МРНТИ 06.01
УДК 330
DOI 10.58319/26170493_2023_3_16

ОБЕСПЕЧЕНИЕ КАЧЕСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПОПОВА Л. В.[1]
доктор экономических наук
[1]Орловский государственный университет имени И.С. Тургенева, г. Орёл, Российская Федерация

АННОТАЦИЯ. С увеличением объема цифровых данных и переходом многих бизнес-процессов в онлайн-формат, угрозы информационной безопасности становятся все более серьезными. Хакерами они доведены практически до совершенства. В условиях растущей веб-угрозы и повышенного внимания к кибербезопасности руководство организаций более серьезно стало заниматься вопросами защиты цифровых устройств и информации. Важным элементом комплексной стратегии гарантии безопасности выступает сегодня киберстрахование.В работе сделан вывод, что, несмотря на то, что страхование от цифровых рисков является относительно новым явлением, оно представляет собой довольно перспективное направление в области страховой защиты, имея большой потенциал в будущем. В статье раскрываются основные преимущества киберстрахования, включая защиту от убытков, связанных с киберинцидентом, помощь в восстановлении информации после кибератак, возмещение расходов, предотвращение будущих атак, поддержка в случае нарушения целостности данных, а также снижение риска финансовых потерь. Автором проводится анализ цифровых атак, их воздействия на сферу киберстрахования с учетом ведущих участников, исследуется текущее положение киберстрахования, выделяются основные направления развития, глобальные тенденции. Особое внимание в работе уделяется прогнозированию будущих киберугроз, разработке стратегий защиты, применимости их для компаний всех отраслей экономики и размеров бизнеса.

КЛЮЧЕВЫЕ СЛОВА: киберстрахование, прогнозирование, цифровизация, киберпреступность, информационные системы, информационная безопасность.

АҚПАРАТ ҚАУІПСІЗДІГІН САПАСЫН ҚАМТАМАСЫЗ ЕТУ

ПОПОВА Л. В.[1]
экономика ғылымдарының докторы
[1]И.С. Тургенев атындағы Орлов мемлекеттік университеті, Орел қ., Ресей Федерациясы

АҢДАПТА. Цифрлық деректер көлемінің ұлғаюымен және көптеген бизнес-процестердің онлайн форматқа көшуімен ақпараттық қауіпсіздікке қауіп төндіруде. Хакерлер оларды дерлік кемелдікке жеткізді. Веб-қауіптің артуы және киберқауіпсіздікке назардың артуы жағдайында ұйымдық көшбасшылық цифрлық құрылғылар мен ақпаратты қорғауға көбірек мән берді. Бүгінгі күні киберсақтандыру қауіпсіздікті қамтамасыз етудің кешенді стратегиясының

маңызды элементі болып табылады, бұл жұмыс цифрлық тәуекелдерден сақтандыру салыстырмалы түрде жаңа құбылыс болғанына қарамастан, ол үлкен әлеуетке ие сақтандыруды қорғау саласындағы жеткілікті перспективалы бағыт болып табылады деген қорытындыға келеді. болашақта. Мақалада киберсақтандырудың негізгі артықшылықтары, соның ішінде киберинцидентке байланысты шығындардан қорғау, кибершабуылдардан кейін ақпаратты қалпына келтіруге көмектесу, шығындарды өтеу, болашақ шабуылдардың алдын алу, деректер бұзылған жағдайда қолдау көрсету және сақтандыру жағдайларын азайту қарастырылған. қаржылық шығындар тәуекелі. Автор жетекші қатысушыларды ескере отырып, цифрлық шабуылдарды, олардың киберсақтандыру саласына әсерін талдайды, киберсақтандырудың ағымдағы жағдайын қарастырады, дамудың негізгі бағыттары мен жаһандық трендтерді көрсетеді. Болашақ киберқауіптерді болжауға, қорғау стратегияларын әзірлеуге және олардың барлық экономикалық секторлар мен бизнес көлемдеріндегі компанияларға қолданылуына ерекше көңіл бөлінеді.

ТҮЙІН СӨЗДЕР: киберсақтандыру, болжау, цифрландыру, киберқылмыс, ақпараттық жүйелер, ақпараттық қауіпсіздік.

