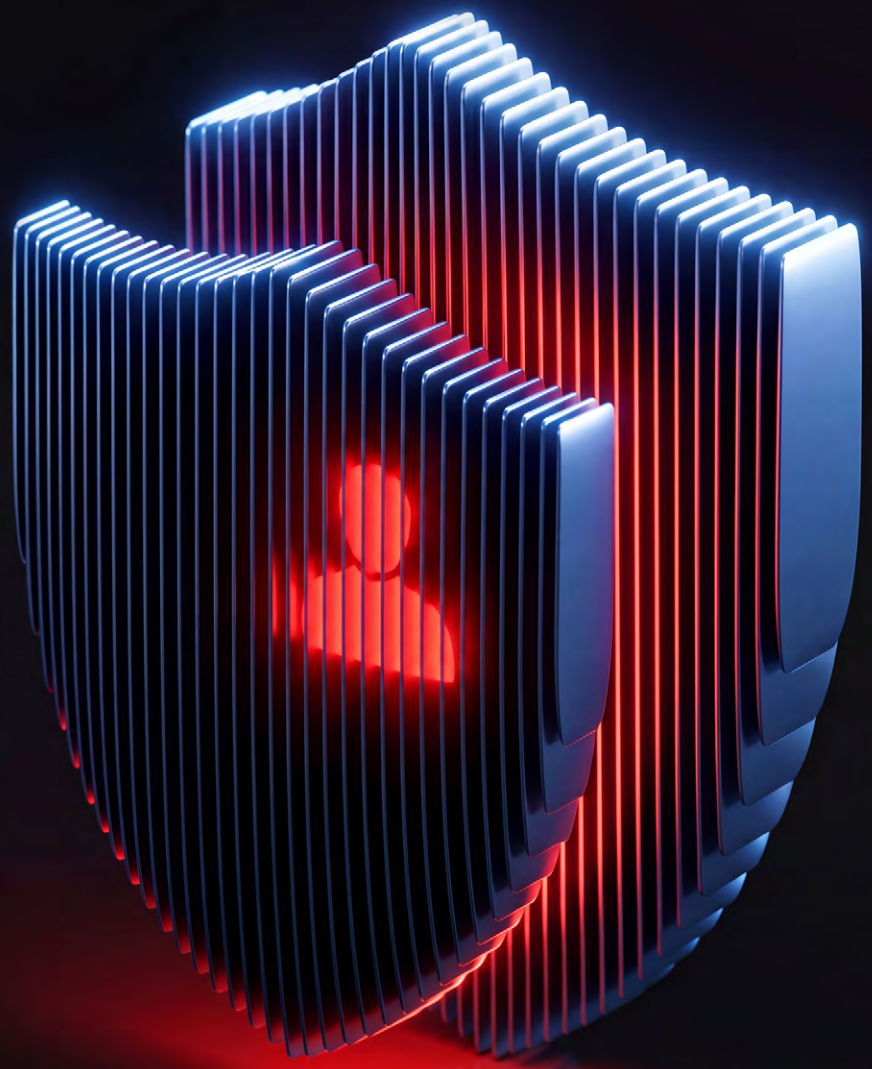
The Edgers × SuperJob × positive education

ТРАНСФОРМАЦИЯ РОЛИ CISO В РОССИИ: РАЗРЫВ МЕЖДУ ОЖИДАНИЯМИ И РЕАЛЬНОСТЬЮ



Совместное исследование
The Edgers x SuperJob x PT Education

Май 2026

СОДЕРЖАНИЕ

Анастасия Федорова

руководитель образовательных программ Positive Education, Positive Technologies

— Россия входит в число наиболее атакуемых стран мира: по данным Positive Technologies, с середины 2024-го по сентябрь 2025 года на нее пришлось от 14 до 16% всех успешных кибератак в мире. По итогам 2025 года аналитики ожидают рост числа успешных атак на 20–45% к предыдущему году, а в 2026-м — еще на 30–35%. Предпосылок для того, чтобы тренд изменился, нет: расширяется цифровая инфраструктура, растет число организованных группировок, геополитическая напряженность не снижается.

На этом фоне кибербезопасность перестала быть исключительно технической темой, ее все чаще обсуждают законодатели и первые лица крупных компаний. Так, с 2025 года в России существенно ужесточена ответственность за утечки персональных данных, включая введение оборотных штрафов, расширены полномочия контролирующих органов. А тема «новой киберреальности» регулярно поднимается на уровне крупных деловых форумов уровня ПМЭФ-2025 и ЦИПР-2025, хотя еще несколько лет назад это происходило лишь на специализированных технических конференциях.

На этом фоне логично ожидать, что усиление внимания к кибербезопасности изменит и роль людей, которые за нее отвечают. Речь идет о CISO (chief information security officer — директор по информационной безопасности) — это руководители, которые отвечают за защиту цифровой инфраструктуры компании, управляют киберрисками и выстраивают процессы безопасности. Но так ли это происходит на практике? И какие именно изменения переживает эта роль прямо сейчас? Этим вопросам посвящено данное исследование.

