EURASIAN JOURNAL OF ACADEMIC RESEARCH
Innovative Academy Research Support Center
UIF = 8.1 | SJIF = 7.899 www.in-academy.uz

PROTECTION IN THE DIGITAL AGE: THE MEANING AND IMPORTANCE OF CYBER CRIME INSURANCE

Abdullaev Sherkhan
Master's student at Tashkent Law University
Specialties "Cyber Law"
https://doi.org/10.5281/zenodo.11262010

ARTICLE INFO

Received: 14th May 2024
Accepted: 22th May 2024
Online: 23th May 2024

KEYWORDS

Digital technology, cybercrime, ABO, insurance.

ABSTRACT

In today's world, where digital technology plays an increasingly important role in our daily lives and business processes, cybercrime is becoming a growing threat. Attacks on computer systems, data theft and online fraud cause significant losses to both individuals and companies. In response to these threats, there is a growing demand for cybercrime insurance as a means of protecting against potential financial loss and reputational damage. This essay will examine the significance and importance of cybercrime insurance in today's world.

ЗАЩИТА В ЦИФРОВУЮ ЭПОХУ: ЗНАЧЕНИЕ И ВАЖНОСТЬ СТРАХОВАНИЯ ОТ КИБЕРПРЕСТУПНОСТИ

Абдуллаев Шерхан
Магистрант Ташкентского юридического университета
Специальности «Кибер право»
https://doi.org/10.5281/zenodo.11262010

ARTICLE INFO

Received: 14th May 2024
Accepted: 22th May 2024
Online: 23th May 2024

KEYWORDS

Цифровые технологии, киберпреступность, НПА, страхование.

ABSTRACT

В современном мире, где цифровые технологии играют все более значимую роль в нашей повседневной жизни и бизнес-процессах, киберпреступность становится все более серьезной угрозой. Нападения на компьютерные системы, кража данных и мошенничество в сети интернет приносят значительные убытки как частным лицам, так и компаниям. В ответ на эти угрозы растет спрос на страхование от киберпреступности как средство защиты от потенциальных финансовых потерь и репутационного ущерба. В этом эссе рассмотрим значимость и важность страхования от киберпреступности в современном мире.

Страхование - это важнейшая составляющая функционирования рыночных отношений, являющаяся обязательным элементом социальной и экономической систем общества, которая затрагивает интересы личности, а также обеспечивает необходимую защиту имущественных интересов хозяйствующих субъектов, нарушенных вследствие наступления неблагоприятных обстоятельств природного или иного характера[1].

Первоначально, страхование от киберпреступности представляет собой инструмент защиты, который помогает компаниям и частным лицам минимизировать риски, связанные с потенциальными кибератаками. Ни одна компания или организация не застрахована от возможности стать жертвой хакеров или киберпреступников. Страхование от киберпреступности позволяет защитить компанию от потери данных, финансовых убытков и репутационного ущерба в случае успешной атаки. Это помогает снизить финансовые риски и обеспечить более стабильное функционирование бизнеса.

Во-вторых, страхование от киберпреступности стимулирует компании улучшать свои кибербезопасностные практики. Для получения страховки от киберрисков компании часто вынуждены проходить аудит своей кибербезопасности и внедрять меры защиты. Это в свою очередь способствует повышению уровня безопасности компьютерных систем и защите конфиденциальной информации. Таким образом, страхование от киберпреступности играет важную роль в повышении общего уровня кибербезопасности, кроме того, страхование от киберпреступности может оказаться крайне полезным в восстановлении после кибератаки. Даже при наличии мер предосторожности и многоуровневых систем защиты, атаки все равно могут произойти. В таких случаях страхование от киберпреступности помогает компаниям быстрее восстановиться после инцидента, предоставляя финансовую поддержку для восстановления данных, возмещения ущерба и восстановления репутации, однако, страхование от киберпреступности также имеет свои ограничения и вызовы. Одним из них является сложность оценки рисков в цифровой среде. Быстро меняющаяся природа киберугроз делает сложным прогнозирование потенциальных угроз и оценку рисков. Это может привести к тому, что страховые компании будут иметь трудности с определением стоимости полисов и устанавливать соответствующие премии.

Кроме того, страхование от киберпреступности может также способствовать некоторому уровню невнимательности со стороны компаний в области кибербезопасности. Некоторые компании могут полагаться слишком сильно на страхование, забывая о необходимости регулярного обновления и улучшения своих кибербезопасностных мер. Это может привести к тому, что компании становятся более уязвимыми к кибератакам, несмотря на наличие страхового полиса.

Особая актуальность киберстрахования проявляется в периоды после проведения каких-либо масштабных кибератак. Так, например, после атаки на серверы американской компании Yahoo (вторая по популярности в мире поисковая система) в 2014 году, спрос на страхование кибер-рисков только в одной Америке вырос в 3 раза. Тогда хакеры взломали около 500 млн. аккаунтов пользователей, и им стала доступна

[1] https://cyberleninka.ru/article/n/ponyatie-i-printsipy-strahovaniya

личная информация абонентов, такая как даты рождения, номера телефонов и пароли. Также в США всплеск спроса на кибер-страхование наблюдался и после взлома хакерами системы бюро кредитных историй Equifax. Злоумышленники завладели личной информацией более чем 140 млн. американцев, такой как номера водительских удостоверений, и счетов социального страхования[2].

