Вестник Челябинского государственного университета. 2022. № 11 (469). С. 177—181.
ISSN 1994-2796 (print). ISSN 2782-4829 (online)
Bulletin of Chelyabinsk State University. 2022;(11(469):177-181. ISSN 1994-2796 (print). ISSN 2782-4829 (online)

Обзорная статья

УДК 338.24

doi: 10.47475/1994-2796-2022-11119

НОВЫЕ ВЫЗОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МАЛОГО И СРЕДНЕГО БИЗНЕСА

Дмитрий Александрович Плетнев[1], Сергей Николаевич Викулин[2], Павел Геннадьевич Щелканогов[2], Александр Дмитриевич Плетнев[3]

[1] Челябинский государственный университет, Челябинск, Россия, pletnev@csu.ru, ORCID: 0000-0002-6494-572X

[2] ООО «Защитник сайтов», Челябинск, Россия, vuln.detector@internet.ru

[3] Университет ИТМО, Челябинск, Россия, pletnev.sasa@gmail.com

Аннотация. Дан обзор актуальных в 2022 г. вызовов информационной безопасности малого и среднего бизнеса в России. Особое внимание уделено вопросу соотношения стоимости и эффекта таких систем, субъективному восприятию необходимости таких систем руководством фирм, вопросам доверия к отечественным и зарубежным разработкам в этой сфере, а также надежности зарубежных поставщиков. Сформулированы предложения по совершенствованию государственной и медийной поддержки темы обеспечения информационной безопасности малого и среднего бизнеса.

Ключевые слова: информационная безопасность, малый бизнес, средний бизнес, малый и средний бизнес

Для цитирования: Плетнев Д. А., Викулин С. Н., Щелканогов П. Г., Плетнев А. Д. Новые вызовы информационной безопасности малого и среднего бизнеса // Вестник Челябинского государственного университета. 2022. № 11 (469). Экономические науки. Вып. 78. С. 177—181. doi: 10.47475/1994-2796-2022-11119.

Review article

NEW CHALLENGES TO INFORMATION SECURITY OF SMALL AND MEDIUM BUSINESS

Dmitry A. Pletnev[1], Sergey N. Vikulin[2], Pavel G. Shchelkanogov[2], Alexander D. Pletnev[3]

[1] Chelyabinsk State University, Chelyabinsk, Russia, pletnev@csu.ru, ORCID: 0000-0002-6494-572X

[2] LLC SiteProtector, Chelyabinsk, Russia, vuln.detector@internet.ru

[3] ITMO University, Chelyabinsk, Russia, pletnev.sasa@gmail.com

Abstract. The article provides an overview of the information security challenges of small and medium-sized businesses in Russia that are relevant in 2022. Particular attention is paid to the question of the ratio of the cost and effect of such systems, the subjective perception of the need for such systems by the management of firms, issues of trust in domestic and foreign developments in this area, as well as the reliability of foreign suppliers. Proposals have been formulated to improve state and media support for the topic of ensuring information security for small and medium-sized businesses.

Keywords: information security, small business, medium business, small and medium business

For citation: Pletnev DA, Vikulin SN, Shchelkanogov PG, Pletnev AD. New challenges of information security of small and medium business. *Bulletin of Chelyabinsk State University.* 2022;(11(469):177-181. (In Russ.). doi: 10.47475/1994-2796-2022-11119.

Введение

Перед рассмотрением основных особенностей информационной безопасности малых и средних предприятий в современных условиях назовем ключевые аспекты их деятельности, попадающие под «зонтик» понятия «информационная безопасность». Во-первых, это угроза потери (или фальсификации) данных информационной системы предприятия, баз данных, документов вследствие

вирусной активности. Во-вторых, это нарушение нормального порядка работы информационной системы (в том числе сайтов и онлайн-магазинов). В-третьих, это риск сбора, похищения и неправомерного использования информации о работе предприятия и его клиентов. В-четвертых, это риск отвлечения бизнеса и его руководства от решения производственных и маркетинговых задач в случае актуализации угроз. В-пятых, это риск отказа работы приобретенных ранее информационных систем и систем информационной безопасности. В современных условиях обеспечение информационной безопасности имеет свою специфику, которую руководители бизнеса должны учитывать при выборе стратегии обеспечения информационной безопасности своих компаний. И, более того, для предприятий малого и среднего бизнеса также существуют свои актуальные вызовы, анализ которых и является целью настоящей статьи.