Чтобы получить ответы, мы провели глубинные интервью с тремя группами участников: действующими CISO, генеральными директорами и техническими директорами и CIO — всего опросили 43 респондентов. Такая выборка позволила сопоставить три взгляда на одну функцию и зафиксировать расхождения в ожиданиях, языке описания ценности и критериях оценки эффективности.

Выводы исследования будут полезны в первую очередь трем аудиториям. Сами CISO смогут сверить собственное восприятие роли с тем, чего от них ждут коллеги и руководство, и получить ориентиры для профессионального развития. Руководители компаний — лучше понять, как выстроить взаимодействие с функцией информационной безопасности и сформулировать внятные критерии оценки ее эффективности. Рынок корпоративного образования увидит, какие компетенции сегодня в дефиците и какие программы нужны индустрии кибербезопасности.

EXECUTIVE SUMMARY

КОРОТКО О ГЛАВНОМ

Рынку требуется новый тип CISO — руководитель, способный выступать «переводчиком» между технологическими рисками и угрозами для бизнеса.

Кибербезопасность вышла за пределы технологической функции и стала одним из факторов устойчивости бизнеса. Руководители компаний все чаще связывают цифровую безопасность с финансовой стабильностью, непрерывностью операций и репутацией организации. Однако большинство CEO по-прежнему воспринимают CISO только как руководителя технологической функции.

В результате возникает разрыв между ожиданиями бизнеса и реальной ролью директора по информационной безопасности. Такой специалист должен уметь объяснять угрозы и обосновывать инвестиции в безопасность в терминах бизнес-рисков, устойчивости и стратегических последствий для компании. Однако ни университетские программы, ни большинство программ дополнительного профессионального образования сегодня системно не формируют подобный профиль.

ПЯТЬ ОСНОВНЫХ ВЫВОДОВ

1 **>40%**

CEO и CISO по-разному оценивают зрелость роли. Больше 40% CISO в исследовании оценивают себя на уровне 8–9 баллов из 10, и лишь 13,4% опрошенных демонстрируют умеренную самокритику. Тогда как оценка роли со стороны CEO заметно ниже: высокую оценку (7–10 баллов из 10) дали лишь 25% опрошенных.

2 **37.5%**

Более чем в трети компаний отсутствует регулярный диалог между CEO и CISO. 37,5% CEO отметили, что не взаимодействуют с CISO напрямую, или вовсе не смогли оценить своего директора по информационной безопасности.

3 **62.5%**

Участие CISO в стратегическом планировании остается ограниченным. Более половины компаний воспринимают безопасность как технологическую функцию, а не как полноценного участника стратегических решений: 62,5% опрошенных CEO не ожидают активного участия CISO в стратегическом планировании компании.

4 **50%**

Кибербезопасность и бизнес говорят на разных языках. CISO описывают киберриски в терминах уязвимостей, устойчивости инфраструктуры и технических метрик. А топ-менеджмент принимает решения, опираясь на финансовые последствия и устойчивость бизнеса. Связь между показателями ИБ и бизнес-результатами часто остается слабой или неочевидной, поэтому 50% CISO прямо говорят о том, как важно «переводить» с языка кибербезопасности на язык бизнеса.

5 **100%**

Рынок образования не решает проблемы взаимопонимания CEO и CISO. 100% опрошенных нами сходятся в одном: существующие программы обучения не закрывают имеющиеся вопросы.

ЧТО ЭТО ЗНАЧИТ ДЛЯ БИЗНЕСА

Разрыв между ожиданиями топ-менеджмента бизнеса и текущей ролью CISO имеет системный характер. Безопасность постепенно становится частью управленческой повестки компаний, однако язык коммуникации, структура ответственности и система метрик директора по информационной безопасности практически не изменились. В итоге киберриски все чаще обсуждаются на уровне совета директоров и топ-менеджмента, но функция кибербезопасности продолжает работать преимущественно в операционном и техническом контурах. Из-за этого отсутствует полноценный управленческий диалог, позволяющий оценить масштаб подобных рисков и возможные последствия киберинцидентов.

КАК МЫ ОЦЕНИВАЛИ

Исследование провели в формате глубинных интервью с представителями трех ключевых ролей: CISO, CEO и CTO/CIO. Всего 43 респондента. Среди них топ-менеджеры разных отраслей с разным масштабом бизнеса: банковская розница и финтех, технологические и e-com-платформы, ритейл и FMCG, промышленность и электроэнергетика, телеком, продуктовые IT-компании. Такая выборка позволила сопоставить три взгляда на одну и ту же функцию — информационную безопасность — и зафиксировать расхождения в ожиданиях, языке описания ценности и критериях оценки эффективности. Методология исследования носила качественный характер, то есть интервью строились на основе открытых вопросов.

ЧТО МЫ ХОТЕЛИ ПОНЯТЬ

Целью исследования было выявить системные разрывы в восприятии роли CISO и определить ключевые барьеры на пути трансформации CISO в полноценного бизнес-партнера. Полученные результаты отражают качественную картину текущего состояния роли директора по информационной безопасности и позволяют сформулировать практические рекомендации для CISO, CEO и рынка корпоративного образования.

ЧТО МОЖНО СДЕЛАТЬ

Чтобы преодолеть разрыв, нужны синхронные изменения сразу на трех уровнях.

