для нахождения уязвимостей создатели вирусов используют различные методы, например:

- реверс-инжиниринг и поиск ошибок в алгоритме работы ПО;
- дизассемблирование кода и поиск ошибок в самом коде ПО;
- фаззинг-тестирование — тестирование программного обеспечения, суть заключается в обработке программой большого количества информации, которая изначально содержит неверные параметры [3].

Классические антивирусы не способны обнаружить такую атаку, поэтому их защита для компаний незначительна. Для эффективной защиты от атак 0-day используют проактивные технологии защиты. Они эффективно обеспечивают защиту от новых, известных, атак и вирусов. Но всё равно абсолютную защиту данный метод предоставить не может, т.к. нельзя защититься от всего, тем более от новой атаки.

Проактивная защита — это комплекс организационных и технических мер, которые позволяют расширить понятие защищённости и повысить реакцию web-приложений на новые угрозы и нападения [4].

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

Не стоит забывать про обычные вирусы и атаки, которые постоянно мешают компаниям нормально функционировать. В 2022 году на российские компании было совершено в два раза больше атак, чем в прошлом году, примерно 900 тысяч хакерских атак. Атаки от обычных активистов, которые не преследуют коммерческие цели, значительно снизились, а именно DDoS-атаки на web-ресурсы. 2022 год был очень опасен для компаний, никогда не было таких активных и хаотичных атак на разные ресурсы Российской Федерации, которые к концу года перешли в более целенаправленные и конкретные атаки. Значительно выросли сетевые атаки. Сканирование сети происходит автоматизированными инструментами, для компрометации учётных записей пользователей и разведки сети компаний. Хоть и таких инцидентов мало, но это означает, что такая информация более интересна для злоумышленников.

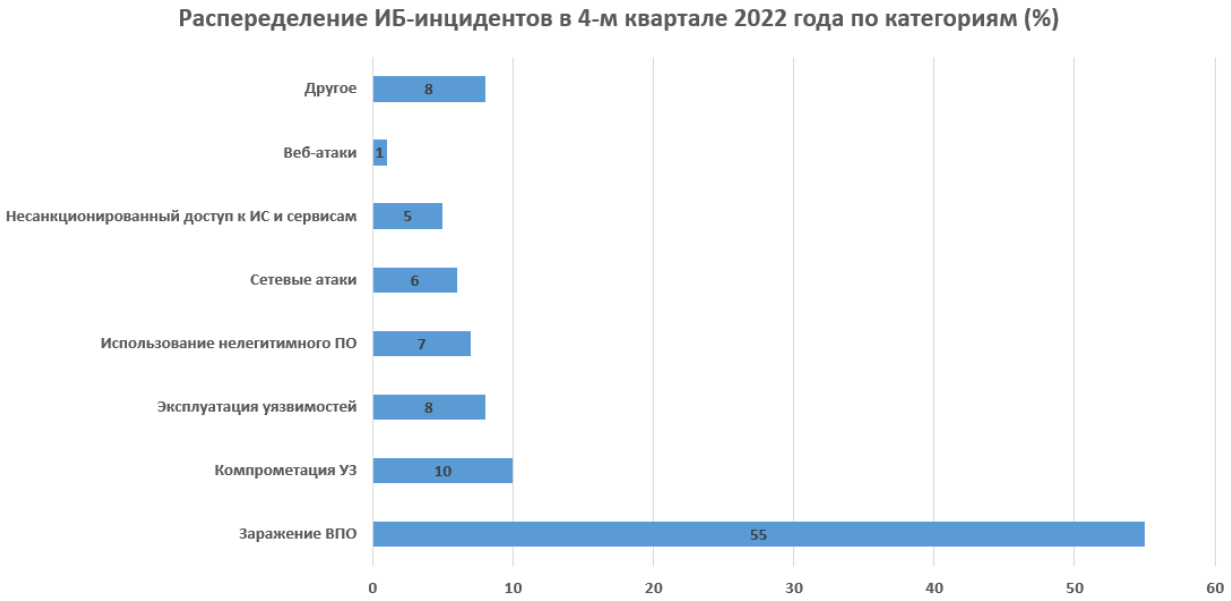

Рис. 1. Категории атак на российские компании [5]
Fig. 1. Categories of attacks on Russian companies [5]

В 62% случаев хакеры использовали вредоносное ПО, в основном шифровальщики, направленные на кражу конфиденциальных данных и получение выкупа. Но всё же, больший процент атак совершён на частные лица, ведь у не грамотного пользователя легче украсть данные, чем у целой компании.

