УДК 336

**М.Н. Степанова**

# РОЛЬ СТРАХОВАНИЯ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В рамках обеспечения экономической безопасности страны особую актуальность приобретает такой ее элемент, как информационная безопасность. Рост числа совершаемых киберпреступлений и реализации иных видов киберрисков предопределяют необходимость развития страхования рисков информационной безопасности с учетом специфики их проявления, определяющей особенности создаваемого страхового покрытия. В предложенном материала представлено обоснование возрастающей роли страхования в обеспечении информационной безопасности как решения, формируемого в рамках предоставления страховых услуг на особом целевом сегменте.

*Ключевые слова:* киберстрахование, страхование информационной безопасности, тенденции страхового рынка, обеспечение информационной безопасности.

**M.N. Stepanova**

# THE ROLE OF INSURANCE IN ENSURING INFORMATION SECURITY

Within the framework of ensuring the economic security of the country, such an element as information security becomes particularly important. The increase in the number of cybercrimes committed and the implementation of other types of cyber risks predetermine the need for the development of information security risk insurance, taking into account the specifics of their manifestation, which determines the features of the insurance coverage being created. The proposed material provides a justification for the increasing role of insurance in ensuring information security as a solution formed within the framework of providing insurance services in a special target segment.

*Keywords:* cyber insurance, information security insurance, insurance market trends, information security assurance.

Процесс интеграции является мировой тенденцией XXI века. Кроме очевидных достоинств, связываемых с развитием IT-технологий, он предопределяет и появление серьезных проблем, к числу которых относят рост числа и вероятности рисков информационной безопасности, минимизация которых может рассматриваться в качестве одной из составляющих обеспечения экономической безопасности страны.

Специалистами отмечается, что «благодаря развитию современного общества, характеризующегося глобальными взаимосвязями между различными субъектами посредством информационных технологий, все больший масштаб приобретает киберпреступность» [1, с. 77], представляющая серьезную угрозу

национальной экономике и экономическим интересам ее агентов. Злоумышленники весьма активно эксплуатируют уязвимости сетевой инфраструктуры, выбирая объекты с максимальной концентрацией информации, содержащей персональные данные и ограниченными возможностями в построении надежной системы противодействия кибератакам (типы наиболее часто атакуемых отраслей представлены на рис. 1).

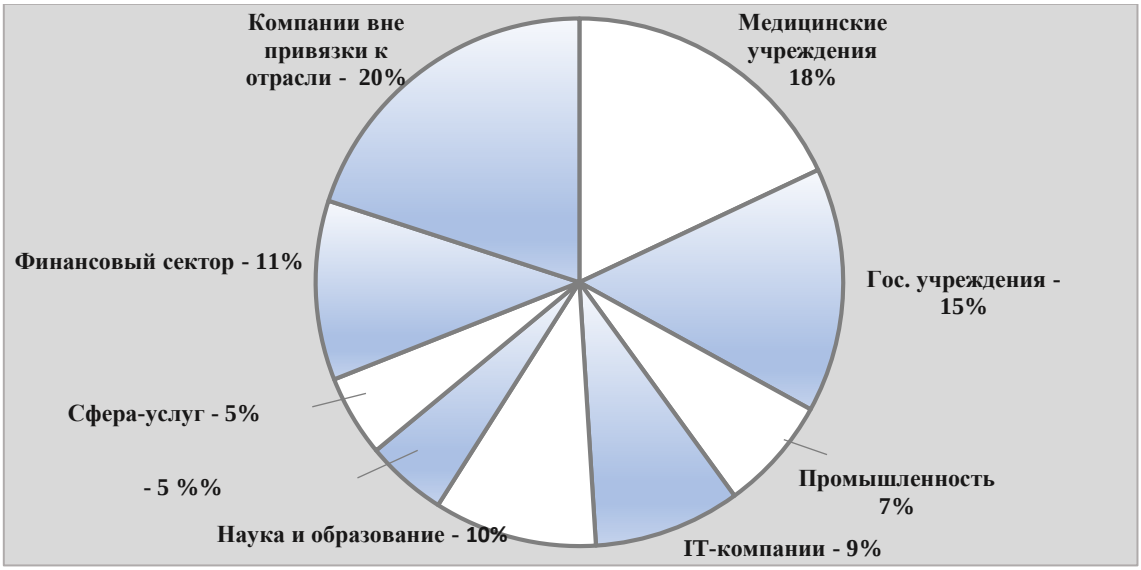


Рис. 1. Категории жертв киберпреступности среди организаций на мировом рынке в 2021 г. и их структура*

*Составлен по: [2]

Как видно, в настоящее время атакам в большей мере подвергаются медицинские и государственные учреждения, а также финансовый сектор, включая банки, инвестиционные и брокерские компании, платежные системы и т.п., в меньшей степени — промышленные предприятия, онлайн-сервисы и сфера услуг.