Актуальная проблема обеспечения безопасности малого и среднего бизнеса нашла свое отражение в свежих научных исследованиях Н. П. Макаркина и коллег [1], Г. В. Гарате [2], Е. В. Акинфеевой [3], С. А. Петренко и коллег [4], Е. В. Кудряшовой [5]. Высказываются предложения о налоговом стимулировании внедрения систем информационной безопасности, делается акцент на оценке экономической эффективности, а также описываются отдельные критические риски в этом направлении. Однако в систематизированном виде вызовы информационной безопасности малого и среднего бизнеса в России не названы.

Основные вызовы информационной безопасности малого и среднего бизнеса

Одним из важных вопросов обеспечения информационной безопасности является проблема соотнесения стоимости и выгод от применения современных решений в этой области. Известные игроки рынка предлагают решения стоимостью около 1 млн руб. в год для защиты всей компании (см. таблицу на с. 179).

Несложный расчет для случая покупки продукта за 1 млн руб. в год для защиты всей компании покажет, что для малого или среднего бизнеса, который оценивает вероятность наступления самых неблагоприятных событий в области информационной безопасности в 3—5 %, уравновешивающие затраты должны составить 1 000 000 / 0.04 = 25 000 000 (руб.). Представить себе ситуацию, когда сторонний хакер, вирус или атака приведут к подобным убыткам компании с оборотом 200—300 млн руб., получается не у каждого директора. Поэтому решение о покупке известной, имеющей хорошую репутацию, но дорогой системы откладывается.

С другой стороны, на рынке существуют не столь известные и более дешевые решения, в том числе разработанные отечественными специалистами. Казалось бы, отличный вариант для небольшого бизнеса. Однако здесь помимо чисто финансового критерия возникает вопрос доверия: насколько результаты проверки точны? Насколько сотрудничество с такой фирмой позволит избежать угроз и, кроме того, не создать новых из-за недобросовестного поставщика услуг в области информационной безопасности.

И в этом вопросе необходимо вспомнить о так называемой сигнальной теории М. Спенса, Дж. Акерлофа и Дж. Стиглица, согласно которой доверие может основываться на особых сигналах, говорящих о качестве товара или услуги. В случае услуг информационной безопасности такого рода сигналом могут стать национальная сертификация, наработанная репутация и отзывы довольных клиентов, публичное использование системы авторитетными организациями. Один из основных сигналов для профессионального сообщества — наличие устойчивого выражения на сленге применительно к продуктам компании (банальный пример — «вэдэшка», «сигналка для бизнеса»). Укоренение в бизнес-культуре таких названий (по типу «ксерить» или «гуглить») само по себе факт признания качества и надежности.

Одной из неожиданных проблем обеспечения информационной безопасности является «страусиная» позиция некоторых руководителей компаний: пока угрозы не актуализировались, по умолчанию лучше считать, что все в порядке. Информация об угрозах, рисках, «дырах» в системе защиты воспринимается с отрицательной коннотацией, а те, кто с ней приходит к руководителям, предлагая защиту, — чуть ли не как сама потенциальная угроза. Получается, как в старину: приносившему дурную весть султан рубил голову. Так и сейчас: лучше незнание рисков и угроз — спокойнее спится. Очевидно, что подобная позиция ставит организацию в уязвимое положение, но недостаточная осведомленность о последствиях и недостаточно проработанный вопрос об ответственности руководителя за управление информационными потоками (в том числе за утечку персональных данных) позволяют считать такой выбор разумным.

Характеристики популярных сервисов, обеспечивающих информационную безопасность в компаниях малого и среднего бизнеса
Characteristics of popular services that provide information security in small and medium-sized businesses