1. CISO необходимо системно развивать бизнес-компетенции и навыки управленческой коммуникации.
2. CEO — сформулировать понятные критерии оценки киберустойчивости и способности CISO их обеспечить.
3. Рынок образования — создавать практико-ориентированные программы для CISO, соединяющие технологическую экспертизу, бизнес-мышление и навыки стратегического управления.

Результат совместной трансформации приблизит компании к обеспечению киберустойчивости — способности выдерживать инциденты, адаптироваться к ним и быстро восстанавливать работу критически важных процессов.

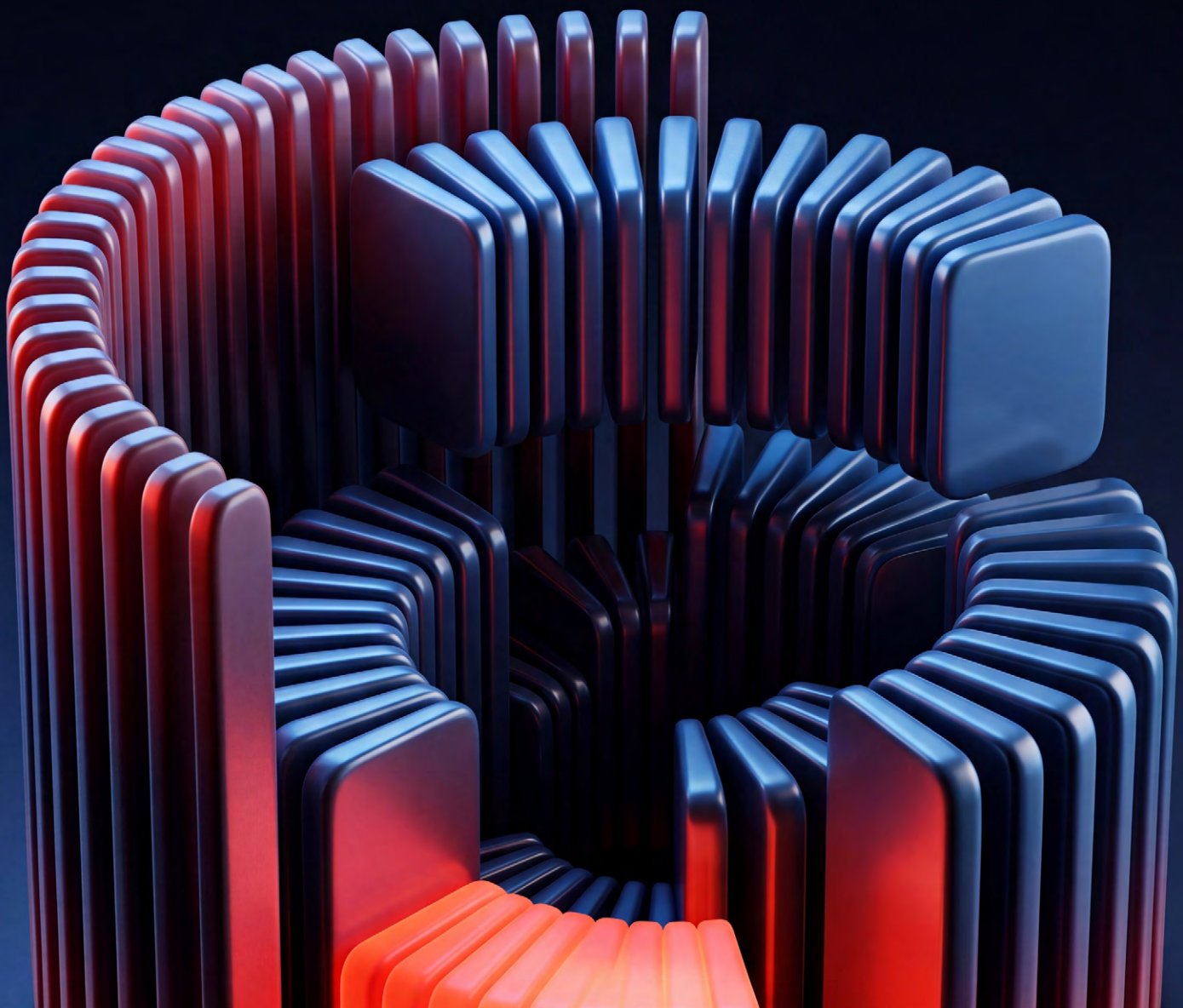
ГЛАВА 1

КАРТА НЕПОНИМАНИЯ: ТРИ ВЗГЛЯДА НА ОДНУ РОЛЬ

Одну и ту же позицию CISO опрошенные нами респонденты видят по-разному.

- CEO ждут стратегического партнера, который способен говорить на языке бизнеса;
- CTO/CIO оценивают директоров по информационной безопасности, как партнеров по технологическому блоку;
- сами CISO уверены, что уже работают в партнерской модели и с CEO и с CTO/CIO.

В этой главе мы покажем, где расходятся ожидания и оценки роли, и почему этот разрыв создает проблемы.