Существуют различные методы управления, теоретически предполагающие снижение вероятности киберрисков или убытков от их реализации: уклонение от рисков, их локализация, диверсификация, компенсация потерь. Однако, на практике они срабатывают не всегда, т. к. организационная структура киберпреступности имеет сложную архитектуру, достаточно часто уровнем выше, чем у крупных международных корпораций с отлаженными бизнес-процессами, работающую на опережение.

Одним из возможных финансовых инструментов защиты от негативных последствий кибератак является страхование, относящееся к методу уклонения от рисков наравне с отказом от рискованных и ненадежных проектов. Традиционные страховые полисы, как правило, исключают защиту на случай реализации киберрисков, что привело к оформлению страхования информационной безопасности в качестве отдельного направления страховой защиты, ориентированного на потребности компаний, осуществляющих цифровые финансовые операции

или хранящие персональные данные клиентов, включая медицинскую и финансовую информацию.

Страхование информационной безопасности переходит в класс методов управления информационными рисками, набирающих наибольшую популярность, но при этом еще недостаточно полно сформировавшихся теоретически и отлаженных практически. Достаточно обратить внимание на то, что наряду с сочетанием «страхованием информационных рисков» достаточно часто оперируют термином «киберстрахование», не вникая в суть возможных различий. В мировой практике они не только используются в качестве синонимичных, но и имеют еще несколько аналогов, среди которых наиболее распространение получили 1) страхование кибербезопасности (англ. cybersecurity insurance); 2) страхование киберответственности (англ. cyber liability insurance); 3) страхование информационной безопасности и конфиденциальности (англ. Information security and privacy insurance). Если за рубежом они легко взаимозаменяемы, то в российской практике можно встретить разные мнения насчет оснований для этого, хотя чаще все же преобладает посыл на то, что по сути «страхование информационных рисков» мало чем принципиальным отличается от «киберстрахования».

Стоит отметить, что термин «киберстрахование» появился относительно недавно и до настоящего времени одного, абсолютно конкретного определения ему не дано. Авторы представляют этот концепт многогранным и транслируют различные точки зрения на этот счет [3].

Один подход основан на том, что киберстрахование — это факультативное направление страхования, обеспечивающее финансовую возможность восстановления после крупных убытков, с помощью которого предприятия могут вернуться к нормальному функционированию, сохранению стабильности, платежеспособности и снижению потерь в результате перерыва в производстве, вызванного различными киберугрозами [4]. В условиях объективного отсутствия у структур IT-безопасности возможности обеспечить полную непроницаемость информационных систем, страхование киберрисков предлагают рассматривать как решение, формируемое в рамках страховых услуг наравне с другими составляющими ассортимента страхового рынка, ориентированное на компании с высокой долей компьютеризации и интерактивностью бизнеса [4]. В связи с этим киберстрахование представляют как готовый страховой продукт, направленный на защиту информационных рисков любых компаний, чей бизнес прямым или косвенным образом связан с обработкой и хранением данных [5].

Другой взгляд на киберстрахование основан на том, что это прежде всего составной элемент цифрового страхования. «Страховая защита от специфических рисков, свойственных цифровой экономике, представляет лишь первую часть цифрового страхования. Если раньше к цифровому страхованию относилось страхование электронных рисков (при аварии в электросетях и т.п.), рисков электронной коммерции, то в условиях цифровой экономики актуальность приобретают страхование киберрисков, страхование интернет-вещей (имущества физических и юридических лиц, управляемого через интернет), ответственность искусственного интеллекта перед третьими лицами и другие, еще скрытые цифровые риски», — отмечают исследователи [6, 7].