QUALITY ASSURANCE OF INFORMATION SECURITY

POPOVA L. V.[1]
Doctor of Economic Sciences
[1]Orel State University named after I.S. Turgenev, Orel, Russian Federation

ABSTRACT. As the volume of digital data increases and many business processes move online, information security threats are becoming increasingly serious. Hackers have perfected them to near perfection. With the growing web threat and increased focus on cybersecurity, organizational leaders have become more serious about protecting digital devices and information. Cyber insurance is an important element of a comprehensive security guarantee strategy.The paper concludes that, despite the fact that insurance against digital risks is a relatively new phenomenon, it represents a rather promising direction in the field of insurance protection, with great potential in the future. The article reveals the main benefits of cyber insurance, including protection against losses associated with a cyber incident, assistance in recovering information after cyber attacks, reimbursement of expenses, prevention of future attacks, support in the event of a data breach, as well as reducing the risk of financial losses. The author analyzes digital attacks, their impact on the sphere of cyber insurance, taking into account the leading participants, examines the current situation of cyber insurance, highlights the main directions of development, global trends. Special attention in the work is paid to forecasting future cyber threats, development of defense strategies, their applicability for companies of all industries and business sizes.

KEYWORDS: cyber insurance, forecasting, digitalization, cybercrime, information systems, information security.

ВВЕДЕНИЕ. В современном мире, глубоко проникшем в эру цифровизации, где каждая сфера жизни и профессиональной деятельности охвачена виртуальными технологиями, крайне важно уделять внимание информационной безопасности и применять разнообразные стратегии для снижения рисков возникновения кибератак. Как счи-

тает А.Д. Назарова цифровые угрозы непрерывно развиваются, изменяются, становятся более изощренными. Злоумышленники разрабатывают новые методы атак на критические системы, делая предвидение всех потенциальных угроз затруднительным [1, с. 2214]. Хотя в большинстве случаев уязвимости в работе появляются из-за человеческого фактора, например, из-за неосознанных или преднамеренных действий сотрудников при использовании информационно-технологической инфраструктуры, ошибочной настройки программного обеспечения. Некоторые компании имеют ограниченные ресурсы в виде передового оборудования, лицензионного программного и аппаратного обеспечения, квалифицированных специалистов в данной сфере, обладающих способностью во время выявлять, предотвращать возникающие происшествия, что делает их более уязвимыми перед современными угрозами, даже при наличии правильно подобранных стратегий. Так, существует огромное количество неизвестных факторов, переменных, способных повлиять на кибербезопасность организаций. По мнению С. Ф. Фейзиевой даже изменения в законодательстве, постоянное обновление программного обеспечения, внедрение новых технологий, обучение цифровой грамотности сотрудников, других мер оказывается недостаточным дабы оказать защиту от цифровых угроз в полной мере. В реальности никто не застрахован от возможности столкнуться с киберинцидентом, исключить полностью возможность атаки невозможно [2, с. 813]. Всегда найдутся те, кто способен преодолеть самые надежные системы защиты.

Киберпространство является эпицентром не только стандартных хакерских атак, но и более сложных, искусных способов воздействия, какие уже не являются абстрактными, становятся конкретными проблемами, с которыми сталкиваются как крупные компании, так и физические лица. Последствия атак простираются далеко за пределы прямых затрат на восстановление оборудования, включая в себя непрямые риски, такие как временные простои в доступе к сервисам, выплаты компенсаций клиентам, расходы на проведение расследований инцидентов, репутационные угрозы. Эксперты прогнозируют, что киберпреступность будет продолжать развиваться, используя усовершенствованные подходы, техники обмана, которые продолжат оказывать серьезное влияние на повседневную жизнь, рабочие процессы (рис. 1) [3, с. 17].

Специалисты Е.А. Антонян, Е.Н. Клещина делают вывод, что одним из ключевых моментов прогнозирования киберпреступлений является не столько ответ на уже известные угрозы, сколько антиципация потенциальных тенденций развития киберпреступности в будущем [4, с. 14]. В таких ситуациях разумно обратить внимание на страхование рисков, т.е. приобретение страхового полиса на случай, если инцидент все-таки произойдет. Киберстрахование – это вид страхования, который помогает организациям свести к минимуму потери и издержки, связанные с цифровыми угрозами, чтобы обеспечить оперативную реакцию на инциденты безопасности, предоставляя компаниям комплексную защиту. В отличие от стандартных видов страхования, таких как страхование имущества или медицинское страхование, киберстрахование обеспечивает защиту от онлайн-угроз, связанных с кибербезопасностью: вирусы, вредоносное программное обеспечение, фишинговые атаки, утечки информации, атаки DDoS, программы-вымогатели, мошенничество, а также другие виды киберпреступлений. Процесс киберстрахования начинается с оценки рисков, где страховая компания проводит анализ данных о защищенности экономического субъекта для определения уровня уязвимости, возможных опасностей. На основании полученной информации страхов-