CEO ПРО CISO: НИЖЕ ОЖИДАНИЯ

Больше трети опрошенных CEO (37,5%) хотят, чтобы CISO умел считать риски в деньгах. В их ответах ожидания финансового обоснования инвестиций в кибербезопасность с оценкой уровня риска и приоритизацией планов развития : «управлять размером риска и трейд-оффами», «сделать стратегический план бюджета», «находить баланс между затратами и уровнем риска», «умение делать cost–benefit анализ». Также 50% респондентов подчеркивает: CISO должен глубоко понимать специфику бизнеса. От этого управленца ожидают «погружение в бизнес», «понимание бизнес-процессов компании», «понимать, что критично, а что нет», «сам будет понимать, какие изменения в процессы нужно привнести».

От CISO также ожидают способность к стратегическому мышлению (25%) и развитые навыки коммуникации (25%). В ответах звучат формулировки «способный стратегически взглянуть на картинку», «нужна стратегическая роль», «уметь доносить свои мысли, аргументировать позицию и экономику решений», «управление отношениями». CEO прямо говорят о необходимости отстаивать баланс между затратами и риском, поскольку цена ошибки «может составлять миллиарды рублей».

Техническая экспертиза фигурирует почти в 37,5% ответов как обязательная. Респонденты говорят о «глубоких ИТ-компетенциях», «компетенциях ИТ-архитектора» и знании «лучших современных практик». При этом CEO описывают техническую глубину как «гигиенический минимум», не достаточный для полноценного партнерства с бизнесом.

КАК CEO ОЦЕНИВАЮТ CISO

Четверть респондентов, отвечая на вопрос «Как вы оцениваете текущие навыки и уровень зрелости CISO в вашей организации?», дали высокую оценку 7 или 8 баллов из 10. Подчеркивались «навык управления здоровым балансом риска», «умение строить сильную команду», «правильное управление ресурсами», «делает вещи правильно». Впрочем, даже здесь звучат оговорки о необходимости большей интеграции в бизнес-процессы.

Однако 37,5% CEO формулируют оценку как «слабо» или «недостаточно». В этих ответах одни и те же проблемы: CISO слабо погружен в бизнес и остается на уровне решения ИТ-задач. Один из спикеров прямо говорит, что CISO «не видел рисков и слишком много вовлекался в задачи ИТ-сегмента», другой отмечает «не хватает погружения в бизнес» и неспособность «стратегически взглянуть на картинку».

Также 37,5% либо затруднилась с оценкой, либо не взаимодействуют с CISO напрямую. Формулировки «не готов отвечать на вопрос» и «это не в фокусе моего внимания» показывают, что в ряде компаний диалог между CISO и CEO попросту отсутствует.

— CISO — больной вопрос для нас, меняем специалиста уже третий раз, всем не хватает погружения в бизнес. Не видим человека, способного стратегически взглянуть на картинку, сделать стратегический план бюджета, четко уложится в стратегические цели компании.

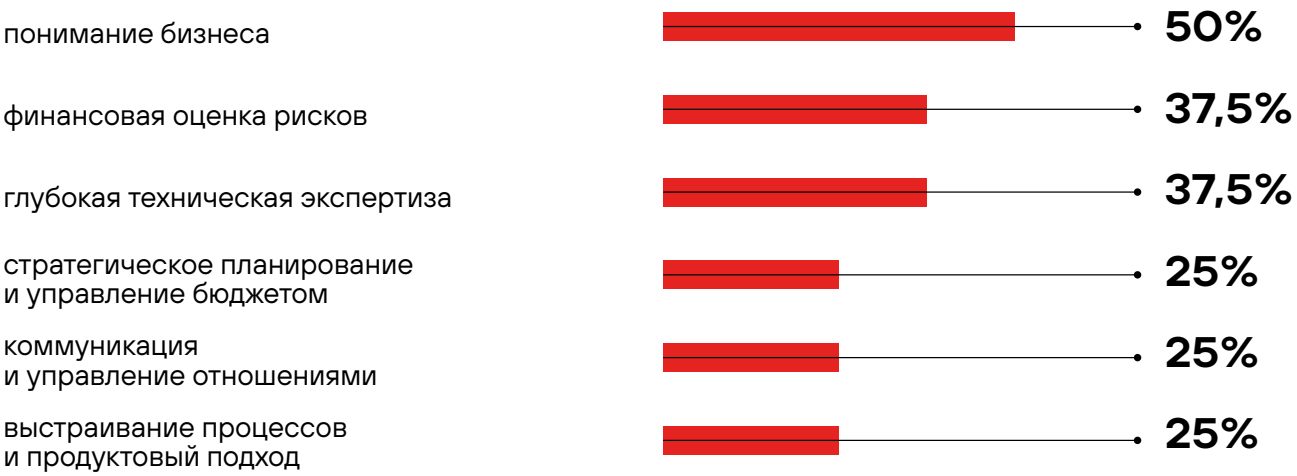
CEO, участник исследования (анонимно)

— CISO должен понимать, что бизнес планирует в плане развития компании, чтобы знать, как построить защиту. Но сейчас его роль — скорее принимать информацию и работать как поддержка. Он должен контролировать ключевые процессы и понимать, какие системы не должны иметь доступ к внешнему контуру.