Определяя место киберстрахования в общей страховой системе, отметим, что регулятор относит его к ряду сегментов имущественного страхования, чаще — страхования имущества, реже — страхования ответственности юридических лиц и страхованию предпринимательских рисков.

Российская практика страхования ориентирована на минимизацию следующих видов рисков, влияющих на информационную безопасность субъектов (представлено на примере страховой компании «Ингосстрах»):

1. Риски гибели (уничтожения), утраты (пропажи), повреждения имущества либо иных объектов гражданских прав:

– нарушение безопасности, повлекшее утрату электронных данных и/или компьютерных программ, находящихся в собственности или законном владении/пользовании страхователя;

– нарушение безопасности, повлекшее хищение интеллектуальной собственности страхователя в электронной форме;

– нарушение безопасности, повлекшее неправомерное использование вычислительных ресурсов страхователя третьими лицами (как пример, это спам-рассылки, использование оборудования для генерации криптовалюты и другие);

– нарушение безопасности, сопровождающееся вымогательством в отношении страхователя (кибер-вымогательство);

– нарушение безопасности, повлекшее кражу застрахованного имущества, иного, чем денежные средства и акции;

– нарушение безопасности, повлекшее хищение денежных средств и акций в электронной форме со счета страхователя третьими лицами путем: неправомерного введения в его информационную систему электронных команд, подготовленных или модифицированных третьими лицами без ведома или согласия страхователя, а также в результате неправомерного перевода денежных средств со счета страхователя путем компрометации ключа его электронной подписи (электронной подписи лиц, имеющих право на распоряжение денежными средствами страхователя);

– нарушение безопасности, повлекшее гибель или повреждение застрахованного имущества в результате пожара, взрыва или поломки;

– ущерб деловой репутации страхователя вследствие событий.

2. Риски гражданской ответственности:

– наступление гражданской ответственности перед третьими лицами по компенсации морального вреда, причиненного в результате нарушения конфиденциальности, включая разглашение персональных данных;

– наступление гражданской ответственности перед третьими лицами в связи с причинением вреда жизни и здоровью третьих лиц в результате нарушения безопасности.

3. Риски убытков от перерыва в производстве:

– нарушение безопасности, повлекшее перерыв в коммерческой (производственной) деятельности страхователя из-за недоступности либо значительного снижения производительности;

– нарушений в работе информационной системы страхователя, полной или частичной недоступности электронных данных.

4. Риски возникновения расходов на информационную защиту.

Страхование распространяется на такие объекты гражданских прав, как компьютерное оборудование и программы, электронные базы данных (электронные данные); охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации; иное имущество и имущественные права по усмотрению сторон.

Киберстрахование предлагается многими из тех поставщиков, которые предоставляют сопутствующее страхование бизнеса, такое как страхование от ошибок и упущений, страхование ответственности бизнеса и страхование коммерческой собственности. Страховое покрытие может распространяться на расходы, связанные со сбоем в работе; платежами по причине запуска программ-вымогателей; восстановлением и дешифровкой данных, включая восстановление необходимого программного обеспечения, расследование киберпреступлений и восстановление деловой репутации.

Мировой опыт демонстрирует некоторые особенности формирования объема страхового покрытия. Так, большинство зарубежных страховщиков включают в договор «покрытие от первой стороны», применяемое к убыткам, которые непосредственно влияют на компанию или «покрытие от третьей стороны», которое применяется к убыткам, понесенным другими лицами в результате кибер-события или инцидента на основе их деловых отношений с этой компанией.

«Покрытие от первого лица» подразумевает, что бизнес определенной компании подвергается кибератаке, например, атаке программ-вымогателей или утечке данных, и рассматривается конкретно с ее стороны. Данное покрытие может включать: расходы на адвоката для определения обязательств по уведомлению и нормативным актам; восстановление и замену утерянных или украденных данных; услуги по уведомлению клиентов; потерянный доход из-за перерывов в деятельности; антикризисное управление и связи с общественностью; кибервымогательство и мошенничество; судебные расходы для расследования нарушения; сборы, штрафы и штрафы, связанные с кибератакой.