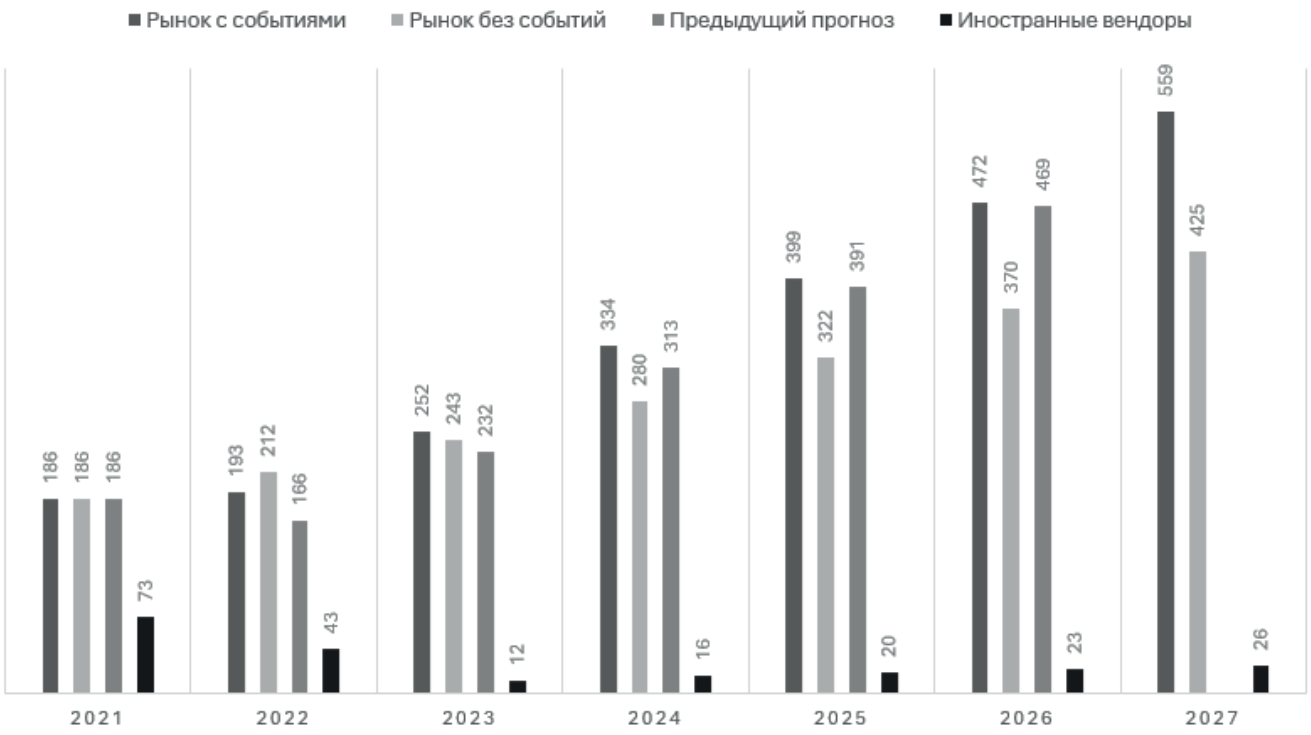

Рисунок 1 – Прогноз развития рынка кибербезопасности России

щик определяет стоимость полиса, дает заключение. Затем следует этап оформления, на котором заключается договоренность о цене и условиях страхования, составляется документ, в котором прописываются правила, условия. После оформления страховки, страховая компания может предложить рекомендации по улучшению кибербезопасности клиента, в последующем оказывать консультационную поддержку в данной области. В случае возникновения киберинцидента страховщик предоставляет компенсацию за ущерб, понесенный компанией в результате атаки. Страховая компания не только выплачивает возмещение по страховому случаю, позволяя компании снизить затраты по восстановлению после инцидента, но и берет на себя дополнительные услуги, такие как консультации специалистов по кибербезопасности, помощь в расследовании инцидента, восстановлении данных, систем [5, с. 875].

