УДК 004.042 **DOI: 10.18413/2518-1092-2020-5-4-0-5**

Величко М.С.
Маслова М.А.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК УСЛУГА В НОВОМ ДИСТАНЦИОННОМ МИРЕ

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

e-mail: maksim_velichko_2000@mail.ru, mahechka-81@mail.ru

Аннотация
2020 год в Российской Федерации привел к изменениям в работе компаний, государственных учреждений, а также ИБ-подразделений в частности, что в свою очередь привлекло внимание всех вышеуказанных к перепланировке дальнейшего ведения бизнеса. Первенствующим фактором, послужившим изменениям на рынке информационной безопасности в Российской Федерации и в принципе во всем мире, является переход подавляющего количества компаний на удаленный режим работы из-за неожиданной пандемии. Из-за спонтанного характера изменений организации были вынуждены перестраиваться на ходу, изменять методы и способы обеспечения информационной безопасности, более того совершать переход на новые технические средства для распознавания по принципу “свой – чужой”, в том числе, с использованием искусственного интеллекта. Так же возникла огромная проблема с персоналом, его опытом, грамотностью и оснащенностью рабочими местами в домашних условиях, в том числе с их защищенностью. Появилась четкая проблема, которая требовала незамедлительного решения и выхода из сложившегося положения без больших потерь и с минимальными затратами.
Ключевые слова: бизнес; удаленный режим работы; обеспечение информационной безопасности; «удаленка»; технологий обеспечения информационной безопасности.

UDC 004.042

Velichko M.S.
Maslova M.A.

INFORMATION SECURITY AS A SERVICE IN THE NEW REMOTE WORLD

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

e-mail: maksim_velichko_2000@mail.ru, mahechka-81@mail.ru

Abstract
The year 2020 in the Russian Federation led to changes in the work of companies, government agencies, and information security departments in particular, which in turn attracted the attention of all of the above to the redevelopment of further business operations.
The primary factor that has led to changes in the information security market in the Russian Federation and, in principle, around the world, is the transition of an overwhelming number of companies to remote operation due to an unexpected pandemic. Due to the spontaneous nature of changes, organizations were forced to rebuild on the go, change methods and methods of ensuring information security, and even make the transition to new technical means for recognition on the “friend–foe” principle, including using artificial intelligence. There was also a huge problem with the staff, their experience, literacy and equipment of workplaces at home, including their security. There was a clear problem that required an immediate solution and a way out of the current situation without large losses and with minimal costs.
Keywords: business; remote mode of operation; information security; "remote"; information security technologies.

ВВЕДЕНИЕ

Существенный скачок нагрузки на ИТ и ИБ-подразделения, является следствием спонтанного и широкого перехода на формат удалённой работы. Возникла резкая необходимость разработки новых, современных средств защиты информации для всех направлений сфер

деятельности человека. При этом они должны соответствовать законам, правилам и требованиям, выдвигаемым к ним. Необходимо стало очень внимательно выбирать платформы для работы, проведения совещаний, учебы, обработки документов, электронных торгов и т.д., чтоб они не только были приоритетными, но и самое главное безопасными. Данный переход должен быть адаптированным к базовым принципам наступивших трудностей, с проведением анализа рисков и проблем информационной безопасности при защите каналов удаленной работы. Обострился вопрос профессиональной грамотности сотрудников в области информационной безопасности, так как возросли риски инцидентов информационной безопасности.

ОСНОВНАЯ ЧАСТЬ

Однако, ряд организаций видит в сложившейся ситуации благоприятное развитие. “В дальнейшем это может изменить структуру ключевых рисков ИБ и в значительной мере повлиять на развитие ИБ, и критичность проектов. В перспективе 2-3 лет ИБ и ИТ всё больше будет уходить в облака, чтобы подобные резкие переходы на «удалёнку» не были столь болезненными для бизнеса", – полагает Алексей Горелкин, “CEO Phishman”.

Дмитрий Пудов – заместитель генерального директора по технологиям и развитию группы компаний “Angara”, отмечает три основных изменения в текущем моменте времени: стремительная эскалация российских производителей, совершенствование организационных вопросов, повышенное внимание к использованию управляемых сервисов (Managed Services) в ИБ. “Я достаточно оптимистично оцениваю перспективы российского рынка ИБ. Более того, текущая ситуация может даже стать катализатором роста. Произошедшее заставило многие организации обратить внимание на существующие пробелы в этой области, на вопросы готовности к безопасному цифровому взаимодействию с клиентами и партнерами”, – заявляет Дмитрий Пудов.

