МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра финансов и кредита

АВТОРЕФЕРАТ

на выпускную квалификационную работу (магистерскую работу)

по направлению 38.04.01 Экономика

профиль «Финансовое планирование»

студентки 3 курса экономического факультета

Емельяновой Анастасии Олеговны

Тема работы: «Совершенствование страхования рисков информационной безопасности в России**»**

Научный руководитель:

Зав. кафедры финансов и кредита,

к.э.н., доцент _____ О. С. Балаш

Зав. кафедрой финансов и кредита,

к.э.н., доцент _____ О. С. Балаш

Саратов 2023

К началу 2021г. был достигнут значимый уровень внедрения информационных технологий, который помог сохранить устойчивость экономического развития России в условиях пандемии. За последние 20 лет произошло глобальное изменение цифровой инфраструктуры, покрытия Интернета и распространение мобильных устройств, что послужило поводом для создания линейки цифровых услуг и сервисов для граждан и предприятий. Если сравнить с временами финансового кризиса 2008г., то число смартфонов, которые в 2007–2008гг. только начали появляться, к 2021г. достигло 3,2 млрд. Количество пользователей сети Интернет с отметки 1,6 млрд возросло до 4,1 млрд человек (уровень распространения вырос с 23% до 54% населения). Глобальный интернет–трафик увеличился с 4 тыс. до 100 тыс. Гб в секунду. За 5 лет к началу 2021г. объем выручки электронной торговли в мире вырос более чем в 2,5 раза, достигнув отметки 3,5 трлн долл. Другими словами, состоялся огромный технологический прорыв, благодаря которому сформировались предпосылки для перевода ключевых процессов в цифровую среду и обеспечения их бесперебойности во время пандемии. Внедрение цифровых платформ и бизнес–моделей легло в основу устойчивых конкурентных преимуществ за счет уменьшения издержек и обеспечения лучшего качества «потребительского опыта».

Такая тенденция развития привела к заметному росту рынков дистанционных сервисов, например, таких как электронная коммерция, онлайн–образование, удаленная работа и телемедицина. Цифровые каналы превратились из периферийно−ориентированного на пользователей−новаторов — в массовый, а порой и единственный способ реализации повседневных потребностей населения и бизнеса.

За 2021г. опережающими темпами увеличилась аудитория онлайн−сервисов: при росте мирового населения на 1% число интернет−пользователей возросло на 7,3%, а количество активных аккаунтов в социальных сетях — на 13,2% (годовой прирост по данным на январь 2022г.). Произошли локальные сдвиги и в структуре потребления, благодаря которым

отдельные онлайн−услуги в 2021г. росли существенно быстрее долгосрочных среднегодовых темпов, значительно обгоняя прогнозы, которые были сделаны до пандемии.

На фоне замедления роста бизнес−сервисов, в том числе в сфере финансовых технологий, существенно увеличилось потребление информационного контента через дистанционные каналы при ощутимом сдвиге в сторону развлекательного и игрового форматов: за 2021г. мировой рынок онлайн−видео вырос на 29,2%, музыки — на 25,9%, видеоигр — на 23,2%. Однако в ближайшие 3–5 лет ожидается существенное замедление соответствующих сегментов рынка.

Вовлечение новых категорий населения обеспечило бум по целому ряду направлений: доля потребителей телемедицины в США возрасла с 11% до 46% в сравнении с 2020г.; на 640% увеличилось количество регистраций на образовательной онлайн−платформе Coursera20; прирост числа работников, полностью перешедших в ходе пандемии на удаленную работу, составил 27%.

Таким образом, цифровизация бизнеса и распространение дистанционных каналов передачи информации порождает новые риски.

Актуальность выбранной темы определена потребностью в разработке и введении условий, позволяющих обезопасить данные в киберпространстве. Такие условия очень важны для достижения определенного уровня безопасности информации.