Продукт	Цена за 1 IP-адрес	Краткое описание (со слов представителей самой компании или ее промоутеров)	Особенности
Netsparker[1]	Около 100 000 руб. при покупке минимум 5 адресов	Netsparker Desktop WebApplication Security Scanner — однопользовательский сканер безопасности для веб-приложений. Сканер максимально автоматизирован и доступен в виде локальной версии ПО для операционных систем Windows. Исторически сложилось так, что автоматизированные сканеры веб-приложений имеют противоречивую репутацию у специалистов информационной безопасности. Считается, что автоматизированные сканеры часто подвержены ложным срабатываниям и обнаруживают только простые уязвимости	
Max Patrol 8 (XSpider)[2]	200—500 руб. в год	Система позволяет своевременно обнаружить уязвимости информационной системы, провести комплексный анализ сетевого оборудования, операционных систем, СУБД, прикладных систем и ERP-систем, веб-приложений, а также контролировать соответствие основным стандартам информационной безопасности (ISO 27001, PCI DSS, CIS). MaxPatrol 8 гибко масштабируется и подходит как для небольших компаний, так и для крупных территориально распределенных предприятий	Лидер российского рынка. По информации с сайта, до 80 %
Rapid7[3]	По запросу	Rapid7 Managed Detection and Response (MDR) использует многоуровневый подход к предоставлению превосходных услуг для вашей команды. Rapid7 SOC действует как продолжение вашей команды и защищает вашу среду от сложных атак, поэтому ваша команда может сосредоточить свое время и энергию на наиболее важных инициативах в области безопасности	Один из мировых лидеров
RedCheck[4]	2180—4360 руб. в год, при покупке от 3 или 10 лицензий, в зависимости от продукта	Программное обеспечение RedCheck — современное средство анализа защищенности, позволяющее выявлять уязвимости операционных систем и приложений, потенциально опасные настройки, осуществлять оценку соответствия требованиям политик и стандартов, проводить инвентаризацию оборудования и программ, формировать детальные отчеты. Программное обеспечение RedCheck использует передовые технологии SCAP для решения широкого спектра задач: от поиска уязвимостей до оценки соответствия отечественным и международным стандартам безопасности. Программа RedCheck позволяет реализовать ряд мер, обязательных для информационных систем персональных данных (ИСПДн), государственных информационных систем (ГИС) и автоматизированных систем, обрабатывающих конфиденциальную информацию	
Nessus Professional	По запросу	Tenable Nessus — надежная система безопасности и оценки уязвимости, которая позволяет сканировать неограниченное количество IP-адресов. Решение дает полное представление о конкретной сети, ее активах и уязвимостях, которые постоянно меняются	Возможны проблемы с поставками в Россию
Vuln-Detector	1000—5000 руб. в месяц	Полный спектр услуг для защиты интернет-сервисов и ваших клиентов от уязвимостей, контроль за сетевым периметром организации и безопасностью сети/сервера/сайта	–

Примечания

[1] https://softlist.biz/catalog/product-netsparker-desktop-web-application-security-scanner/
[2] https://store.softline.ru/positive-technologies/maxpatrol-8/
[3] https://www.rapid7.com/services/managed-services/managed-detection-and-response-services/service-overview/
[4] https://store.softline.ru/alteks-soft/redcheck/

Перечень и способ реализации рисков и угроз постоянно меняется, и система, безопасная вчера, может оказаться под угрозой сегодня. По этой причине возникает задача постоянного мониторинга системы безопасности и своевременного информирования о новых угрозах. Однако стоит отметить, что сегодняшняя работа руководителя малого и среднего предприятия многогранна и не всегда целесообразно содержать в штате целый отдел, обеспечивающий информационную безопасность. Как правило, может идти речь просто о специалистах в IT-сфере. А для таких пользователей внешней системы информационной безопасности важно, чтобы информация поступала в лаконичной форме и только тогда, когда угрозы безопасности действительно существенны, иначе она может затеряться в общем информационном потоке.

Современные реалии международной экономической кооперации таковы, что использование известных программных решений в сфере обеспечения информационной безопасности, произведенных в недружественных странах, сопряжено с рисками отказа в обслуживании и даже с нарушением принятых обязательств, вплоть до шпионажа в пользу правительств своих стран. В таких условиях вопрос импортозамещения в этой сфере становится жизненно важным для нормальной работы предприятий. Однако готовых продуктов, которые могут составить конкуренцию раскрученным мировым брендам (в том числе для малого и среднего бизнеса), крайне мало, и они не получили достаточной известности. Для компаний, развивающих такие продукты, нужен режим наибольшего благоприятствования, вплоть до существенных налоговых льгот и продвижения продуктов в бизнес-среде.

Важной является способность предсказывать вновь появляющиеся угрозы и действовать на опережение, что позволит воспользоваться «окном возможностей» в момент, когда конкуренты будут разбираться со свалившейся на них новой угрозой, «чинить» сайт и восстанавливать данные. И это могут быть угрозы, которые не проявляются прямо, но влияют на эффективность компании: например, косметические правки внедренным вирусом на сайте компании (замена символов кириллицы на латиницу и т. п.) сводят на нет усилия по продвижению сайта компании в Интернете.