В «Кросс Технолоджис» замечают возросший уровень зрелости компаний и отмечают, что многие организации пришли к процессам центров мониторинга кибербезопасности и постепенно начинают внедрять SOAR системы с оптимизацией сценариев реагирования в рамках бизнес-процессов. “Тренды сегодняшнего дня – это SOAR (автоматизация), сети нулевого доверия, поведенческая аналитика об этом свидетельствую регулярные запросы, поступающие от заказчиков в нашу компанию. На первое место встают вопросы автоматизации процессов инцидент менеджмента, по части реагирования и расследования инцидентов информационной безопасности с внедрением систем помощи принятия решений на базе алгоритмов машинного обучения, – рассказывают в «Кросс Технолоджис»”.

По мнению директора департамента развития технологий компании “Аладдин Р.Д.” – Дениса Суховея, рынок ИБ приобрёл совершенно новые приоритеты. Проблемы внедрения и функционирования методов и технологий обеспечения информационной безопасности стали первоочередной задачей подавляющего большинства организаций. Недавняя обстановка была такова: внедрение мер защиты предприятиями было следствием уже произошедших инцидентов в компаниях. Текущая ситуация свидетельствует об обратном: предприятия прилагают все усилия, чтобы вести упреждающую политику защиты от угроз информации [5, 6].

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

Опыт спонтанного объединения ресурсов в экстренных обстоятельствах 2020 года, а также объективные изменения развития экономики и бизнеса побудили преобразования к подходам обеспечения информационной безопасности. Прогресс в развитии большинства технологий чаще всего является импульсом для изменений в информационной безопасности, а из этого вытекает рост инвестирования в целом.

Генеральный директор “EveryTag” Сергей Войнов прогнозирует, что подобные изменения ориентиров ИБ в организациях из крупного, среднего и малого бизнеса приведут не только к противодействию угрозам утечки информации, но и гарантированно определят злоумышленников. Помимо этого, Сергей отмечает, что компании будут прилагать больше усилий при подготовке

персонала к правилам безопасной работы с информацией, так как текущая ситуация далека от идеала [7].

Руководитель Дирекции информационной безопасности компании “Калуга Астрал” Дмитрий Елфимов считает, что повсеместная информатизация бизнеса и государственных органов всё также будет влиять на изменения в рынке ИБ. К характерным изменениям можно отнести усиленное внедрение искусственного интеллекта для решения вопросов защиты информации, он примет на себя часть оперативных, ситуационных решений, что снизит нагрузку на специалистов по информационной безопасности.

Директор по развитию “Аванпост” Олег Губка утверждает, что несмотря на условия пандемии для рынка ИБ пока не наступили значимые негативные последствия. Он также характеризует апрель месяц оптимизацией к новым условиям, которым свойственна низкая рыночная активность. С другой стороны, май отличился возросшим количеством запросов от партнеров и заказчиков. “Хочется надеется, что такая высокая активность сохранится до конца года и она не будет подвержена привычным сезонным колебаниям. Это поможет лучше справится с внешними негативными факторами, влияющими на российскую экономику в целом”, – говорит Олег Губка [8].

Председатель совета директоров “СёрчИнформ” Лев Матвеев считает, что весна и лето 2020 года оказали стрессовое воздействие на компании, что в свою очередь послужило проверкой отказоустойчивости представителей рынка. “Кто закатал рукава и работает, имеет технически сильный продукт – защищен своим же продуктом от всех невзгод. А у кого были скорее хорошие продажи и административный ресурс, тот просит помощи у государства. Отчасти исход нынешнего кризиса повлияет на рынок в 2021-2022 году: может оказаться, что ряду вендоров будет нечего предложить заказчикам. Но спроса меньше не станет. Чем больше бизнес-процессов уходит в «цифру», тем больше информации нужно защищать: ведь одно дело, когда ты за ПК читаешь новости, совсем другое – когда оформляешь сделку в электронном документообороте. Процесс цифровизации не останавливается, поэтому верхняя планка рынка ИБ продолжит расти. Вдобавок недавний массовый переход на «удаленку» обнажил многие проблемы корпоративной безопасности, повысил требования к защите”, – рассказывает Лев Матвеев.