Рост большинства отраслей экономики зависит от инновационных технологий, таких как искусственный интеллект, продвинутая аналитика и т.д., при внедрении которых усиливаются киберугрозы — компании и клиенты сталкиваются с новыми видами рисков. Чем больше датчиков, интерфейсов и данных, тем значительнее потенциальная поверхность для кибератак. Другими словами, чем сложнее информационная инфраструктура предприятия, тем выше вероятность угроз. Недостаточное внимание к средствам защиты информационных сетей может подвергнуть компанию серьезной опасности

заражения вредоносными программами и атаками, блокирующим сервисы и оборудование, а также возможной утечке данных и другим угрозам.

Проблема хищения, модификации, подделки информации приобрела наибольшее значение при развитии информационно–коммуникационных технологий. Кибератаки не только грозят потерей персональных данных, но и могут повлиять как на функционирование финансовых и коммерческих организаций, так и на экономику государства в целом.

Небезопасно и использование облачных сервисов, предоставляющих услуги по хранению информации, которые, как правило, расположены в других странах, а доступ к таким хранилищам зависит от скорости соединения и возможных сбоев.

Вместе с тем бизнес испытывает трудности с наймом и сохранением специалистов по кибербезопасности. Их число, согласно исследованию Международного консорциума по сертификации в области безопасности информационных систем, на текущий момент составляет ≈ 3,1 млн человек. Исследования показывают, что одной из наиболее востребованных технологических профессий является аналитик в области информационной безопасности. Несмотря на то, что уровень образования для работодателей по–прежнему остается важным показателем, предпочтение отдается опыту. Спрос на специалистов информационной безопасности постоянно растет, а число профессионалов, владеющих компетенциями в узкоспециализированных нишах, относительно небольшое. Также по–прежнему существует острая нехватка соответствующих навыков и знаний в сфере безопасности, необходимых для решения сложных задач. Оценка уязвимости систем организации к различным кибератакам, реагирование на инциденты и мониторинг угроз — три области IT, нуждающиеся в персонале, имеющем максимально широкий набор знаний. Проблема усугубляется стремительно возникающими и развивающимися новыми вызовами, что требует постоянного повышения квалификации сотрудников, и она не решается простым увеличением их количества в соответствующих структурах.

Исходя из этого, вполне обоснованно, что предприятия считают обеспечение безопасности приоритетом, а недостаточный уровень защиты от киберугроз заставляет их откладывать важные цифровые инициативы и ограничивает инвестирование в цифровые инновации.

Степень разработанности. Вопрос сущности киберстрахования и его роль в современном обеспечении информационной безопасности конфиденциальной информации исследованы многими современными учеными и практиками, основными из которых являются: Бураева Л.А., Абдуллаев В.Г., Бегларян М.Е., Мамакаев Х.В., Шайданов Т.Р., Казыханов А.А. Современные теоретико–методические основы функционирования рынка информационного страхования изучены Гулько А.А., Антонян М.Г., Махнева О.А., Солодкая А.М. и другими исследователями.

Целью данной выпускной квалификационной работы является выявить особенности в формировании продукта на рынке киберстрахования в России и разработка экономических и организационных основ для повышения эффективности страхования информационных рисков. Данная цель может быть достигнута только при решении ряда задач:

- рассмотреть законодательные основы, организацию и контроль киберстрахования в России;
- рассмотреть формирование и функционирование страховых компаний, предлагающих продукт по страхованию киберрисков в России;
- исследовать динамику основных показателей страхования киберрисков;
- выявить перспективы развития киберстрахования в РФ;
- сформулировать рекомендации по совершенствованию системы киберстрахования в России.

Предметом исследования выпускной квалификационной работы является деятельность страховых компаний, предоставляющих услуги

киберстрахования. Объектом исследования является анализ деятельности рынка страхования информационных рисков по критериям и показателям его деятельности за период с 2020 по 2022гг.