«Покрытие от третьей стороны» обычно защищает компанию от ответственности в отношении третьих лиц, то есть распространяется на судебные иски и штрафы за нарушения правил обработки данных, предъявляемых определенной компании. Страховщик в первую очередь ориентирован на покрытие расходов, связанных с соответствующим судебным процессом. Такое страховое покрытия включает: выплаты потребителям, пострадавшим от нарушения; претензии и расходы по урегулированию, связанные со спорами или судебными исками; убытки, связанные с диффамацией и нарушением авторских прав или товарных знаков; расходы на судебные разбирательства; другие убытки и расходы, связанные с судебными решениями.

Объем затрат на страховое обеспечение может зависеть от нескольких составляющих, включая количество ранее совершенных атак, наличие антивирусных программ и других подобных средств защиты, результат оценки стоимости застрахованного объекта.

В Соединенных Штатах, как и частично в Европейский странах, большинство крупных страховых компаний предлагают клиентам различные возможные

варианты обеспечения кибербезопасности посредством страхования. В зависимости от цены и типа полиса клиент может рассчитывать на покрытие дополнительных расходов, возникающих в результате физического уничтожения или кражи активов информационных технологий. Такие расходы обычно включают расходы, связанные с удовлетворением требований о вымогательстве в результате атаки программ-вымогателей; уведомлением клиентов о нарушении безопасности; оплатой судебных издержек, взимаемых в результате нарушения конфиденциальности; наймом экспертов по компьютерной криминалистике для восстановления скомпрометированных данных; восстановлением идентификационных данных клиентов, чьи персональные данные были скомпрометированы; восстановлением измененных или украденных данных; ремонтом или заменой поврежденных или скомпрометированных компьютерных систем.

Некоторые полисы киберстрахования покрывают расходы на предоставление услуг кредитного мониторинга клиентам, пострадавшим от утечки данных. В сентябре 2018 года Equifax, агентство по отчетности о потребительских кредитах, подверглось утечке данных, в результате которой была раскрыта личная информация 147 миллионов человек. В 2019 году Equifax достигла соглашения с Федеральной торговой комиссией США (ФТС). В рамках соглашения Equifax согласилась потратить 425 миллионов долларов на предоставление бесплатной кредитной отчетности, выплаты наличными — например, для тех, кто уже зарегистрирован в службе кредитного мониторинга, — возмещение времени или денег, потраченных на восстановление после кражи личных данных, и бесплатные услуги по восстановлению личных данных. Полис киберстрахования мог бы покрыть часть расходов Equifax на урегулирование в размере 425 миллионов долларов, предполагая, что обстоятельства утечки его данных были покрыты таким полисом.

Многие политики кибербезопасности исключают предотвратимые проблемы безопасности, вызванные людьми, такие как плохое управление конфигурацией или небрежное обращение с цифровыми активами. В данном случае, страховое покрытие будет исключать:

– ранее существовавшие или предшествовавшие нарушения, или кибератаки, такие как инциденты, произошедшие до приобретения полиса;

– киберсобытия, инициированные и вызванные сотрудниками или инсайдерами;

– сбои в инфраструктуре, не вызванные целенаправленной кибератакой;

– неспособность исправить известную уязвимость, например, компания, которая знает о существовании уязвимости, не может устранить ее и затем подвергается риску из-за этой уязвимости;

– потеря стоимости, вызванная кражей интеллектуальной собственности у вашей компании;

– потенциальная упущенная выгода в будущем;

– затраты на улучшение технологических систем, включая усиление безопасности в системах или приложениях.

Российская практика выработала следующие специфические исключения, ограничивающие страховое покрытие: использование нелицензионного программного обеспечения; неспособность информационной системы справиться с запросами; повторные убытки из-за невыполнения страхователем обязанности незамедлительно блокировать и/или отменить сертификат электронной подписи или неустранением последствий при возможности их устранения самим страхователем.

Для осознания растущей важности киберстрахования, ниже представлены следующие данные отчета HISCOX за 2021 год и опроса LUCY, проведенного Ассоциацией управления рисками и страховыми компаниями [9]:

– средний бюджет IT — компаний, выделенный на киберпреступность в 2021 году составил 21 %, при этом за один год эта доля увеличилась на 63 %, но и этого еще недостаточно, чтобы ограничить влияние киберрисков;

– 28 % компаний стали жертвами кибератак более пяти раз, 47 % очень крупных компаний подверглись ударам веб-хакеров шесть или более раз, 33 % из них подверглись более чем 25 атакам в год;

– 71 % специалистов в области IT-безопасности отметили рост угроз и атак с начала кризиса в области здравоохранения;

– 71 % программ-вымогателей запускается в нерабочее время;

– 80 % компаний фактически «кладет ключ под дверь»;

– прирост количества вирусов-вымогателей в течение одного года составляет 255 % (CNIL подтвердила эту тенденцию, указав, что вымогательство попрежнему является наиболее распространенной атакой и достигло рекордных показателей в 2020 году);

– средний показатель заявок на выкуп, выявленных в 2020 году, составил 100 тыс. долларов, при том, что в 2019 году он был на уровне 10 тыс. долларов.

