УДК 336.368
DOI 10.21685/2587-7704-2020-5-2-7

Open Access | RESEARCH ARTICLE

Предлагаемые продукты по киберстрахованию с учетом специфики малых предприятий

А. Г. Фатеев
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

С. С. Паршина
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. Обоснована необходимость использования услуги страхования киберрисков для малого предпринимательства, приведены имеющиеся на международном рынке продукты по киберстрахованию, адаптированные для потребностей малого бизнеса. Рассмотрено законодательное регулирование в России и за рубежом в области киберстрахования, а также возможность использования его при формировании продуктов страхования киберрисков с учетом специфики малого бизнеса. Выявлены основные проблемы при формировании соответствующего продукта страхования, а также описаны возможные решения.

Ключевые слова: информационная безопасность, киберриски, страхование киберрисков, малые предприятия, система менеджмента информационной безопасности.

Cyber insurance products tailored to the specifics of small businesses

A. G. Fateev
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

S. S. Parshina
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. This article substantiates the need to use the cyber risk insurance service for small businesses and presents the cyber insurance products, adapted to the needs of small businesses, available on the international market. The article considers both the legislative regulation in Russia and abroad in the field of cyber insurance, and the possibility of its use in the formation of cyber risk insurance products, taking into account the specifics of small business. The main problems in the formation of an appropriate insurance product are identified, and their possible solutions are described.

Keywords: information security, cyber risks, cyber risk insurance, small businesses, information security management system.

В настоящее время множество новых и развивающихся угроз кибербезопасности приводит индустрию информационной безопасности в состояние повышенной готовности. Новые изощренные кибератаки, включающие вредоносные программы, фишинг, машинное обучение и искусственный интеллект, подвергают данные и активы организаций, правительств и частных лиц постоянному риску. Согласно докладу World Economic Forum [1], кибератаки считаются вторым риском, вызывающим наибольшую озабоченность у бизнеса во всем мире в течение следующих 10 лет.

Учитывая возросшие риски кибербезопасности во всем мире, крайне важно, чтобы компании предпринимали активные меры по защите своих данных и данных своих клиентов. Один из способов сделать это – приобрести киберстрахование. Сейчас киберстрахование является одним из самых

быстрорастущих секторов страхового бизнеса как для средних и крупных организаций, так и для малого бизнеса. На данный момент 43 % кибератак нацелены на малый бизнес, при этом 60 % предприятий закрываются в течение полугода после кибернападения. Слабая защищенность малых предприятий не только влияет на саму организацию, но и может привести к реализации атаки на крупные организации через настроенные доверительные каналы, поэтому крупные компании начинают требовать от своих поставщиков наличия страхования от киберрисков. На рис. 1 представлена линейчатая диаграмма, показывающая актуальность типов кибератак для малого бизнеса в 2017 и 2018 гг. [2]. Из-за возросшей конкуренции со стороны киберстраховщиков многие малые компании могут позволить себе купить полис киберстрахования. Многие зарубежные страховые компании предлагают свои продукты по страхованию киберрисков с учетом потребностей малого бизнеса.