Научная новизна исследования заключается уже в самой постановке темы. По существу, настоящая выпускная квалификационная работа представляет собой опыт комплексного изучения процессов рынка страхования информационных рисков. Специфика современного киберстрахования изучена как элемент государственно–политического подхода и доказано, что киберстрахование является одним из главных направлений на рынке страхования в целом.

Научной новизной определена необходимость проведения реформы государством в части улучшения рынка страхования киберрисков с целью повышения уровня информационной безопасности компаний.

В данной работе киберстрахование рассматривается в качестве инструмента для решения приоритетной проблемы предприятий в условиях повсеместной цифровизации. Определены основные тенденции в области киберрисков, изучена динамика кибератак. Рассмотрены мероприятия, проводимые в России с целью предотвращения киберпреступлений. Систематизированы основные причины реализации киберугроз в банковской сфере, в числе которых не последнее место занимает человеческий фактор. Сформулированы выводы о том, что для предотвращения киберугроз необходимо внедрение банковских инноваций, основанных в том числе на использовании позитивного зарубежного опыта по применению процессно–ориентированного подхода, технологий BigData, блокчейн, биометрической идентификации клиентов.

Практическая значимость исследования обусловлена его результатами. Собранные и обобщенные в работе материалы, сделанные в ней выводы, могут быть использованы при написании обобщающих и проблемных трудов по вопросам сферы киберстрахования как регионального, так и муниципального уровня. Они могут найти применение в учебном процессе при чтении

лекционных курсов по финансам, спецкурсов, при разработке учебных пособий, студенческих дипломных и курсовых сочинений, что определило теоретическую значимость исследования.

Методологической основой, подготовленной выпускной квалификационной работы, стали принципы и методы научного познания. Диалектика такова: невозможно провести надлежащее исследование, если не следовать таким принципам как историзм, объективность и системность.

Принцип историзма означает развитие каждого элемента в его взаимосвязи и взаимозависимости с другими явлениями и событиями. Именно с этих позиций, мы пытались подойти к изучению деятельности рынка страхования информационных рисков.

Принцип объективности исследования означает стремление с определенной долей объективности показать накопленный опыт в решении вопросов финансового обеспечения инвестиционного процесса и его результатов.

Принцип системности означает невозможность рассматривать сферу страхования информационных рисков в отрыве от государственной политики в целом, проводимой в той или иной период исторического развития.

В ходе исследования применялись следующие методы научного познания:

- конкретно–исторический метод, позволивший проанализировать развитие механизма финансирования в строгой последовательности происходящих в обществе событий;
- логический метод дал возможность использовать ряд теоретических положений, выработанных учеными и проанализировать, обобщить статистический материал;
- ретроспективный метод позволяет определить место образовательной сферы в жизни человеческого общества, выявить особенности финансирования на различных этапах истории;

- структурно–функциональный метод способствовал определению основных направлений использования выделяемых финансовых ресурсов и эффективность деятельности киберстрахования;
- сравнительный анализ дал возможность выделить общее, особенное и единичное в механизмах рынка страхования киберрисков;
- статистический метод использовался для обработки статистических данных, имеющихся по теме исследования. Это является особо ценным для последующих выводов и предложений, сделанных по ходу исследования.

Нормативно–правовая база выпускной квалификационной работы включает в себя анализ таких документов как законодательные и нормативные акты Государственной Думы и Правительства РФ, Министерства экономики, Гражданский и Налоговый Кодексы РФ,

Практическую базу составляют официальные данные Центрального Банка России, Росстата, отчётные данные Всероссийского Союза Страховщиков в сотрудничестве с Торгово–промышленной палатой России, а также исследования дочерней компании СберБанка BI.ZONE.

Структура выпускной квалификационной работы. В первой главе дана общая характеристика рынка страхования, подробнее рассмотрен рынок страхования информационных рисков, а также объекты страхования рисков информационной безопасности.