CEO, участник исследования (анонимно)

В результате выстраивается следующая картина: большинство CEO ждут управленца рисками, встроенного в стратегию и экономику бизнеса. При этом фактическую зрелость CISO в ряде компаний оценивают как «недостаточную». Основные проблемы: недостаток стратегического мышления, низкая интеграция в бизнес и неспособность переводить киберриски в финансовые показатели. Техническая экспертиза оценивается высоко.

Ожидания CEO от CISO*



*Респонденты могли указывать несколько компетенций, поэтому сумма процентов превышает 100%.

CTO И CIO ПРО CISO: НОСИТЕЛЬ ИНЖЕНЕРНОЙ ЭКСПЕРТИЗЫ И ПАРТНЕР

Опрошенные нами CTO (технические директора) и CIO (директора по информационным технологиям), формулируя ожидания от CISO, начинают с технической базы. У 60% опрошенных звучат формулировки «понимание и способность защищать периметр», «техническая защита периметра», «сильные инженеры», «инструменты маскирования, безопасная разработка». CISO прежде всего носитель инженерной экспертизы, способный выстроить защиту на уровне инфраструктуры, разработки и сетевого периметра.

При этом больше половины респондентов (60%) добавляют, что важно понимать процессы и бизнес-контекст конкретной компании. Один из спикеров формулирует: «безопасность рассматривается с точки зрения бизнес-эффективности и адекватной оценки рисков».

Еще один повторяющийся мотив касается стиля взаимодействия и командной работы: «умение работать с командой», «самостоятельно закрывать минимальный консалт по безопасности», «быстрое погружение». Для технических и ИТ-директоров CISO — работник технологического блока, который понимает ИТ-ландшафт, но при этом говорит на языке инженеров и может донести их ожидания до бизнеса.

КАК CTO И CIO ОЦЕНИВАЮТ CISO

Картина оценки у CTO и CIO значительно более позитивна, чем у CEO — 80% опрошенных дают высокую оценку: «Это партнер, с которым я в равноправном диалоге», «Оцениваю текущие навыки как очень высокие». Лишь пятая часть (20%) респондентов фиксировала дефицит понимания бизнес-процессов и говорила о «слишком стандартном подходе».

Среди CTO и CIO в большинстве случаев CISO воспринимается как технологический партнер, способный обеспечивать устойчивость периметра, развивать DevSecOps и участвовать в стратегическом диалоге. Восприятие здесь заметно отличается от оценки CEO и демонстрирует более высокий уровень доверия. Один из CIO подчеркивает значимость «собственного высокоуровневого взгляда» и умения формулировать задачу «на языке бизнеса: что и зачем собираешься делать».

Анатолий Шипов

управляющий директор, Сбертех

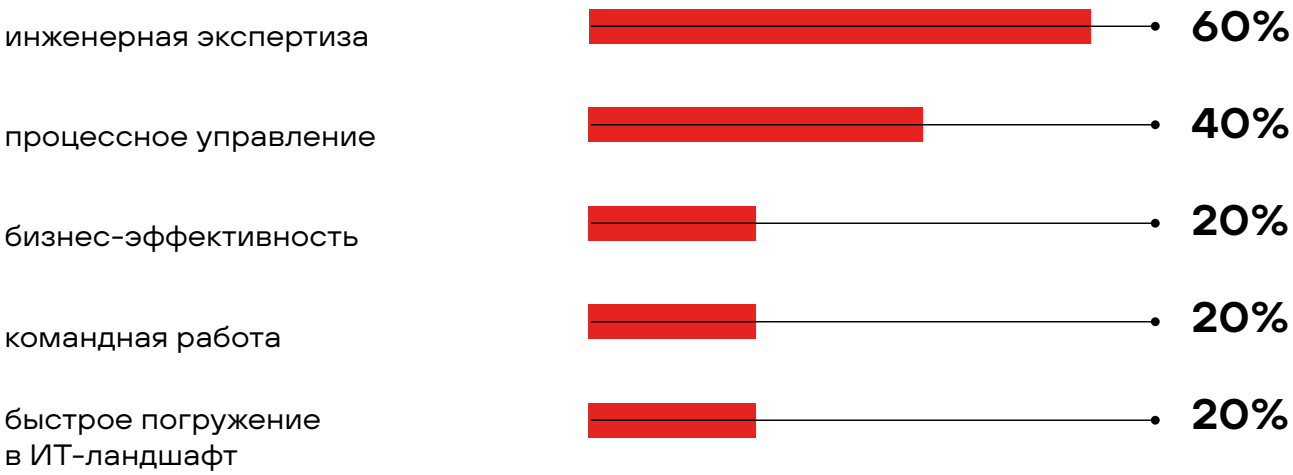
— **Для меня важно, чтобы CISO был не только про безопасность, но и хорошо понимал бизнес. Я на практике вижу примеры, когда CISO генерирует идеи и гипотезы, которые напрямую влияют на рост выручки компании.**

Сергей Путятинский

вице-президент по операционной деятельности и информационным технологиям ФГ БКС

— Конечно, CISO должен участвовать в стратегическом диалоге. Бюджеты на ИБ растут, их нельзя считать на уровне погрешности. Здесь мы управляем вероятностной функцией, а с другой стороны — это вполне конкретные деньги и важно определить границу между адекватным инвестированием в вероятностные события. Следовательно CISO должен уметь коммуницировать на уровне топ-менеджмента в рамках стратегических сессий.