Директор по развитию бизнеса “Positive Technologies” в России Максим Филиппов, прогнозирует возможные проблемы блокировки бюджетов компаний и задержек поставок оборудования. Помимо этого, акцентирует внимание на острых вопросах увеличения числа инцидентов ИБ, вызванных повышенной активностью злоумышленников. По мнению Максима Филиппова, всё вышеперечисленное приведет компании к заморозке их проектов. “Если режим удаленной работы затянется, то можно прогнозировать вероятные изменения в ландшафте российского рынка ИБ, в том числе за счет поглощений и банкротств тех его игроков, которые не смогут аккуратно и вдумчиво спланировать свой кэш-флоу, оптимизировать затраты, то есть в целом подготовиться к тому, чтобы «проскочить» этот год. Негативные тренды, сопряженные с этими событиями, мы будем остро чувствовать не только во второй половине 2020-го года, но и в следующем 2021-ом году. И, пожалуй, следующий 2021-ый год вызывает не меньшую тревогу, чем вторая половина текущего”, – добавляет эксперт.

Директор по стратегическому развитию Axoft, дистрибутора ИТ-решений разных вендоров Евгений Куртуков утверждает, что из всех сегментов ИТ-рынка ИБ уверенно держит планку первенства, о чем свидетельствует рост прибыли в этой отрасли. Опыт работы компании “Axont” показывает, что частично ИТ-проекты переносятся, а необходимость в ИБ, наоборот, носит первостепенный характер у заказчиков. “Доходит до удивительного. У нас есть блок решений по направлению network performance (производительность сети). Казалось бы, эта тема должна быть сейчас «горячей», потому что многие ушли на удаленку, нагрузка на сеть возрастает. Но даже проекты в этой области сдвигаются из-за ИБ”, – заявил представитель Axoft.

Михаил Прибочий – управляющий директор “Лаборатории Касперского” в России, СНГ и Прибалтике, рассказывает о положительной динамике компании, несмотря на падение прибыли в некоторых её сегментах. Подобный рост обусловлен массовой повышенной необходимостью в ИБ

организаций-заказчиков. Продажи через сервис-провайдеров и корпоративные решения показывают наиболее высокие результаты, а именно благодаря сервисам Kaspersky xSP Value Added Services. Особенностью этого канала является то, что продажи ведутся большинством сотрудников, работающих на дому. Обратной стороной такого подхода является повышенная опасность угроз информации, отсюда вытекает необходимость усиленной защиты указанного канала [5-8].

Увеличилось на 50% число атак злоумышленников на инфраструктуру в корпоративном секторе. Заказчики пришли к выводу о необходимости усилении защиты инфраструктуры в целом, тогда как ранее многими компаниями предполагалось, что защиты конечной точки будет достаточно [2-4].

В неблагоприятной ситуации оказался разработчик DLP-решений Infowatch, о чем свидетельствует снижение продаж в первой четверти 2020 года. Константин Левин, вице-президент по продажам компании пояснил, что текущие обстоятельства неразрывно связаны со стагнацией крупного корпоративного бизнеса [1, 11].

Директор по развитию бизнеса Positive Technologies в России Максим Филиппов, отмечает пока что неплохую динамику роста компании, ссылаясь на показатели периода 2019 года. Подобным ростом организация обязана 3 крупным контрактам, а также заказчикам в лице государственного сектора и компаний с государственным участием. Следствием снижения спроса со стороны среднего и малого бизнеса стало ослабление динамики внедрения сканера уязвимостей XSpider. “Наши региональные продажи демонстрируют положительную динамику, но уже есть негативные тренды. Мы это связываем с тем, что региональным руководителям со стороны правительства была дана некая индульгенция на распоряжение бюджетами с точки зрения ликвидации последствий сложившейся ситуации. И очевидно, что тут бюджеты информационной безопасности у некоторых из них стали разменной монетой: они либо приостановились, либо перенеслись на будущие периоды”, – пояснил Максим Филиппов.

Более того, компании “Positive Technologies” и “Лаборатория Касперского” начали чаще сталкиваться просьбами клиентов об отсрочках платежей, предоставлении специальных скидок, обосновывая их текущей ситуацией. Клиенты иногда требуют скидки, отсрочки, бесплатные поставки, даже ничем это, не мотивируя [10].