В 2022 году увеличились атаки на российские сегменты и все ключевые отрасли экономики. Можно выделить следующие позиции:

– государственный сектор — был целью №1, было зафиксировано 403 атаки, что на 25% больше, чем в прошлом году. Государственный сектор был лакомым кусочком для преступных организаций, желающих похитить секретную информацию и навредить стране;

– промышленность — злоумышленники хотели остановить работу отраслевой промышленности, или замедлить выпуск продукции. Было зафиксировано 223 атаки, что на 7% больше в отличии от прошлого года. В основном использовались методы социальной инженерии, в некоторых случаях компрометация программного обеспечения в компаниях;

– медицина — уже несколько лет занимает 3-е место по атакуемым отраслям, занимает лидирующую позицию по утечке данных. Более чем в 80% случаев происходит утечка конфиденциальных данных клиентов. В системах медучреждений содержатся колоссальный объем данных, преступники могут получить такие конфиденциальные данные как: историю

болезни, ФИО, информацию о состоянии здоровья, номер телефона, реквизиты счетов, номеров карт, адрес прописки, или электронной почты, дату рождения и любую другую медицинскую информацию.

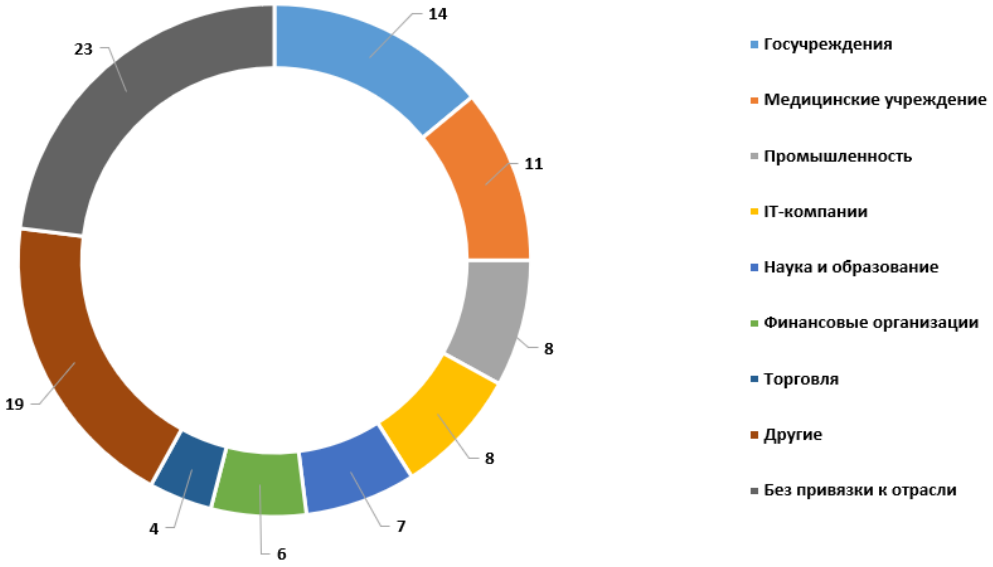

Рис. 2. Категории жертв среди организаций
Fig. 2. Categories of victims among organizations

– финансовый сектор — по сравнению с прошлым годом атаки на данный сектор снизились на 7%. Компании более подготовлены к атакам, но это не гарантирует хорошей защищённости. Positive Technologies провели исследование, в ходе которого в 86% случаев получили доступ к локальной сети. Помимо этого, было выяснено, что в режиме реального времени можно проникнуть глубже в сеть даже не опытному злоумышленнику. В ходе проверки все эксперты смогли получить полный доступ к инфраструктуре компании и показали, что будет, если злоумышленник попадёт в сеть [6 - 8];

– IT-компании — процент атак снизился, однако 6% атак принадлежат данному сектору. IT-компании более готовы к атакам и в большинстве таких компаниях есть квалифицированный сотрудник информационной безопасности, который обеспечивает защиту сети и способен потягаться со злоумышленником в режиме реального времени. Как и во всех компаниях, в большинстве случаев используется метод социальной инженерии, ведь так гораздо легче проникнуть в сеть компании, приложив минимум усилий;

– наука и образование — количество атак в отличии от 2021 года не изменилось, злоумышленников всё так же интересует конфиденциальная информация, преимущественно персональные данные клиентов и сотрудников. Каждая вторая атака была совершена шифровальщиками, целью данной атаки было получение выкупа от организации за украденную информацию. Также подбирали пароли от учётных записей и пользовались скомпрометированными данными;

– пользователи — количество атак на обычных пользователей выросло на 44%, что привело к масштабным утечкам данных. 17% от общего числа атак пришлось на пользователей. Способы атак такие же, как и в прошлых отраслях.