Ожидания CTO/CIO от CISO*



*Респонденты могли указывать несколько компетенций, поэтому сумма процентов превышает 100%.

CISO ПРО CISO: РОСТ ОТВЕТСТВЕННОСТИ И РАСШИРЕНИЕ ФУНКЦИЙ

В ответах CISO ключевым рубежом изменения роли почти повсеместно выступает 2020 год и последующие регуляторные изменения. Сразу 36,7% респондентов связывают повышение своей роли в компании с импортозамещением, ужесточением законодательства, ростом числа атак и появлением новых требований государства. Звучат формулировки «КИИ всё поменял», «250-ФЗ сильно поменял ландшафт», «ужесточение законодательства», «появилось большое количество регуляторных требований», «нужно знать рынок импортозамещения», «нельзя пользоваться ничем нерусским, нужно разрабатывать самостоятельно». Также треть (33,3%) CISO сказали, что в последние годы их задачи стали скорее бизнесовыми. Еще 20% отметили рост количества атак и угроз.

Все те же 36,7% опрошенных нами отметили, что их статус и значимость внутри компании выросли. Ответы варьируются от «роль выросла кардинально» и «CISO стал замгендиректора» до «генеральный директор озвучил важность кибербезопасности на уровне совета директоров», «роль сместилась от исполнения нормативных требований к выработке рекомендаций для бизнеса», «стали ожидать решений более высокого уровня». У части CISO появились многолетние бюджеты и прямой диалог с генеральным директором компании.

Еще 13% опрошенных говорят о переходе от бумажной безопасности к реальной ИБ. Формулировки звучат жестко: «уже прекратили ждать дежурную пятую точку», «рынок перешел к реальной ИБ», «раньше KPI измерялись временем обнаружения, сейчас максимум три минуты простоя банка». Другие подчеркивают, что роль стала «менее бумажной», более «суверенной», с акцентом на совместные OKR и KPI с бизнесом.

Кстати, 23,3% респондентов фиксируют, что ожидания принципиально не изменились или изменились умеренно: «моя роль не сильно поменялась», «чего ждали, то и реализовалось», «ожидания те же, бюджеты меньше».

САМООЦЕНКА КОМПЕТЕНЦИЙ: ВЫСОКАЯ ПЛАНКА И ЭФФЕКТ УВЕРЕННОСТИ

Почти половина CISO (43,3%) оценивают себя высоко — на уровне 8–10 баллов или в сопоставимых формулировках. Прямые оценки звучат так: «10 из 10, поэтому и пошел в операционку». Один из участников подчеркивает, что его компетенции «выходят за рамки CISO на общее управление ИТ». Другой говорит о себе как об «ученом в ИБ» с собственной методологией оценки рисков и считает себя «одним из лучших».

Что интересно, ровно столько же респондентов (43,3%) не дали прямой оценки или уклонилась от ответа. Лишь 13,4% опрошенных демонстрируют умеренную самокритику. Один оценивает себя на 3 из 5, чтобы сохранить стимул к росту, другой упоминает разрыв в части MBA и понимания управленческой линейки.

> — **После 2020 года к моей роли появилось больше доверия, а мое влияние внутри компании возросло. Генеральный директор устно всем членам совета директоров озвучил важность инфобезопасности, появились отдельные приказы и диалог с бизнесом стал лучше. Но теперь чаще спрашивают о результатах.**
>
> CISO, участник исследования (анонимно)

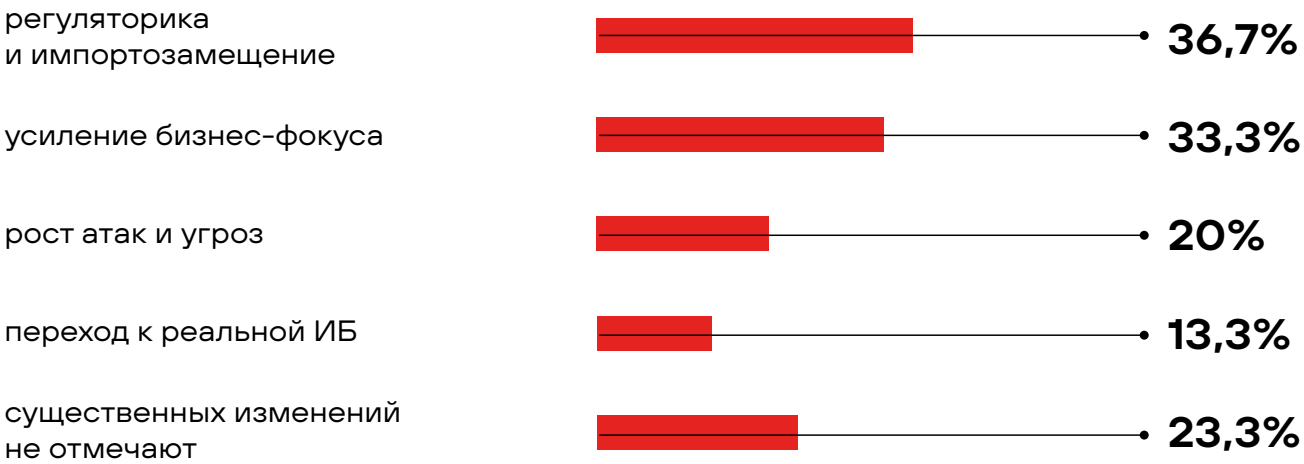
В совокупности картина демонстрирует выраженную уверенность в собственных компетенциях у значительной части CISO, особенно среди тех, кто работал в условиях значительного роста числа атак на компанию.