ЗАКЛЮЧЕНИЕ

Подводя итог всему вышеперечисленному, можно уверенно утверждать о беспрецедентном влиянии пандемии, а как следствие удаленного режима работы на все сегменты ИТ и ИБ в частности. По большей части ИБ показывает своевременную готовность оказать усиленную поддержку безопасности нового формата работы компаний и отреагировать на стремительно возросший спрос рынка. Что касательно заказчиков, то крупные ИТ-компании и государственный сектор смогли оперативно адаптироваться к текущей ситуации. Их основной проблемой, стала необходимость повышения информационной грамотности сотрудников. Представители малого и среднего бизнеса, вдобавок к этой проблеме, столкнулись с более ощутимыми финансовыми трудностями, что может стать причиной банкротства некоторых компаний. Эффективность внедрения новых бизнес-моделей и технологий выражается в том, что часть организаций заявляют о своей готовности продолжить работу в удаленном режиме после отмены карантина. Из сложившейся ситуации видно, что благодаря дистанционному формату не только это повлияло на увеличение роста защиты информации на более высоком уровне, но и на ее качество оказываемых услуг.

Список литературы

1. Бутин А.А., Василевская А.Н. Обзор основных рекомендаций по предупреждению инцидентов информационной безопасности в условиях удаленной работы и режима самоизоляции // Информационные технологии и математическое моделирование в управлении сложными системами. 2020. № 2 (7). С. 39-45.
2. Более половины российских компаний в период пандемии увеличили расходы на

кибербезопасность, 2020 г. URL: https://www.cnews.ru/news/line/2020-07-17_bolee_poloviny_rossijskih – (дата обращения: 29.10.2020).

3. Гончаренко Ю.Ю., Кушнарев А.А., Исаков С.А. Программная реализация методики определения актуальных угроз безопасности персональных данных // Научный результат. Информационные технологии. – Т.4, №1, 2019. С. 9-14.

4. Ерышов В.Г., Ерышов Н.В. Анализ угроз информационной безопасности в условиях перехода сотрудников организации на удаленный режим работы // Национальная безопасность России: актуальные аспекты. Сборник избранных статей Всероссийской научно-практической конференции. СПб, 2020. С. 17-20.

5. Ермакова Е.О. Устойчивость информационной среды учреждения при организации удаленной работы // Системы управления, сложные системы: моделирование, устойчивость, стабилизация, интеллектуальные технологии. Материалы VI Международной научно-практической конференции, посвященной 100-летию со дня рождения профессора А.А. Шестакова. Елецкий государственный университет им. И.А. Бунина. Елец, 2020. С. 131-134.

6. Информационная безопасность (рынок России), 2020 г. URL: https://www.tadviser.ru/index.php/Статья:Информационная_безопасность_(рынок_России)#.D0.9E.D0.B6.D0.B8.D0.B4.D0.B0.D0.BD.D0.B8.D1.8F_.D0.BF.D0.BE_.D0.B8.D1.82.D0.BE.D0.B3.D0.B0.D0.BC_.D0.B3.D0.BE.D0.B4.D0.B0 – (дата обращения: 19.10.2020).

7. Как российский рынок информационной безопасности переживает эпидемию коронавируса в 2020 году URL: https://www.anti-malware.ru/analytics/Market_Analysis/how-russian-information-security-market-experiencing-coronavirus-epidemic-in-2020 – (дата обращения: 23.10.2020).

8. Как пандемия меняет ИБ-рынок, 2020 г. URL: https://www.comnews.ru/content/205669/2020-04-20/2020-w17/kak-pandemiya-menyaet-ib-rynok – (дата обращения: 25.10.2020).

9. Коронавирус и кибербезопасность: Информационная безопасность в условиях пандемии COVID-19, 2020 г. URL: https://expert.ru/2020/04/9/informatsionnaya-bezopasnost-v-usloviyah-pandemii-covid-19/ – (дата обращения: 23.10.2020).

10. Логинова Е.В. Обеспечение информационной безопасности коммерческого предприятия при переводе сотрудников на удаленную работу // Национальная безопасность России: актуальные аспекты. Сборник избранных статей Всероссийской научно-практической конференции. СПб, 2020. С. 12-15.