Вторая глава посвящена анализу текущей ситуации на рынке страхования информационных рисков в России (взят период 2020–2022гг.), и анализу развития отрасли страхования киберрисков в России.

В третьей главе раскрываются перспективы развития и предложения по улучшению продуктов, предлагаемых на рынке киберстрахования в России.

Учет инновационных способов борьбы с несанкционированными доступами к информационной системе банка, своевременная корректировка условий и ликвидация причин для появления тех или иных рисков в совокупности сократит шансы на банковский кризис, уменьшит материальный

ущерб банков от кибератак, что положительно скажется на экономических показателях страны. Проблема кибербезопасности систем управления в современном мире является актуальной, так как касается безопасности не только технических средств и устройств, но и интересов общества. Обеспечение безопасности в цифровом пространстве — финансовый приоритет для большинства субъектов хозяйствования. При этом вопрос определения объема инвестиций в решения по управлению рисками пропорционально мерам по поддержке цифровых инициатив становится самым важным, так как модернизация систем безопасности после их внедрения, как правило, гораздо более дорогостоящее и менее эффективное мероприятие.

Компании все чаще рассматривают кибербезопасность не как статью расходов, а как инвестиционную стратегию. Приоритеты в распределении финансовых средств они устанавливают на основе анализа всего портфеля осуществляемых инициатив, приоритизации цифровых активов, от которых зависит непрерывность и стабильность бизнес–процессов, оценки рисков по степени критичности и возможностей в области киберзащиты в сравнении с отраслевыми показателями. По мнению экспертов консалтингового агентства McKinsey около 50% систем компаний не являются критичными с точки зрения кибербезопасности. Повышая цифровую устойчивость, они могут экономить до 20% затрат, направленных на защиту наиболее значимых, чувствительных цифровых активов.

При принятии обоснованных инвестиционных решений и возможности измерения эффективности снижения рисков или сравнения с другими корпоративными инвестициями важна их экономическая оценка, что дает возможность реализации более широкого спектра мероприятий по обеспечению кибербезопасности фирмы, включая обучение, поставщиков и цепочки поставок, киберстрахование. Последнее представляет собой передачу компаниями некоторых рисков, которые могут нанести значительный финансовый и операционный ущерб, специализированным страховым агентствам. Киберстрахование становится важным элементом управления

рисками, при этом его продукты не могут заменить надежную корпоративную программу информационной безопасности, а лишь дополняют ее, обеспечивая страховое покрытие, например, в таких областях, как ответственность за утечку данных, затраты на расследование нарушений, уведомление пострадавших сторон, штрафы и другие расходы. Сегодня это неотъемлемая часть ведения бизнеса.

Каждая организация предпринимает определенные действия по защите целостности инфраструктуры и программного обеспечения своих цифровых цепочек поставок, меры по управлению данными рисками, взаимодействию на общих стандартах во всей Сети, внедрению принципов безопасного поведения в киберпространстве. Многие инциденты — результат человеческой ошибки, особенно в таких сферах, как фишинг, взлом деловой электронной почты — самых распространенных форм кибератак. При этом слишком мало компаний предпринимают действия по созданию сильной культуры кибербезопасности. Ознакомление сотрудников с потенциальными угрозами, их осведомленность на всех уровнях о видах кибератак и лучшими методами их отражения, повышение квалификации и тестирование кибернавыков — наиболее эффективные формы смягчения последствий, которые могут значительно снизить вероятность возникновения киберсобытия или минимизировать его последствия.

Таким образом, цифровая трансформация открывает множество новых возможностей для бизнеса, создавая при этом значительные проблемы в сфере цифровой безопасности. Все чаще предупреждение и ослабление киберрисков рассматривается как часть бизнес–процесса, становится фактором поддержки и ускорения инноваций, бизнес–приоритетом для высшего руководства. Сегодня кибербезопасность как модель управления рисками, обеспечения доверия и взаимовыгодного сотрудничества может стать для компаний фактором роста и развития.