Алексей Волков

вице-президент
по информационной
безопасности, «Билайн»

— Безопасность перестала быть дополнительной услугой, сейчас это полноценная часть архитектуры любого сервиса или продукта, основной критерий его качества и надежности. Роль CISO перешла от технической функции «галочки» к стратегическому управлению бизнес-рисками, в технологически зрелой компании ИБ — это горизонтальная функция, пронизывающая все процессы. Иными словами, CISO теперь оценивают по тому, насколько он помогает бизнесу расти, быстро восстанавливаться после сбоев и отраженных атак, принимать взвешенные управленческие решения в условиях неопределенности и сохранять доверие рынка.

Какие факторы повлияли на изменение роли CISO*



*Респонденты могли указывать несколько компетенций, поэтому сумма процентов превышает 100%.

ВЫВОД: ТРИ МНЕНИЯ, КОТОРЫЕ НЕ СХОДЯТСЯ

Картина складывается противоречивая. CEO хотят видеть CISO как стратега, который умеет считать риски в деньгах и встроен в бизнес. При этом половина из них либо затрудняется оценить своего директора по информационной безопасности, либо не контактирует с ним напрямую. Общая оценка находится на уровне «слабо» или «недостаточно». Проблема, с точки зрения руководителей бизнеса, одна: **CISO слишком погружен в технику и слабо понимает бизнес.**

Технические директора оценивают CISO гораздо выше. Большинство CTO воспринимает их как равноправных участников технологического диалога. Для технических директоров это партнер, который обеспечивает защиту периметра, решает сложные задачи и говорит на понятном инженерам языке.

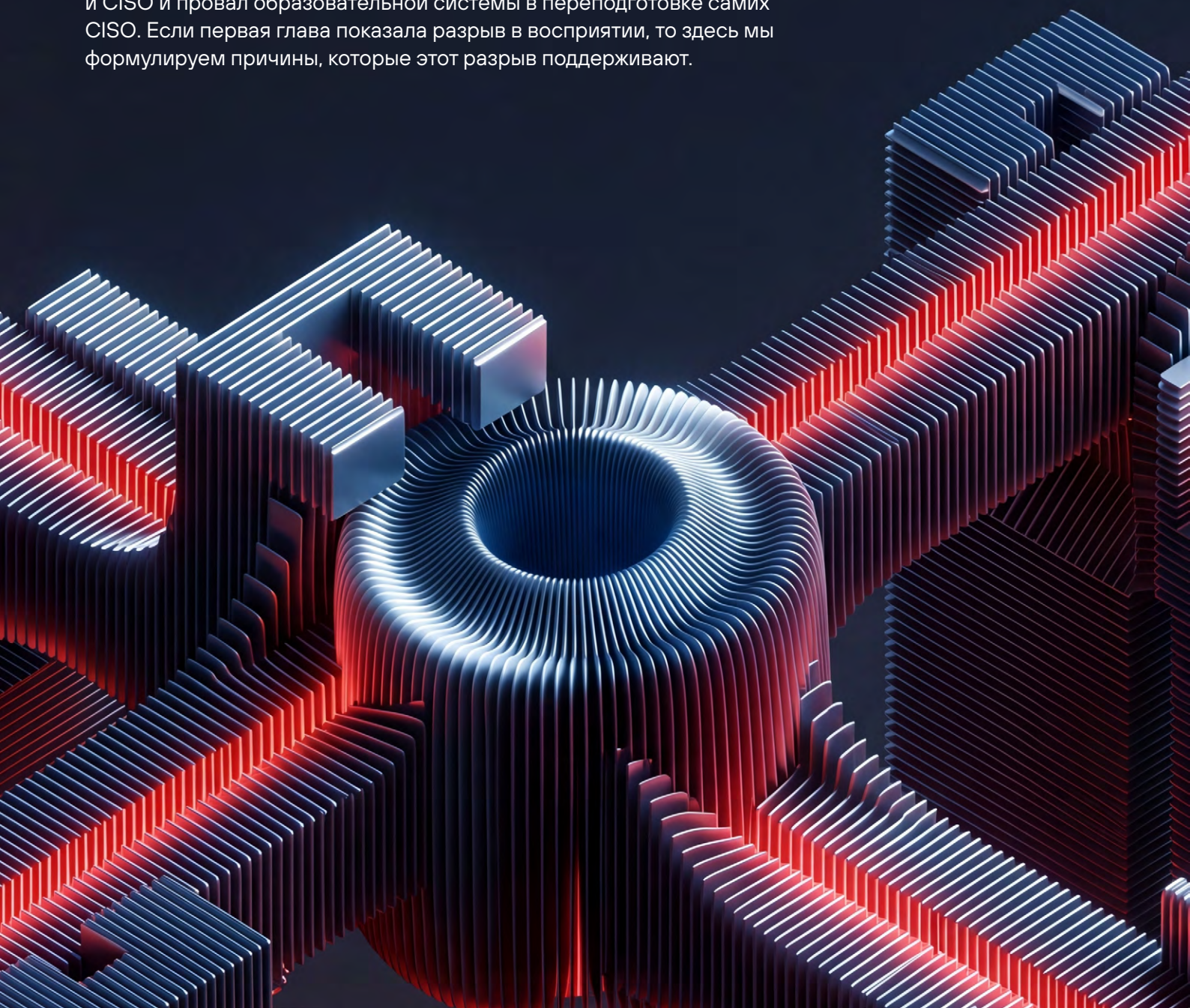
Сами CISO оценивают себя очень высоко. Больше половины ставят себе 8–10 баллов, часть отмечает, что их задачи выходят за пределы роли директора по информационной безопасности. Они говорят о росте расширении полномочий и смещении роли к стратегическим задачам.