Выводы

Описанные выше вызовы и особенности информационной безопасности малого и среднего бизнеса в России на современном этапе важны и требуют адекватного ответа со стороны бизнес-сообщества, органов власти и академических кругов. Конкретными шагами, которые позволили бы продвинуться в вопросах обеспечения информационной безопасности российских компаний малого и среднего бизнеса, должны стать:

1. Повышение осведомленности и грамотности руководителей малого и среднего бизнеса в отношении современных угроз информационной безопасности, базовых правил, позволяющих минимизировать угрозы без привлечения сторонних организаций.
2. Создание национальных рейтингов и реестров, в которые должны включаться отечественные, прошедшие проверку и имеющие положительную репутацию сервисы.
3. Популяризация информации об уязвимостях информационных систем для работников и клиентов компаний с целью повышения их готовности адекватно реагировать на угрозы.
4. Повышение ответственности компаний, оперирующих персональными данными, за попадание этих данных злоумышленникам, совершенствование законодательства и практики правоприменения в этом направлении.
5. В перспективе после апробации на пилотном проекте — введение для компаний, оперирующих персональными данными, страхования рисков утечки информации с варьированием страховых премий в зависимости от уровня информационного иммунитета и используемых средств обеспечения информационной безопасности, и с обязательным информированием клиентов о наличии или отсутствии страховой защиты.
6. Льготные условия, гранты на разработку со стороны государства и институтов развития, узкоспециализированные хакатоны, что будет способствовать развитию рынка в сфере информационной безопасности и, как следствие, снизит цену на услуги в сфере информационной безопасности, в том числе для малого и среднего бизнеса.

Список источников

1. Цифровизация бизнеса в условиях пандемии / Н. П. Макаркин, А. П. Горина, О. Н. Алферина, Н. В. Корнеева // Вестник Алтайской академии экономики и права. 2020. № 11-1. С. 80—85. DOI: 10.17513/vaael.1397.

2. Гарате Г. В. Применение передовой методологии безопасности в беспроводных сетях // Известия СПбГЭТУ ЛЭТИ. 2019. № 3. С. 31—37.

3. Акинфеева Е. В. Информационная безопасность как фактор эффективной деятельности компании // Вестник МИРБИС. 2019. № 4 (20). С. 79—88. DOI: 10.25634/MIRBIS.2019.4.9.

4. Петренко С. А., Петренко А. А., Костюков А. Д. Киберустойчивость цифровых экосистем // Защита информации. Инсайд. 2021. № 4 (100). С. 17—23.

5. Кудряшова Е. В. Проблемы техники налогового стимулирования обеспечения кибербезопасности для малого и среднего бизнеса // Финансы и кредит. 2019. Т. 25, № 3 (783). С. 609—617. DOI: 10.24891/fc.25.3.609.

References

1. Makarkin NP. Digitalization of business in a pandemic. *Vestnik Altayskoy akademii ekonomiki i prava = Bulletin of the Altai Academy of Economics and Law*. 2020;(11-1):80-85. DOI: 10.17513/vaael.1397. (In Russ.).

2. Garate GV. Application of advanced security methodology in wireless networks. *Izvestiya SPbGETU LETI = Proceedings of SPbGETU LETI*. 2019;(3):31-37. (In Russ.).

3. Akinfeeva EV. Information security as a factor in the effective operation of the company. *Vestnik MIRBIS = Bulletin of MIRBIS*. 2019;(4(20):79-88. DOI: 10.25634/MIRBIS.2019.4.9. (In Russ.).

4. Petrenko SA. Cyber resilience of digital ecosystems. *Zashchita informatsii. Insayd = Information security. Inside*. 2021;(4(100):17-23. (In Russ.).

5. Kudryashova EV. Problems of tax incentives to ensure cybersecurity for small and medium-sized businesses. *Finansy i kredit = Finance and credit*. 2019;(25-3):609-617. DOI: 10.24891/fc.25.3.609. (In Russ.).

Информация об авторах

Д. А. Плетнев — кандидат экономических наук, доцент, доцент кафедры экономики отраслей и рынков.

С. Н. Викулин — генеральный директор.

П. Г. Щелканогов — директор по продажам.

А. Д. Плетнев — студент.

Information about the authors

Dmitry A. Pletnev — Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of Economics of Industries and Markets.

Sergey N. Vikulin — General Manager.

Pavel G. Shchelkanogov — Sales Director.

Alexander D. Pletnev — Student.

Статья поступила в редакцию 20.09.2022; одобрена после рецензирования 12.10.2022; принята к публикации 18.10.2022.

The article was submitted 20.09.2022; approved after reviewing 12.10.2022; accepted for publication 18.10.2022.

Вклад авторов: авторы сделали эквивалентный вклад в подготовку публикации.

Contribution of the authors: the authors contributed equally to this article.

Авторы заявляют о потенциальном конфликте интересов, который не влияет на представленные выводы (двое из соавторов статьи являются работниками компаний — участников рынка обеспечения информационной безопасности).

The authors declare a potential conflict of interest that does not affect the presented conclusions (two of the co-authors of the article are employees of companies participating in the information security market).