Романенко Н. в статье «Страхование информационных рисков предприятий как инструмент риск-менеджмента» пишет, что в настоящее время в мировой практике страховые компании предлагают страховую защиту следующих видов рисков:

1. Риск хищения конфиденциальной информации и ее дальнейшего использования работниками организации;
2. Риск хищения преступниками информации о клиентов банков, такой как номера кредитных карт и счетов;
3. Риск кражи денег со счетов клиентов банков;
4. Риск разглашения секретной информации сотрудников компании;
5. Риск остановки работы предприятия из-за сбоев компьютерной сети, сайта организации и т. п.;
6. Получения убытка организацией, в связи с размещением ложной информации и др[3].

Страхование от киберпреступности играет все более важную роль в современном цифровом мире. Оно представляет собой не только инструмент защиты от потенциальных финансовых потерь и репутации ущерба, но и стимулирует компании улучшать свои кибербезопасностные практики. Однако, необходимо помнить, что страхование от киберпреступности не является панацеей, и компании должны продолжать инвестировать в кибербезопасность и принимать меры для защиты от киберугроз.

Применения международных норм содействия и стандартизация для применения НПА, и международные стандарты кибербезопасности: Организации, такие как Международная организация по стандартизации (ISO) и Международное бюро стандартов (IEC)[4], разрабатывают стандарты и рекомендации по кибербезопасности. Примером может служить стандарт ISO/IEC 27001, который предоставляет набор мер и процедур для управления информационной безопасностью в организации. Страховые компании могут ориентироваться на такие международные стандарты при оценке кибербезопасностных практик своих клиентов и разработке условий страхования.

В рамках международных отношений и торговли, существуют законы и нормативные акты, регулирующие обработку и защиту данных. Примерами могут служить Общее регулирование по защите данных (GDPR) в Европейском Союзе и Личная информация о здоровье и портативная страховка (HIPAA) в Соединенных Штатах. Страховые компании, оперирующие в различных юрисдикциях, должны учитывать

[2] https://cyberleninka.ru/article/n/strahovanie-informatsionnyh-riskov-kiberstrahovanie
[3] Романенко Н.А. Страхование информационных рисков предприятий как инструмент риск-менеджмента // Финансовые исследования - 2018 №7. С. 13-24
[4] https://www.iso.org/standard/27001

такие международные нормы при разработке полисов страхования от киберрисков и адаптации их к местным требованиям.

Если же говорить о международном сотрудничестве в борьбе с киберпреступностью, то выделяют такие международные организации как Организация Объединенных Наций (ООН), Интерпол и другие, играют важную роль в содействии международному сотрудничеству в борьбе с киберпреступностью. Страховые компании могут сотрудничать с такими организациями для обмена информацией о новых угрозах и методах защиты, а также для разработки общих подходов к оценке и управлению киберрисками.

Международные стандарты отчетности о кибербезопасности: Многие международные организации и стандартизирующие организации разрабатывают стандарты отчетности о кибербезопасности для оценки и демонстрации эффективности киберзащиты. Примером может служить Фреймворк кибербезопасности Национального института стандартов и технологий (NIST) в США[5]. Страховые компании могут использовать такие стандарты для оценки кибербезопасности потенциальных клиентов и разработки условий страхования.

В целом, использование международных норм и стандартов в страховании от киберпреступности позволяет создать более единый и эффективный подход к оценке, управлению и снижению киберрисков как на местном, так и на международном уровнях. Это способствует повышению безопасности в цифровой среде и защите интересов компаний и частных лиц от киберугроз.

В Узбекистане применяются нормативно-правовые акты (НПА), которые регулируют различные аспекты жизни общества, включая сферу страхования от киберпреступности. Вот несколько примеров применения норм НПА в Узбекистане в контексте страхования от киберпреступности:

В Узбекистане существует ряд законодательных актов, регулирующих страховую деятельность в целом. Например, "О страховании" является основным законодательным актом, определяющим правовые основы страхования в стране. В рамках этого закона могут устанавливаться и нормы, касающиеся страхования от киберпреступности, включая требования к страховым полисам, процедуры компенсации убытков и другие аспекты, нормы по защите информации: в контексте кибербезопасности важно также учитывать нормы и требования по защите информации. Законы и постановления, касающиеся защиты персональных данных и информационной безопасности, регулируют сбор, обработку и хранение информации, включая данные, связанные с киберпреступностью. Эти нормы могут оказывать влияние на требования к страхованию от киберугроз и обязанности страховых компаний по защите информации клиентов.

Регулирование кибербезопасности: Правительство Узбекистана также может принимать специальные постановления и нормативные акты, направленные на улучшение кибербезопасности в стране. Эти нормы могут включать в себя требования

[5] https://www.nist.gov/cyberframework

к киберзащите организаций, включая страховые компании, и меры по предотвращению киберпреступности. Такие нормы могут также оказывать влияние на разработку страховых продуктов и условий страхования от киберрисков.

Узбекистан может также принимать во внимание международные нормы и стандарты в области кибербезопасности при разработке своего законодательства и нормативных актов. Это может включать в себя соблюдение международных соглашений и стандартов, таких как Конвенция о киберпреступности и стандарты ISO/IEC по управлению кибербезопасностью.

Таким образом, нормы НПА в Узбекистане оказывают влияние на различные аспекты страхования от киберпреступности, включая правовую основу деятельности страховых компаний, требования к защите информации и кибербезопасности, а также учет международных стандартов и соглашений в этой области.

References:

1. https://www.nist.gov/cyberframework
2. https://www.iso.org/standard/27001
3. https://cyberleninka.ru/article/n/ponyatie-i-printsipy-strahovaniya
4. https://lex.uz/
5. https://cyberleninka.ru/article/n/strahovanie-informatsionnyh-riskov-kiberstrahovanie
6. Романенко Н.А. Страхование информационных рисков предприятий как инструмент риск-менеджмента // Финансовые исследования - 2018 №7. С. 13-24