УДК 368.8

РОЛЬ КИБЕРСТРАХОВАНИЯ В СИСТЕМЕ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ: МЕСТО ГОСТ Р 59516-2021 И ISO/IEC 27102

Абдулаев В.А.[1] (магистрант),
Научный руководитель – доктор технических наук, профессор Швед В.Г.[1]
[1]Университет ИТМО
abdulaevvusal@gmail.com

Введение. Рост зависимости организаций от информационных систем сопровождается увеличением числа киберинцидентов и связанных с ними финансовых потерь. В условиях невозможности полного устранения киберрисков востребованы механизмы, компенсирующие последствия инцидентов информационной безопасности. Киберстрахование рассматривается как инструмент передачи части остаточного риска страховой организации [2; 3]. Однако анализ российской практики показывает, что страховые продукты часто приобретаются в отрыве от системного управления рисками, что порождает несоответствие между покрытием и реальным риск-профилем. Согласно опросу страхового брокера АСТ (2025 г.), 86 % страховщиков указывают на переоценку компаниями собственной защищённости, а 71 % – на непонимание страхового продукта как ключевой барьер развития рынка [6]. Указанные обстоятельства обусловливают необходимость определения места киберстрахования в системе менеджмента информационной безопасности (СМИБ).

Основная часть. Управление информационной безопасностью базируется на риск-ориентированном подходе, реализуемом в рамках СМИБ в соответствии с ISO/IEC 27001 и ISO/IEC 27005 [2]. В рамках данного подхода идентифицируются активы, угрозы и уязвимости, оцениваются вероятности и последствия инцидентов, выбираются стратегии обработки риска (снижение, принятие, передача). Передача риска посредством страхования трактуется как дополнение к организационным и техническим мерам защиты [2; 3].

Национальный стандарт ГОСТ Р 59516-2021 устанавливает правила страхования рисков информационной безопасности и прямо указывает на необходимость использования результатов риск-оценки при формировании условий страхования (перечень событий, лимиты ответственности, порядок урегулирования убытков) [3]. Международный стандарт ISO/IEC 27102 позиционирует киберстрахование как вариант обработки киберрисков и регламентирует взаимодействие сторон на основе данных СМИБ [5]. Применение результатов риск-оценки позволяет обеспечить адекватность страхового покрытия, повысить точность андеррайтинга и снизить информационную асимметрию [1; 3; 5].

Количественные параметры российского рынка подтверждают его начальную стадию развития. По итогам 2025 г. объём рынка оценивается в 3,5–4 млрд руб. (менее 0,2 % глобального объёма в 15,6 млрд долл.) [7]; уровень проникновения среди крупных предприятий составляет 12,5 % [8]. Для сравнения: в ряде европейских стран этот показатель достигает 22–39 % [8]. Потенциал роста российского сегмента оценивается экспертами в 7–10 млрд руб. к 2027–2028 гг. [7], однако его реализация сдерживается как нормативными ограничениями (невозможность страхования штрафов и выкупов), так и организационными барьерами, включая отсутствие у страхователей формализованных процедур оценки рисков [6; 8].

Интеграция киберстрахования в СМИБ обеспечивает использование данных о рисках при формировании страхового покрытия, а также применение информации о произошедших инцидентах для корректировки оценок и совершенствования мер защиты

[2; 3; 5]. Это способствует повышению эффективности управления киберрисками и устойчивости организации к последствиям киберинцидентов.

Выводы. Киберстрахование целесообразно рассматривать как элемент системы управления информационной безопасностью, обеспечивающий передачу части остаточных киберрисков. Эффективность страховой защиты непосредственно зависит от степени интеграции страховых процессов в контур СМИБ. Стандарты ГОСТ Р 59516-2021 и ISO/IEC 27102 формируют методологическую основу для такой интеграции, позволяя согласовывать параметры страхового покрытия с реальным риск-профилем организации [3; 5]. Преодоление выявленных барьеров (нормативных и организационных) является условием реализации потенциала российского рынка киберстрахования.

Список использованных источников:

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. действующая) [Электронный ресурс]. – Режим доступа: https://normativ.kontur.ru/document?moduleId=1&documentId=501173 (дата обращения: 24.02.2026).
2. Степанова М.Н., Юсупова М.Н. Генезис российской практики киберстрахования // Журнал прикладных исследований. 2021. Т. 9. № 6. С. 874-881.
3. ГОСТ Р 59516-2021 «Информационные технологии. Менеджмент информационной безопасности. Правила страхования рисков информационной безопасности» [Электронный ресурс]. – Режим доступа: https://base.garant.ru/405037679/ (дата обращения: 24.02.2026).
4. ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management [Электронный ресурс]. – Режим доступа: https://pecb.com/en/whitepaper/iso-iec-27005-information-technology-security-techniques-information-security-risk-management (дата обращения: 24.02.2026).
5. ISO/IEC 27102:2019 Information security management – Guidelines for cyber-insurance [Электронный ресурс]. – Режим доступа: https://www.iso.org/standard/72436.html (дата обращения: 24.02.2026).
6. Исследование страхового брокера АСТ «Тренды киберстрахования 2025: страховщики vs страхователи» (цит. по: РБК Компании, 14.11.2025) [Электронный ресурс]. – Режим доступа: https://companies.rbc.ru/news/ZXLRCiHw9X/ (дата обращения: 25.02.2026).
7. Объем российского рынка киберстрахования за год вырос до 4 млрд рублей (TAdviser, 28.01.2026) [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Статья:Киберстрахование (дата обращения: 25.02.2026).
8. Рынок киберстрахования начал активно расти на фоне новых атак (Korins.ru, 19.01.2026, цит. эксперта Игоря Расторгуева) [Электронный ресурс]. – Режим доступа: https://www.korins.ru/posts/13320-rynok-kiberstrahovaniya-nachal-aktivno-rasti-na-fone-novyh-atak (дата обращения: 25.02.2026).

Автор _____ В.А. Абдулаев

Научный руководитель _____ В.Г. Швед