МАТЕРИАЛЫ И МЕТОДЫ ИССЛЕДОВАНИЯ. Киберстрахование обычно индивидуализируется под нужды каждой конкретной компании, учитывая ее специфику, особенности бизнеса, риск-профиль, что дает возможность выбирать наиболее подходящие виды защиты и оказываемых услуг.

Поскольку киберугрозы постоянно эволюционируют, и рынок киберстрахования также меняется с течением времени. Решение о том, нужно ли компании киберстрахование, зависит от ряда факторов, включая размер, тип бизнеса, наличие ценных данных, степень взаимодействия с интернетом, информационными системами, уровень необходимой киберзащиты. Для того, чтобы принять правильное решение, следует обратить внимание на несколько основных признаков, которые могут указывать на необходимость применения страхования. Во-первых, если организация хранит и обрабатывает конфиденциальную информацию, такую как личные данные клиентов, финансовые сведения, интеллектуальную собственность. Во-вторых, если организация зависит от информационных технологий, онлайн-платформ для своей деятельности. В-третьих, если организация не имеет достаточного уровня кибер-

Рисунок 2 – Результат опроса, показывающий какие организации применяют практику киберстрахования в 2022 году

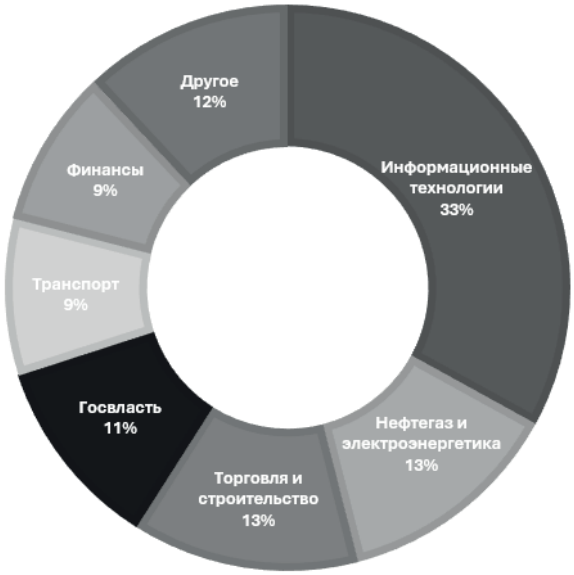

Рисунок 3 – Результат опроса, показывающий сколько организаций планируют внедрить киберстрахование

защиты или не в состоянии самостоятельно обеспечить надежную защиту своих данных и информационных систем. Соответствуя хотя бы одному из перечисленных критериев, с большой степенью вероятности, стоит обратить внимание на продукт цифрового страхования.

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ. Как заключают В.И. Андрейкович, А.Е. Железнюк, О.Л. Конюкова цифровое страхование полезно для физических и юридических лиц, но сфера его применения и цели все-таки отличаются [6, с. 7]. В современных реалиях киберстрахование целесообразнее для организаций, которые хотят защитить себя от потенциальных угроз безопасности в цифровой эпохе. Актуальные исследования показывают, что страховые компании все чаще включают в свои предложения услуги по консультированию, поддержке в случае киберсобытий.

По результатам опроса, полученным «РТК-Солар» в 2022 году, лишь небольшой процент компаний – около 6%, воспользовались страхованием от киберугроз [7, с. 6]. Заметно, что большинство из этих организаций относится к сферам финансов и информационных технологий, являющихся наиболее авангардными в плане цифровизации. Это объяснимо, поскольку такие предприятия обладают достаточными средствами не только для разработки систем информационной безопасности, но и для их финансовой поддержки через страхование. В то же время, страхование киберрисков также привлекает внимание руководства компаний в более традиционных секторах экономики. Примером тому служит нефтегазовая и электроэнергетическая отрасли, а также государственные структуры, на которые приходится 16% компаний, страхующих свои цифровые риски (рис. 2).

В России наибольший интерес к комплексному страхованию киберрисков пока проявляют крупные финансовые организации, для которых обрыв работы даже небольших частей сети может вызвать приостановку бизнес-операций. При этом, те, кто воспользовался таким видом страхования, отмечают, что данная услуга позволила им намного

быстрее оправиться после инцидента, а две трети убеждены, что внедрение страхования повысило привлекательность компании для клиентов, сотрудников, партнеров. Вопреки скептицизму остальных участников рынка, пренебрегать постоянно увеличивающимся количеством цифровых атак с каждым годом становится все проблематичнее. Потому, в перспективе, количество планирующих внедрить киберстрахование в рабочие процессы составляет 21%. И все же, структура распределения показывает, что преобладает область компаний информационных технологий – 33%, в то время как представители экономического сектора несколько запаздывают – только 9% из них планируют заниматься страхованием киберрисков (рис. 3).