Из-за роста атак бюджет информационной безопасности увеличили у государственных структур на 26%, средства пошли на продление лицензий, закупку нового железа и ПО. Объём рынка информационной безопасности в 2021 году достиг 98,6 млрд. рублей, что означает рост на 8%, в 2022 году вырос на 10-20% [10]. В начале 2022 года компании думали, что рынок упадёт на 20%, из-за ухода западных производителей, но из-за активных атак на инфраструктуру Российской Федерации многие компании столкнулись с проблемами, на которые нужно было реагировать.

Заказчики стали чаще обращаться к экспертам, что привело к росту рынка и резкому увеличению спроса на сервисы ИБ. Это вызвано некоторыми причинами:

– выросли продажи firewall'ов примерно в 3 раза и во столько же раз анализаторы кода на поиск уязвимостей;

– сфера ИБ более готова к отечественному импортозамещению, чем вся остальная IT-сфера, часть бюджетных средств заказчиков были перенаправлены на средства защиты, т.к. срочно требовались новые инвестиции для проектов;

– государство стало требовать от кибербезопасности результата — отсутствия взломов и утечек информации, а не как раньше, сертификации объектов, что заставило «расшевелиться» сфере ИБ.

В 2023 году рынок ИБ закрепится на отечественном производителе, если в 2022 ещё были некоторые закупки западных разработчиков, то в будущем это будет сводиться к нулю. В 250-м указе президента было указано, что после 1 января 2025 года все компании обязаны использовать средства защиты информации только отечественного производителя. Это приведёт к появлению новых средств и серьёзной борьбе компаний-гигантов, кто первый успеет, тот и получит большую выгоду и преимущества.

К 2025 году прогнозируют рост рынка на 43,8 млрд. рублей, что в общей сумме будет равно 131,8 млрд. рублей. В 2022 году множество зарубежных производителей ушли из страны, что привело к некоторым проблемам. Но где есть минусы, там есть и плюсы. Правительству пришлось задуматься о замене таких производителей, что привело к идее отечественного импорт замещения. С 2025 года отечественным компаниям будет запрещено использовать иностранное ПО, поэтому большинство проектов развиваются довольно быстро. Уже в 2023 и 2024 годах начнут внедрение некоторых отечественных ПО на предприятиях и начнут их тестирование, а к 2025 и 2027 по прогнозу закончат все проекты по импортозамещению [9, 11- 13].

ЗАКЛЮЧЕНИЕ

Кибербезопасность очень важна в любой области, будь то бизнес-сфера, медицина, образование, или государственные учреждения. На основе проведённого исследования становится понятно, что злоумышленники никогда не сидят на месте, регулярно следят за всеми обновлениями и появлением новых технологий, постоянно ищут способы проникнуть через защиту, чтобы взломать ту, или иную компанию. Поэтому не стоит недооценивать своих «врагов», необходимо качественно защищать себя и свою компанию. Для этого необходимо обучаться грамотному использованию ПК и существующих программ для защиты от угроз и уязвимостей, также обучать персонал своих компаний проводя постоянные курсы повышения квалификации, а также при необходимости переквалификации. Ни в коем случае нельзя экономить на бюджете направленным на обеспечение безопасности компании, ведь лучше потратить лишние средства на защиту, чем потерять всё из-за экономии.

Конечно, чаще всего нападения совершаются на частные лица, ведь украсть их данные гораздо легче, потому что они менее подготовлены к нападениям, но и большинство компаний тоже страдает от нападений. Уже довольно скоро появятся альтернативные отечественные ПО, которыми начнут пользоваться компании для повседневной деятельности и защиты своих сетей и т.д. Такое ПО будет легче настраивать, модернизировать, т.к. оно разработано нашими программистами, что принесёт свои плоды.

Список литературы

1. Авраменко В.С., Бобрешов-Шишов Д.И., Маликов А.В. Способ выявления уязвимостей «нулевого дня» на основе анализа поведения эксплойтов // Проблемы технического обеспечения войск в современных условиях. – 2018. – С. 45-48.

2. Гладушенко С.Г., Искольный Б.Б. Оценка вероятности компьютерных атак нулевого дня // REDS: Телекоммуникационные устройства и системы. – 2017. – Т. 7. – №. 4. – С. 481-483.