Таким образом, проведенное исследование позволило прийти к выводу о том, что киберстрахование — это особое направление страховой защиты, используемое с целью осуществления минимизации рисков информационной безопасности. Можно отметить, что теоретическая база киберстрахования еще не сформирована должным образом, но растущая опасность киберпреступности и значимость минимизации ее последствий являются хорошей мотивацией развития теории киберстрахования, определяя необходимость более точной детализации его содержания и области применения. Что касается практики его реализации, то она во-многом будет предопределяться не только спецификой формирования российской страховой среды, но и ее общемировыми тенденциями [10], мало зависящими от происходящих геополитических изменений.

## Список использованной литературы

1. Мамаева Л.Н. Кибер-страхование как способ обеспечения информационной безопасности / Л.Н. Мамаева, В.И. Ларионов // Экономическая безопасность и качество. — 2018. — № 1 (30). — С. 76–79. — EDN YVESYV.

2. Киберстрахование: как обеспечить информационную безопасность бизнесу. — 2019. — URL: https://www.business.ru. (дата обращения: 05.04.2022).

3. Степанова М.Н. Генезис российской практики киберстрахования / М.Н. Степанова, М.Н. Юсупова // Журнал прикладных исследований. — 2021. — Т. 9, № 6. — С. 874–881.

4. Кулюкина И.С. Страхование киберрисков / И.С. Кулюкина // Проблемы и перспективы развития кооперации и интеграции в современной экономике : сб. ст. Междунар. науч.-практ. конф., Саратов, 14–15 марта 2019 г. — Саратов : Центр соц. агроинноваций СГАУ, 2019. — С. 107–115. — EDN WBEAJP.

5. Игнатова И.О. Киберстрахование как современный способ обеспечения информационной безопасности в эпоху технологий: российский и зарубежный опыт / И.О. Игнатова // Страховое право. — 2021. — № 1 (90). — С. 45–47. — EDN ULGMOD.

6. Просветова А.А. Особенности цифровизации страхового рынка в России / А.А. Просветова, Е.В. Жегалова // Экономика и предпринимательство. — 2020. — № 9 (122). — С. 230–232. — DOI 10.34925/EIP.2020.122.9.045. — EDN ZWXUOX.

7. Брызгалов Д.Н. Страхование электронных рисков / Д. Н. Брызгалов, А.А. Цыганов // Директор-Инфо. — 2002. — № 47. — С. 35–41.

8. Правила страхования информационных рисков. Страховая компания // Ингосстрах : офиц. сайт. — URL: https://www.ingos.ru/Upload/2019/insurance-rules/kb/pravila_info_riskov.pdf (дата обращения: 01.08.2022).

9. Спрос на киберстрахование // Calmins. — URL: https://calmins.com/v-rossii-znachitelno-vyros-spros-na-kiberstrahovanie (дата обращения: 20.04.2022).

10. Степанова М.Н. Анализ ключевых характеристик современного мирового рынка киберстрахования / М.Н. Степанова, М.Н. Юсупова // Журнал прикладных исследований. — 2022. — № 1-1. — С. 54–61. — DOI 10.47576/2712-7516_2022_1_1_54. — EDN WUMBTN.

## Информация об авторе

*Степанова Марина Николаевна* — кандидат экономических наук, доцент, кафедра финансов и финансовых институтов, Институт управления и финансов, Байкальский государственный университет, г. Иркутск, Российская Федерация, e-mail: StepanovaMN@bgu.ru.

## Author

*Marina N. Stepanova* — PhD in Economics, art. Lecturer of finance and financial institutions, Baikal State University, Irkutsk, the Russian Federation, e-mail: StepanovaMN@bgu.ru.