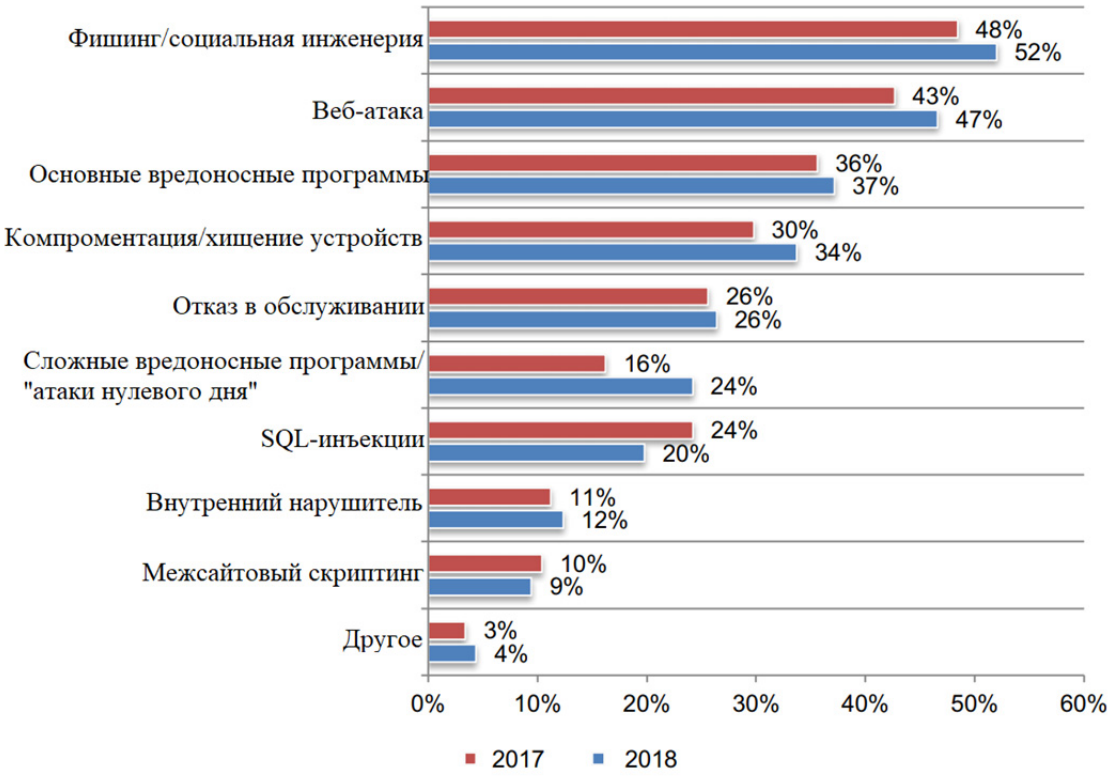

Рис. 1. Линейчатая диаграмма типов кибератак для малого бизнеса в 2017 и 2018 гг.

Одной из лучших компаний по предоставлению услуг киберстрахования для малого бизнеса на мировом рынке являются *Chubb*, *AIG*, *Hiscox*, *Liberty Mutual*, *Travelers*, *CyberDot*.

Ниже будут рассмотрены особенности каждой компании.

Компания *Chubb* занимает 12 % рынка киберстрахования. Предлагаемые полисы киберстрахования включают защиту от различных типов угроз и могут адаптироваться к каждому бизнесу в соответствии с его потребностями. Основными особенностями страховой компании являются:

– снижение потерь и оказание услуг после инцидентов;

– покрытие расходов на вымогательство;

– покрытие от других рисков, таких как социальная инженерия, мошеннические переводы и компьютерное мошенничество.

Компания *AIG* владеет 22 % рынка страхования киберрисков и предлагает гибкие решения, которые могут быть сформированы в соответствии с потребностями каждого клиента. Особенности основных страховых продуктов следующие:

– *CyberEdge* – покрывает расходы, вызванные утечкой информации, а также расходы страхователя на восстановление данных и управление событиями. Данный полис также гарантирует защиту от прерывания работы сети и кибервымогательства;

– *CyberEdge Plus* – покрывает расходы, вызванные кибератаками в физическом мире, такие как расходы на прерывание бизнеса, ущерб имуществу страхователя и третьим лицам, а также различные физические травмы третьим лицам.

Продукция компании *Hiscox* ориентирована только на малый бизнес, особенно на независимых подрядчиков. Компанией создана команда, которая обучает малые предприятия киберрискам и помогает восстановиться после инцидента. Основные услуги, предоставляемые страховой компанией, следующие:

– реакция на утечку информации: покрывает расходы на компьютерный анализ, уведомление и уход за пострадавшими, услуги по защите персональных данных и управление связями с общественностью;

– вымогательство: покрытие расходов при кибервымогательстве;

– восстановление информации: покрытие расходов на замену, восстановление информации или восстановление доступа к информации после киберинцидента;

– перерыв в производстве: покрытие убытков, связанных с полным или частичным прекращением бизнеса в результате кибератаки;

– киберпреступления и обман: покрытие любых денежных потерь в результате неправомерных действий третьих лиц или стратегий социальной инженерии, в рамках которых средства добровольно переводятся другим лицам.

Компания *Liberty Mutual* предлагает услугу страхования от кибератак, адаптированную для малого бизнеса. Деятельность направлена на защиту компаний от издержек, связанных с утечкой данных, атаками хакеров или нарушениями конфиденциальности. Дополнительным ресурсом, предлагаемым данной страховой компанией, является возможность доступа к платформе фильтрации данных, которая предоставляет уведомления о нарушении данных и инструменты для управления киберрисками. Ответственность компании разделена на четыре части:

– информация, подверженная риску: после компрометации конфиденциальной информации покрывает расходы на реагирование;

– вымогательство: покрытие расходов на восстановление информации и систем после утечки данных;

– ответственность перед третьими лицами: после компрометации данных третьих лиц покрытие юридических претензий;

– ответственность за безопасность сети: покрытие убытков третьих лиц, вызванных утечкой конфиденциальных бизнес-данных.