11. Маслова М.А., Лагуткина Т.В. Анализ и выявление положительных и отрицательных сторон внедрения дистанционного обучения // Научный результат. Информационные технологии. – Т.5. – №2. – С. 54-60.

12. Оладько В.С. Инциденты сетевой безопасности в системе цифровой экономики // Научный результат. Информационные технологии. – Т.4, №4, 2019. С. 19-30.

13. Sirotskiy A.A. Information security of the automated systems of financial credit institutions // Contemporary Problems of Social Work. 2016. Т. 2. № 2 (6). P. 185-193.

References

1. Butin A.A., Vasilevskaia A.N. Overview of basic recommendations for preventing information security incidents under remote work and self-isolation mode // Information technology and mathematical modeling in the management of complex systems: electronic scientific journal, 2020. No. 2(7). P. 39-45.

2. More than half of Russian companies have increased spending on cybersecurity during the pandemic, 2020 g. URL: https://www.cnews.ru/news/line/2020-07-17_bolee_poloviny_rossijskih – (data access: 29.10.2020).

3. Goncharenko Yu.Yu., Kushnarev A.A., Isakov S.A., Software implementation of the method for determining the actual threats to the personal data security // Research results. Information technologies, Vol. 4, No. 1, 2019. P. 9-14.

4. Eryshov V.G., Eryshov N.V. Analysis of threats to information security in the context of the transition of employees to remote operation // National security of Russia: topical aspects. Collection of selected articles of the All-Russian scientific-practical conference. SPb, 2020. P. 17-20.

5. Ermakova E.O. Stability of the information environment of the institution when organizing remote work // Control systems, complex systems: modeling, stability, stabilization, intelligent technologies. Materials of the VI International scientific-practical conference dedicated to the 100th anniversary of the birth of Professor A.A. Shestakov. Yelets State University named after I.A. Bunin. Yelets, 2020. P. 131-134.

6. Information security (Russian market), 2020. URL: https://www.tadviser.ru/index.php/Stat`ya:Informacionnaya_bezopasnost`_(ry`nok_Rossii)#.D0.9E.D0.B6.D0.B8.D0.B4.D0.B0.D0.BD.D0.B8.D1.8F_.D0.BF.D0.BE_.D0.B8.D1.82.D0.BE.D0.B3.D0.B0.D0.BC_.D0.B3.D0.BE.D

0.B4.D0.B0— (data access: 19.10.2020).

7. How the Russian information security market is going through the coronavirus epidemic in 2020. URL: https://www.anti-malware.ru/analytics/Market_Analysis/how-russian-information-security-market-experiencing-coronavirus-epidemic-in-2020— (data access: 23.10.2020).

8. How the pandemic is changing the cybersecurity market, 2020. URL: https://www.comnews.ru/content/205669/2020-04-20/2020-w17/kak-pandemiya-menyaet-ib-rynok – (data access: 25.10.2020).

9. Coronavirus and Cybersecurity: Information Security in the COVID-19 Pandemic, 2020. URL: https://expert.ru/2020/04/9/informatsionnaya-bezopasnost-v-usloviyah-pandemii-covid-19/ — (data access: 23.10.2020).

10.Loginova E.V. Ensuring information security of a commercial enterprise when transferring employees to remote work // National security of Russia: topical aspects. Collection of selected articles of the All-Russian scientific-practical conference. SPb, 2020. P. 12-15.

11.Maslova M.A., Lagutkina T.V. Analysis and identification of positive and negative aspects of distance learning implementation // Research results. Information technologies. 2020. T. 5. № 2. P. 54-60.

12. Oladko V.S. Network security incidents in the digital economy system // Research results. Information technologies, Vol. 4, No. 1, 2019. P. 9-14.

13. Sirotskiy A.A. Information security of the automated systems of financial credit institutions // Contemporary Problems of Social Work. 2016. T. 2. № 2(6). P. 185-193.

Величко Максим Сергеевич, студент 4 курса кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности
Маслова Мария Александровна, аспирант, старший преподаватель кафедры «Информационная безопасность» Института радиоэлектроники и информационной безопасности

Velichko Maxim Sergeevich, 4th year student of the Department Information security, Institute of Radioelectronics and Information security
Maslova Maria Alexandrovna, post-graduate student, senior lecturer of the Department «Information security», Institute of Radioelectronics and Information security