УДК 330.1

Бабич Елена Сергеевна,
студентка
Экономико-правовое обеспечение экономической безопасности,
Саратовский государственный технический университет имени Гагарина Ю.А.
Россия, г. Саратов
e-mail: elena.babich.98@mail.ru

КИБЕРБЕЗОПАСНОСТЬ СОВЕРМЕННОГО ЭТАПА РАЗВИТИЯ ЭКОНОМИКИ

Аннотация: *Пандемия COVID-19 и усилия по ее сдерживанию имели серьезные экономические и деловые последствия. По мере того как компании расширяют свои обязательства в отношении удаленной рабочей силы, команды по кибербезопасности должны учитывать новые риски, помогая создавать ценность бизнеса. Повышение уровня кибербезопасности не всегда является достаточным для обеспечения развития цифровой экономики. На сегодняшний день, инциденты кибербезопасности происходят в каждом секторе экономики и повседневной жизни. Для описания проблематики использовался статистический метод и метод анализа. Ключевое значение в этом контексте приобретают проблемы разработки оптимальных механизмов управления социотехническими системами, образующими цифровую экономику. В статье приводится анализ бюджетов организаций и инструменты, которые используются в качестве фундаментальных компонентов для кибербезопасности.*

Ключевые слова: киберпространство, кибербезопасность, цифровая экономика, кибератака, цифровизация.

Babich Elena Sergeevna,
student
Economic and legal support of economic security,
Saratov State Technical University named after Y. Gagarin
Russia, Saratov

CYBER SECURITY STAGE OF ECONOMIC DEVELOPMENT

Abstract: *The COVID-19 pandemic and efforts to contain it have had serious economic and business implications. As companies expand their commitment to a remote workforce, cybersecurity teams must be mindful of new risks to help create business value. Increasing the level of cybersecurity is not always sufficient to ensure the development of the digital economy. Today, cybersecurity incidents occur in every sector of the economy and daily life. To describe the problematic, a statistical method*

and a method of analysis were used. In this context, the problems of developing optimal mechanisms for managing the socio-technical systems that form the digital economy are of key importance. The article provides an analysis of the budgets of organizations and the tools that are used as fundamental components for cybersecurity.

Key words: cyberspace, cybersecurity, digital economy, cyberattack, digitalization.

Основным глобальным трендом жизни современного человека и общества был и остается все больший уход в область онлайн-существования. Этому объективному революционному изменению жизни невозможно и бессмысленно сопротивляться. Но возможно и крайне необходимо учитывать возникающие, в связи с онлайн-существованием, новые возможности в бизнесе и новые угрозы, во всех аспектах общественной жизни: политических, личных, экономических. В связи с этим, наша тема актуальна. Менее чем за десятилетие кибербезопасность стала одной из важнейших системных проблем мировой экономики. Кибербезопасность чаще трактуется, как стратегическая проблема государства, которая затрагивает экономику страны, а так же взаимодействие национальных разработчиков программного обеспечения и систем управления, производителей оборудования и компонентов для обеспечения ИКТ-инфраструктуры. Вместе с тем, развивается цифровая экономика — это экономика, формирование и развитие которой обусловлено активным использованием в экономических процессах современных информационно-коммуникационных технологий (ИКТ) [1, с. 41]. На первый взгляд, основы кибербезопасности совершенствуются, а киберустойчивость растет. Рост расходов на кибербезопасность достигает неприемлемого уровня, и, несмотря на высокие ценники, инвестиции в безопасность, часто не приносят результатов. Совокупные глобальные расходы в настоящее время достигли 145 миллиардов долларов в год и, по прогнозам, превысят 1 триллион долларов в период между 2017 и 2021 годами. Инциденты и нападения продолжают расти, но это только верхушка новой и растущей проблемы.