Политика компании *Travelers* направлена на защиту бизнес-деятельности организаций в различных сферах, независимо от их размера. Основной полис киберстрахования доступен как самостоятельный продукт или как часть пакета страхования бизнеса. Для малого бизнеса компания предлагает продукт под названием *Cyber First for Small Businesses*, который имеет доступную цену и включает в себя:

– уведомление клиентов о возникновении утечки информации;

– мониторинг кредитных карт;

– расходы на услуги консультанта по связям с общественностью;

– расходы на покрытие убытков в случаях предъявления иска третьими лицами.

Компания *CyberDot* предлагает эффективный и доступный полис киберстрахования с учетом потребностей каждой компании. Политика *CyberDot* включает в себя выбор покрытий при следующих инцидентах:

– перерыв в производстве;

– уничтожение цифровых активов;

– социальная инженерия и киберпреступность;

– кибервымогательство.

Владельцы малого бизнеса могут выбрать необходимый вариант покрытия и подходящие страховые премии, начиная с суммы 500 долл., при этом размер страховой суммы начинается с 1 млн долл., но может составить и 3 млн долл. в зависимости от компании. При этом *CyberDot* предоставляет обучение потенциальным рискам для организации-страхователя, чтобы повысить их уровень безопасности.

В России рынок страхования киберрисков только начинает развиваться. Существуют продукты отечественных страховых компаний, которые адаптированы под потребности малых организаций, но они представлены в комплексе с имущественным страхованием, а не обособленно. Основными поставщиками данных услуг для малого бизнеса в РФ являются представительства иностранных организаций, например, такие как *AIG* и *Chubb*.

Основным требованияем при подписании полисов киберстрахования является оценка текущего уровня информационной безопасности организации-страхователя. Отечественные компании испыты-

вают дефицит методической базы технического плана, которая бы позволила им сформировать соответствующий пакет услуг. В настоящее время в России пока не сформированы стандарты в области киберстрахования, не существует какой-либо единой модели, поэтому каждая страховая компания имеет свой индивидуальный подход. В национальном стандарте «Цифровая экономика Российской Федерации» предусмотрен ряд мер, направленных на популяризацию добровольного страхования рисков информационной безопасности и повышение киберкультуры. В апреле 2020 г. был выпущен документ, содержащий общие подходы российских страховщиков к страхованию информационных рисков – комплексному страхованию рисков в связи с кибератаками в отношении малого, среднего и крупного бизнеса, но требующий дальнейшего развития и прогресса в технической части обеспечения услуг страхования киберрисков.

За рубежом же данная область более развита. Так, в 2019 г. был опубликован новый международный стандарт, содержащий руководство по киберстрахованию – ISO/IEC 27102 «Information security management – Guidelines for cyber insurance» [3]. Несмотря на то что стандарт применим для предприятий всех размерностей, его трудно использовать при формировании продукта для страхования информационных рисков для малого предпринимательства, так как данное руководство основывается на системе менеджмента информационной безопасности (СМИБ), которое в большинстве случаев не реализовано в малых организациях в России. При формировании продуктов для малого бизнеса страховая компания должна учитывать размерность при определении ценовой составляющей, актуальности покрытия, формулировке предложений, а также при оценке уровня информационной безопасности. Процесс оценки информационной безопасности организации-страхователя может проводиться с привлечением сторонних экспертов в области информационной безопасности или же самостоятельно страховой компанией на основании заполненной страхователем анкеты. Формирование данной анкеты для страховых компаний представляет собой ряд трудностей, которые препятствуют созданию эффективного опросника, позволяющего с большой вероятностью определить состояние защищенности организации и принять решение о ее страхуемости. При этом важно понимать, что анкеты для малого бизнеса должны быть небольших размеров и содержать вопросы, понятные даже тем организациям, которые недостаточно развиты в сфере информационной безопасности. Развитию данного продукта может поспособствовать создание и внедрение законодательных норм и стандартов, которые бы содержали общие методологии по страхованию киберрисков, в том числе с учетом специфики малого предпринимательства.

Библиографический список

1. The Global Risks Report 2020. World Economic Forum. – URL: http://www3.weforum.org/docs/WEF_Global_Risk_ Report_2020.pdf
2. State of Cybersecurity in Small & Medium Size Businesses. Ponemon Institute. – URL: https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf
3. Стандарт ISO/IEC 27102–2019 [ISO/IEC 27102-2019] Information security management – Guidelines for cyber-insurance.

Образец цитирования:

Фатеев, А. Г. Предлагаемые продукты по киберстрахованию с учетом специфики малых предприятий / А. Г. Фатеев, С. С. Паршина // Инжиниринг и технологии. – 2020. – Vol. 5(2). – С. 1–4. – DOI 10.21685/2587-7704-2020-5-2-7.