Однако при подготовке к заключению соответствующих договоров, страховые компании, зачастую, сталкиваются с множеством препятствий. Часть из них отмечают отсутствие готовности у компаний предоставить доступ к своей инфраструктуре для оценки, что является необходимым условием для приобретения полиса. Другие указывают на ограниченные возможности рынка страхования киберрисков. Со стороны некоторых компаний, это выражается в неспособности позволить услугу из-за высокой стоимости, некоторой доли сомнений. Продукт киберстрахования, является сравнительно новым на рынке, существует лишь ограниченное количество проверенных решений. В связи с чем не все осознают выгоды, воспринимая страхование как ненужные расходы или инвестиции без возврата, не понимая принципов его работы, что обусловлено вариативностью условий страховых полисов, отличающихся в зависимости от специфических потребностей каждой компании. Как бы то ни было, ассортимент продуктов предлагает как решения, покрывающие все возможные цифровые угрозы, так и специализированные страховки. В каждом договоре индивидуально прописываются детали, но при этом имеются исключения, не подпадающие под страховое покрытие.

С.В. Афанасьева, Е.С. Черепанова, Н.В. Шехова считают, что киберстрахование не должно восприниматься как исключительное средство защиты от цифровых рисков [8, с. 14]. Страховой полис в области информационной безопасности в первую очередь разработан для того, чтобы обеспечить финансовую защиту и возместить убытки, понесенные в результате киберинцидентов. Такой подход обусловлен тем, что страховые компании сосредоточены на перераспределении финансовых последствий, а не на управлении самими рисками. Предоставление интегрированных решений по кибербезопасности выходит за рамки специализации страховщика, требуя других компетенций, ресурсов. Страховка помогает компенсировать финансовые потери после атак, но она не способна в полной мере исправить уязвимости в информационных системах, которые часто являются целью для хакеров. В этой связи компаниям необходимо дополнительно инвестировать в меры по повышению уровня защиты своих информационных систем, чтобы снизить вероятность киберугроз, а также потерь, которые могут последовать за ними. Потому, киберстрахование служит важным дополнением к общему плану киберзащиты, но не её заменой.

Все чаще компании различных отраслей, включая крупный и средний бизнес, решают страховать риски, связанные с электронными и компьютерными преступлениями, в рамках общих корпоративных страховых договоров, а не заключать специализированные страховые полисы. Организации выбирают вариант интегрирования страхования киберрисков в договоры банковского страхования, что делает управление более простым. Такой подход позволяет охватить широкий спектр традиционных рисков, характерных для особенностей деятельности конкретной отрасли, исключая потреб-

ность в заключении отдельных документов на каждый вид риска. Помимо упрощения управления, возникают экономические преимущества, поскольку общие договоры страхования зачастую привлекательнее по условиям, стоимости по сравнению со специализированными полисами на страхование киберрисков. Интеграция страхования от цифровых угроз в общие полисы способствует всеобъемлющему решению в управлении рисками, обеспечивая более глубокое покрытие. Сложности с оценкой киберрисков, обусловленные их постоянно изменяющимся характером, также делают интеграцию киберрисков в общие полисы предпочтительной, минимизируя трудности с идентификацией, оценкой потенциальных угроз, упрощая процесс страхования. Кроме того, наблюдается относительно невысокий уровень развития рынка специализированного страхования киберрисков, предлагающий ограниченные варианты покрытия или довольно высокие страховые ставки, стимулируя организации включать угрозы в уже существующие корпоративные страховые договоры.

Несмотря на выбор многих организаций включить страхование киберрисков в общие договоры банковского страхования, необходимость киберстрахования остается актуальной как никогда, являясь ценным инструментом для укрепления устойчивости бизнеса в цифровую эпоху. К тому же, Центральный банк России отмечает постепенное развитие рынка страхования киберрисков с каждым годом. Согласно отчету Банка России глобальный рынок страхования киберрисков планирует вырасти к 2025 году до 20 млрд долларов США [9, с. 22]. Регулятор стремиться создать условия для формирования института страхования цифровых угроз и предоставить дополнительные данные внешним пользователям для разработки страховых моделей. Главной целью страхования киберрисков останется покрытие убытков, возникших в результате успешно реализованных кибератак.