3. Атака нулевого дня информации [Электронный ресурс]. URL: https://dzen.ru/a/W-b33EE2PACqYwQf
4. Проактивная защита [Электронный ресурс]. URL: https://helpdesk.bitrix24.ru/open/9160201/
5. Число кибератак в России и в мире [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Число_кибератак_в_России_и_в_мире
6. Positive Technologies: что принес ушедший год и каких вызовов кибербезопасности ждать в 2023-м [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/about/news/positive-technologies-chto-prines-ushedshij-god-i-kakih-vyzovov-kiberbezopasnosti-zhdat-v-2023-m/
7. Маслова М.А. Риски IT-инфраструктуры и методы их решения // Научный результат. Информационные технологии. – Т.7, №4, 2022. С. 34-40. DOI: 10.18413/2518-1092-2022-7-4-0-4.
8. Российское программное обеспечение (Отечественное ПО) [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Российское_программное_обеспечение_(Отечественное_ПО)
9. Переход на отечественное ПО ускорится в 2023 году [Электронный ресурс]. URL: https://rg.ru/2023/02/02/perehod-na-otechestvennoe-po-uskoritsia-v-2023-godu.html
10. Информационная безопасность (рынок России) [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Информационная_безопасность_(рынок_России)
11. Омельченко В.И., Исаев М.Ю. Использование планшетных компьютеров с отечественным программным обеспечением при проведении учебных занятий // Информационные технологии: актуальные проблемы подготовки специалистов с учетом реализации требований ФГОС. – 2021. – С. 354-357.
12. Голубев О.Б., Попова Е.Ю. Использование отечественного программного обеспечения в учебном процессе // Современные проблемы и перспективы обучения математике, физике, информатике в школе и вузе. – 2020. – С. 168-172.
13. Маслова М.А., Смирнов Н.С. Программная реализация оценки рисков информационной безопасности // Современные проблемы радиоэлектроники и телекоммуникаций. – 2022. – № 5. – С. 203.

References

1. Avramenko V.S., Bobreshov-Shishov D.I., Malikov A.V. A method for identifying zero-day vulnerabilities based on the analysis of exploits behavior // Problems of technical support of troops in modern conditions. – 2018. – pp. 45-48.
2. Gladushenko S.G., Iskolny B.B. Assessment of the probability of zero-day computer attacks // REDS: Telecommunication devices and systems. – 2017. – Vol. 7. – No. 4. – pp. 481-483.
3. Zero-day information attack [Electronic resource]. URL: https://dzen.ru/a/W-b33EE2PACqYwQf.
4. Proactive protection [Electronic resource]. URL: https://helpdesk.bitrix24.ru/open/9160201/.
5. The number of cyber-attacks in Russia and in the world [Electronic resource]. URL: https://www.tadviser.ru/index.php/Статья:Number of cyberattacks in_Russia_and_world.
6. Positive Technologies: what the past year has brought and what challenges to cybersecurity to expect in 2023 [Electronic resource]. URL: https://www.ptsecurity.com/ru-ru/about/news/positive-technologies-chto-prines-ushedshij-god-i-kakih-vyzovov-kiberbezopasnosti-zhdat-v-2023-m/.
7. Maslova M.A. IT infrastructure risks and methods for their solution // Research result. Information technologies. – T.7, №4, 2022. – P. 34-40. DOI: 10.18413/2518-1092-2022-7-4-0-4.
8. Russian software (Domestic software) [Electronic resource]. URL: https://www.tadviser.ru/index.php/Статья:Russian Software Support_(Domestic_BY).
9. The transition to domestic software will accelerate in 2023 [Electronic resource]. URL: https://rg.ru/2023/02/02/perehod-na-otechestvennoe-po-uskoritsia-v-2023-godu.html.
10. Information security (Russian market) [Electronic resource]. URL: https://www.tadviser.ru/index.php/Статья:Information Security (Market_Russia).
11. Omelchenko V.I., Isaev M.Yu. The use of tablet computers with domestic software during training sessions // Information technologies: actual problems of training specialists taking into account the implementation of the requirements of the Federal State Educational Standard. – 2021. – pp. 354-357.
12. Golubev O.B., Popova E.Yu. The use of domestic software in the educational process // Modern problems and prospects of teaching mathematics, physics, computer science at school and university. – 2020. – pp. 168-172.

13. Maslova M.A., Smirnov N.S. Software implementation of information security risk assessment Modern problems of radio electronics and telecommunications. – 2022. – № 5. – P. 203.

Кузьминых Егор Сергеевич, студент третьего курса кафедры Информационная безопасность Института информационных технологий
Маслова Мария Александровна, старший преподаватель кафедры Информационная безопасность Института информационных технологий

Kuzminykh Egor Sergeevich, Third-year Student of the Department Information security, Institute of Information Technologies
Maslova Maria Alexandrovna, Senior Lecturer of the Department Information security Institute of Information Technologies