Некоторые авторы часто связывают понятия кибербезопасность с информационной безопасностью и дают следующую характеристику — это

сочетание различных технологий и процессов, которые предназначены для защиты сетей, устройств и данных от атак или несанкционированного доступа. Информационная безопасность РФ в сфере экономики имеет свою специфику. В экономическом секторе под угрозой в первую очередь: кредитно-финансовая система; система государственной статистики; системы бухучета организаций и предприятий (вне зависимости от формы собственности); учетные и информационные автоматизированные системы федеральных органов исполнительной власти; системы сбора, обработки, хранения и передачи информации (налоговой, финансовой, таможенной, биржевой, а также данных о внешнеэкономической деятельности).

Уже существует глобальная нехватка потенциала в области кибербезопасности (специалистов и всей рабочей силы в целом), и по мере появления новых технологий, разрыв в навыках обеспечения кибербезопасности будет увеличиваться. В связи с этим, в настоящее время, деятельность в области кибербезопасности становится приоритетной и связана со стратегией бизнеса - минимизация нанесения ущерба ИТ-ресурсам. Растущая потребность в надежных методах аутентификации, особенно после стремительно растущей тенденции удаленной работы, дает прибыльные возможности рынку кибербезопасности.

Борис Симис, зам. гендиректора компании PositiveTechnologies, заявил, что российский рынок кибербезопасности вырос почти на четверть за 2020 год. «Наверное, многие эксперты отрасли ожидали, что в 2020 году российский рынок информационной безопасности вырастет. Причем в начале года ожидания находились на уровне в 15% и даже 30%. Все подсчеты происходят достаточно просто – мы связываемся с партнерами, коллегами, конкурентами, оцениваем их рост, делимся своим, подсчитываем средние цифры. В итоге за 2020 год мы получили 25% роста» [2].

По мере увеличения числа пользователей интернета в странах с развивающейся экономикой будут возникать те же проблемы дезинформации и кибератак, что и в более продвинутых киберпространственных странах.

Интернет-мир становится все более сложным и угрожающим. Многим организациям трудно согласовать уровень своих инвестиций в инновации, в области кибербезопасности, с результатами киберустойчивости для их бизнеса. Еще хуже то, что выбор неправильной стратегии инвестирования в технологии кибербезопасности может стоить организации гораздо больше, чем потраченные впустую деньги, это может нанести ущерб бренду, репутации и будущему процветанию организации. И C-suite, и специалисты по безопасности должны чувствовать себя ободренными. Инвестиции в инновации растут, и управление основами, по-видимому, становится лучше. Организации сталкиваются с непосильными издержками, и инвестиции в обеспечение безопасности часто терпят неудачу для большинства. При низких темпах и медленном времени восстановления важно выяснить, что ведущие организации делают по-разному для достижения киберустойчивости. Хорошая новость заключается в том, что большинство организаций в среднем тратят 10,9% своих ИТ-бюджетов на программы кибербезопасности. Лидеры тратят немного больше-11,2%, что недостаточно для того, чтобы объяснить их более высокий уровень производительности. И их инвестиции в передовые технологии, такие как искусственный интеллект, машинное обучение или роботизированная автоматизация процессов, существенно растут. Сегодня 84% организаций тратят более 20% своих бюджетов на кибербезопасность на инструменты, которые используют эти три технологии в качестве фундаментальных компонентов. Это открытие представляет собой хороший шаг вперед по сравнению с 67 процентами, потраченными три года назад. Рост еще более впечатляющий по отношению к лидерам. Три года назад только 41% лидеров тратили более 20% своих бюджетов на кибербезопасность на передовые технологии. Сегодня этот показатель вырос вдвое, до 82%.