В действительности, полная картина и реальное понимание ситуации в области киберугроз затруднительны, поскольку практически отсутствует доступность статистических данных о происшествиях. По мнению Л.Г. Шобей, М.П. Семченко возможность получить широкий обзор, объективное представление о ситуации осложняется из-за ограниченного доступа к соответствующей информации [10, с. 188]. Одни компании предпочитают не публиковать информацию об инцидентах кибербезопасности из-за опасений по поводу возможного разрушения репутации, потери доверия со стороны клиентов и прочего. Ведь открытое разглашение информации о киберинцидентах способно дополнительно ухудшить ситуацию, повысив уровень рисков. Другие организации могут не осознавать важность сбора, анализа данных о случившихся атаках или просто не видят выгоды в добровольном афишировании сведений о случившемся, оставляя эту информацию на внутреннем уровне. Все это приводит к отсутствию ключевой информации для специалистов, страховщиков.

Однако, с появлением каждого нового цифрового преступления возрастает и осознание опасностей. Эта тенденция будет продолжаться и в будущем. В перспективе, страховые компании продолжат активно расширять свои продуктовые линии киберстрахования, разрабатывая новые продукты, адаптированные к современным угрозам в цифровой среде, которые позволят быть гибкими, во время реагировать на появляющиеся вызовы в области информационной безопасности. Поскольку разработка всеобъемлющей стратегии кибербезопасности и её непрерывное улучшение становятся неотъемлемыми элементами успешной защиты от современных цифровых угроз.

ЗАКЛЮЧЕНИЕ. Таким образом, в совре-

менном мире киберстрахование стало неотъемлемой частью безопасности для компаний в различных областях деятельности, не только для тех, кто прямо связан с информационными технологиями. Даже в сферах, где использование цифровых инструментов не является первостепенной задачей, защита от киберугроз приобретает значимость. От промышленного производства до сферы торговли, цифровые решения находят свое применение. Потому необходимо незамедлительно обеспечить надежную защиту ценной информации во всех областях бизнеса. Стоит понимать, что киберинциденты способны произойти в любой момент, поэтому необходимо быть готовым к оперативной реакции на них. Осознание цифровых рисков и умение эффективно реагировать на цифровые атаки – это основа успешной кибербезопасности.

СПИСОК ЛИТЕРАТУРЫ:

1. Назарова, А. Д. Вызовы и решения в области кибербезопасности в эпоху цифровой трансформации / А. Д. Назарова. – Текст : непосредственный / Лучшая научная работа 2023 // Сборник статей IX Международного научно-исследовательского конкурса. – 2023.– С. 19-21.

2. Фейзиева, С. Ф. Угрозы информационной безопасности в сети Интернет: современные вызовы / С. Ф. Фейзиева. – Текст : непосредственный // XXI Международная конференция памяти профессора Л. Н. Когана «Культура, личность, общество в современном мире: методология, опыт эмпирического исследования». – 2018. – С. 809-814.

3. Прогноз развития рынка кибербезопасности в Российской Федерации на 2023-2027 годы [Электронный ресурс]. - Центр стратегических разработок. - URL: https://www.csr.ru/ru/research/prognoz-razvitiya-rynka-kiberbezopasnosti-v-rossiyskoy-federatsii-na-2023-2027-gody/ (дата обращения: 10.03.2024)

4. Антонян, Е. А. Киберпреступность на современном этапе: тенденции и направления противодействия / Е. А. Антонян, Е. Н. Клещина. – Текст : непосредственный // Вестник экономической безопасности. – 2022. – № 5. – С. 11-15.

5. Степанова, М. Н. Генезис Российской практики киберстрахования / М. Н. Степанова, М. Н. Юсупова. – Текст : непосредственный // Журнал прикладных исследований. – 2021. – № 6-9. – С. 974-881.

6. Андрейковец, В. И. Тенденции киберстрахования в Российской Федерации / В. И. Андрейкович, А. Е. Железнюк, О. Л. Конюкова. – Текст : непосредственный // Вектор экономики. – 2023. – № 11 (89). – С. 2-13.

