# НСИС сформулировал принципы единой методологии оценки киберготовности организаций в рамках развития системы страхования киберрисков

Директор по информационной безопасности Национальной страховой информационной системы (НСИС) Алексей Янов в ходе форума «CNews Forum Кейсы: Опыт ИТ-лидеров 2026» предложил в рамках развития системы страхования киберрисков в РФ создать концепцию единой методологии оценки киберготовности организаций, базирующейся на актуальных национальных стандартах.

«Как показывают экспертные обсуждения на рынке, одной из ключевых проблем, сдерживающих развитие киберстрахования, является «размытость» критериев оценки риска. Разные страховщики используют собственные опросники и методики, что приводит к субъективизму при расчете премии и, главное, к сложностям в перестраховании и урегулировании убытков», — отметил А.Янов.

Он предложил внедрить в практику страховщиков обязательный или добровольный (в зависимости от масштаба риска) стандарт оценки на основе ГОСТ Р 57580.х (серии «Безопасность финансовых (банковских) операций»). ГОСТ Р 57580.1 уже зарекомендовал себя как надежный инструмент оценки технического состояния ИБ, на него опирается Банк России в своих нормативных документах. Предлагается доработать стандарт (или создать на его основе отраслевой чек-лист), убрав узкую банковскую специфику (эквайринг и т.д.), для применения во всех секторах экономики (промышленность, МСП, ритейл), уточнил директор по ИБ НСИС.

При этом решается и вопрос неразглашения чувствительной информации по принципу «черного ящика»: автоматизированная система должна не раскрывать страховщику такую информацию (события информационной безопасности, настройки средств защиты и т.д.), а давать интегральную динамическую оценку уровня защиты на базе ГОСТ 57580.2.

Такой подход обеспечит прозрачное ценообразование: страховая премия будет привязана к объективной цифре, рассчитываемой по единой формуле, что критически важно для перестрахования (снижение споров между страховщиками).

Таргетирование рисков может быть устроено следующим способом: крупные предприятия с большими страховыми суммами будут проходить потоковую (on-line) оценку через SIEM-системы и телеметрию, а для МСП будет достаточно периодического прохождения чек-листа (самооценки).

При этом будет обеспечено оперативное урегулирование убытков — при наступлении страхового случая у экспертов будет четкая «база нормального состояния» (слепок соответствия ГОСТу до атаки), что позволит в разы быстрее фиксировать факт взлома, оценивать ущерби отсекать мошенничество.

Одновременно будет происходить стимулирование безопасности — внедрение такого подхода заставит страхователей реально подтягивать уровень киберзащиты, так как «плохая оценка» будет означать высокий тариф или отказ в покрытии, резюмировал Алексей Янов.

**Википедия страхования, 22.06.2026 г.**