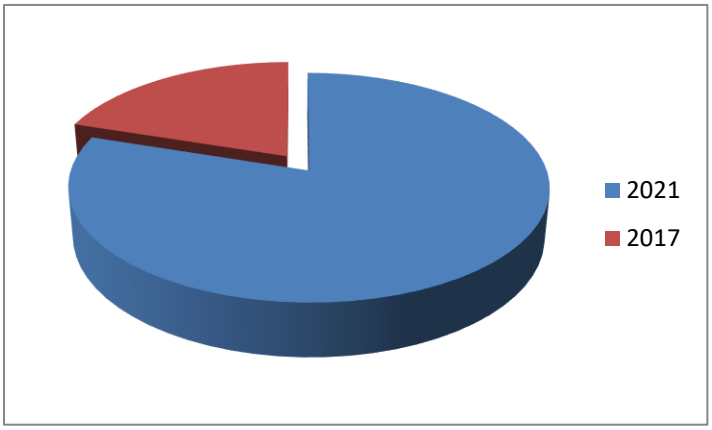

Рисунок 1. Доля организаций, тратящих более 20% своих ИТ-бюджетов на инвестиции в передовые технологии

В 2021 году движение промышленной революции к повсеместному подключению и цифровизации продолжается. Но по мере того, как новые связи и технологии поддерживают социально-экономический прогресс, кибератаки и риски, связанные с этими инновациями, будут увеличиваться по частоте и влиять на них.

Цифровая реакция на кризис COVID-19 также создала новые уязвимости в системе безопасности. Злоумышленники стремятся использовать пробелы, открывающиеся, когда удаленные сотрудники используют небезопасные устройства и сети. Субъекты угроз также используют известные методы атаки, чтобы использовать страхи людей, связанные с COVID-19. Например, Google подсчитала более 18 миллионов вредоносных и фишинговых писем, связанных с новым коронавирусом, на своем сервисе каждый день в апреле. Он также сообщил о выявлении более десятка поддерживаемых правительством групп, использующих темы COVID-19 для этих попыток.

Для поддержки экономики на ведущем уровне, главные сотрудники по информационной безопасности и команды по кибербезопасности страны должны будут подойти к следующему горизонту бизнеса с двойным мышлением. Они должны в первую очередь учитывать новые риски, связанные с переходом на удаленную цифровую рабочую среду, обеспечивая необходимую технологию. Они также должны предвидеть следующее нормальное явление - то, как их

рабочая сила, клиенты, цепочка поставок, партнеры по каналам и коллеги по сектору будут работать вместе, чтобы они могли надлежащим образом задействовать и внедрить безопасность по замыслу. Необходимо также учитывать новый контекст изменяющегося поведения клиентов и сотрудников, и постоянно меняющийся ландшафт угроз. Ответные меры на пандемию подчеркнули жизненно важную роль, которую играет кибербезопасность в обеспечении удаленных операций как во время кризиса, так и после него. По мере того как компании переосмысливают свои процессы и перестраивают архитектуру в ответ на COVID-19, команды по кибербезопасности воспринимаются по-новому. Они больше не должны рассматриваться как препятствие для роста, а должны стать признанными стратегическими партнерами в области технологий и принятия бизнес-решений. Можно заключить, что кибербезопасность цифровой экономики в широком смысле определяется не только ее защищенностью от кибератак и наличием в ней ресурсов, позволяющих функционировать в условиях их успешной реализации, но и качеством программного обеспечения ее образующих.

Список литературы:

1. Аллахвердиева Л.А., Бахшалиев Ф.Р. Кибербезопасность как фактор развития цифровой экономики // Вестник Института экономики РАН. 2019. С. 41-50.

2. Рынок информационной безопасности в РФ вырос на 25% за 2020 год [Электронный ресурс] // Режим доступа: URL: https://zen.yandex.ru/media/cisoclub/rynok-informacionnoi-bezopasnosti-v-rf-vyros-na-25-za-2020-god-6014428cd3c91450c6281f90 (дата обращения 05.02.2021 г.).

3. Шеремет И.А. Цифровая экономика и кибербезопасность ее финансового сегмента // Научные труды Вольного экономического общества. 2018. Т. 210. № 2. С. 23-34