7. Тренды страхования киберрисков на российском рынке [Электронный ресурс]. - РТК Солар - URL: https://rt-solar.ru/?utm_source=yandex&utm_medium=cpc&utm_campaign=Brand_search_rf&utm_content (дата обращения: 10.03.2024)

8. Афанасьева, С. В. Инновационные методы предотвращения киберугроз в целях обеспечения экономической безопасности организации / С. В. Афанасьева, Е. С. Черепанова, Н. В. Шехова. – Текст : непосредственный // Вестник Самарского университета. Экономика и управление. – 2023. – № 2 (14). – С. 7-16.

9. Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2023-2025 годов [Электронный ресурс]. - Банк России. - URL: https://cbr.ru/press/event/?id=15840 (дата обращения: 10.03.2024)

10. Шобей, Л. Г. Цифровизация страхового рынка России: состояние, проблемы и перспективы / Л. Г. Шобей, М. П. Семченко. – Текст : непосредственный // Региональные проблемы преобразования экономики. – 2021. – 6 (128). – С. 184-192.

REFERENCES:

1. Nazarova, A. D. (2023). Challenges and solutions in the field of cybersecurity in the era of digital transformation. *Sbornik statej IX Mezhdunarodnogo nauchno-issledovatel'skogo konkursa – Collection of articles of the IX International Scientific Research Competition*, 19-21 [In Russian].

2. Feyzieva, S. F. (2018). Threats to information security on the Internet: modern challenges. XXI Mezhdunarodnaja konferencija pamjati professora L. N. Kogana «Kul'tura, lichnost', obshhes*tvo v sovremennom mire: metodologija, opyt jempiricheskogo issledovanija – XXI International Conference in Memory of Professor L. N. Kogan «Culture, personality, society in the modern world: methodology, empirical research experience»*, 809-814 [In Russian].

3. Center for Strategic Research. *Forecast of cybersecurity market development in the Russian Federation for 2023-2027*. https://www.csr.ru/ru/research/prognoz-razvitiya-rynka-kiberbezopasnosti-v-rossiyskoy-federatsii-na-2023-2027-gody/

4. Antonyan, E. A. & Kleshchina, E. N. (2022). Cybercrime at the present stage: trends and directions of counteraction. *Vestnik jekonomicheskoj bezopasnosti – Bulletin of Economic Security, 5*, 11-15 [In Russian].

5. Stepanova, M. N. & Yusupova, M. N. (2021). The genesis of Russian cyber insurance practice. *Zhurnal prikladnyh issledovanij – Journal of Applied Research, 6*-9, 974-881 [In Russian].

6. Andreykovets, V. I., Zheleznyuk ,A. E. & Konyukova, O. L. (2023). Trends in cyber insurance in the Russian Federation. *Vektor jekonomiki – The vector of the economy, 11* (89) [In Russian].

7. RTK-Solar. *Cyber Risk Insurance Trends in the Russian*. https://rt-solar.ru/?utm_source=yandex&utm_medium=cpc&utm_campaign=Brand_search_rf&utm_content

8. Afanasyeva, S. V., Cherepanova, E. S. & Shekhova, N. V. (2023). Innovative methods of preventing cyber threats to ensure the economic security of the organization. *Vestnik Samarskogo universiteta. Jekonomika i upravlenie – Bulletin of Samara University. Economics and Management, 2* (14), 7-16 [In Russian].

9. Bank of Russia. *Main directions for the development of information security in the credit and financial sector for the period 2023-2025.* https://cbr.ru/press/event/?id=15840

10. Shobey, L. G. & Semchenko, M. P. (2021). Digitalization of the insurance market in Russia: status, problems and prospects. *Regional'nye problemy preobrazovanija jekonomiki – Regional problems of economic transformation, 6* (128), 184-192 [In Russian].

СВЕДЕНИЯ ОБ АВТОРАХ:

Попова Людмила Владимировна - доктор экономических наук, заведующий кафедрой экономики, финансов и бухгалтерского учета, Орловский государственный университет имени И.С. Тургенева, г. Орёл, Российская Федерация
E-mail: lvp_134@mail.ru

Попова Людмила Владимировна - экономика ғылымдарының докторы, «Экономика, қаржы және есеп» кафедрасының меңгерушісі, И.С. Тургенев атындағы Орлов мемлекеттік университеті, Орел қ., Ресей Федерациясы
E-mail: lvp_134@mail.ru

Popova Ludmila - Doctor of Economic Sciences, Head of the Department of Economics, Finance and Accounting, Orel State University named after I.S. Turgenev, Orel, Russian Federation
E-mail: lvp_134@mail.ru