Разрыв очевиден. Руководители компаний оценивают CISO ниже, чем те оценивают себя. Технические директора довольны своими коллегами, потому что видят в них своих технических партнеров. Часть CISO уверены, что их роль вышла на стратегический уровень, но первые лица компаний этого роста не видят. Этот разрыв восприятия создает почву для конфликтов, недопонимания и проблем во взаимодействии. Руководители ИБ застряли в своем информационном пузыре, где они управленцы высокого уровня, а бизнес-руководство остается в бизнес-ориентированной парадигме, где CISO лишь технический специалист, который плохо переводит технические риски в финансовые последствия.

ГЛАВА 2

ПОЧЕМУ МОСТ НЕ ПОСТРОЕН? ТРИ БАРЬЕРА НА ПУТИ К БИЗНЕС-ПАРТНЕРСТВУ

Во второй главе мы разбираем, почему директор по информационной безопасности во многих компаниях до сих пор не стал полноценным бизнес-партнером. Ниже описаны три системных барьера, которые повторяются от компании к компании: разрозненные метрики эффективности и результативности, разный язык общения CEO и CISO и провал образовательной системы в переподготовке самих CISO. Если первая глава показала разрыв в восприятии, то здесь мы формулируем причины, которые этот разрыв поддерживают.



БАРЬЕР 1: КАЖДЫЙ СЧИТАЕТ ПО-СВОЕМУ

Если задать десяти CISO вопрос о ключевых метриках, которые они выносят на уровень руководства, можно получить десять разных ответов.

Одни фокусируются на риск-ориентированной повестке, представляя «дашборд с приоритизированными ключевыми рисками». Другие структурируют отчетность вокруг сводных показателей — «риски, инциденты, статус ключевых инициатив». Третьи делают акцент на операционных и технических метриках, демонстрируя «масштаб инфраструктуры и уровень покрытия средствами защиты». Наконец, часть руководителей стремится агрегировать состояние функции в интегральный показатель зрелости — «одну цифру по результатам аудита».

Часть CISO стремится говорить с бизнесом на языке экономики, связывая безопасность с финансовыми показателями: «влияние на P&L», «потенциальные потери и издержки», «регуляторные штрафы», «стоимость ошибки», «возврат на инвестиции».

Другая часть сохраняет фокус на операционно-технической повестке, оперируя такими категориями, как «инвентаризация активов», «объекты защиты», «полнота логирования», «пентесты и уязвимости», «SLA и время реагирования».

При этом внутри профессионального сообщества отсутствует единый взгляд на то, какие из этих метрик релевантны для уровня топ-менеджмента. Часть руководителей считает, что избыточная детализация и технические показатели не только не создают ценности для бизнеса «рассказывать CEO про среднее время обработки запроса на первой линии SOC — это полный буллшит», но часть говорят о том, что стейкхолдерам стало интересно вникать вглубь ИБ-повестки.

Многие CISO признаются, что универсального отчета для топ-команды у них нет. Звучат формулировки «с разным срезом информации иду к разным людям», «для каждого стейкхолдера по-разному», «зависит от того, какие метрики человек хочет видеть». Но в итоге, резюмируют опрошенные: «Нет единого отчета, полезного каждому» — поскольку отчет адаптируется под задачи и язык каждой функции.

Полина Кухто

проектный менеджер специализации «Технологии», The Edgers

— **Более 60% опрошенных нами CISO на вопрос «как безопасность уже помогла компании заработать?» называли как косвенные способы заработка: «повысили продажи продукта благодаря повышению уровня безопасности», «получили важную сертификацию», так и прямые «начали продавать внутреннюю ИБ-платформу». Остальные описывают экономический эффект через снижение потерь и расходов, например, сокращение фрода. Несколько человек отмечают, что модель «ИБ как бизнес» работает в основном в ИТ и продуктовых компаниях. А самая частая формулировка звучит просто: «Сэкономил — заработал»**

Первые лица компаний смотрят на эту картину и признают проблему. Из опрошенных нами CEO лишь небольшая часть (12,5%) высоко оценивает способность своего CISO обосновать экономическую ценность безопасности, один спикер оценил своего директора по информационной безопасности в «8–10 баллов по десятибалльной шкале». И, напротив, львиная доля руководителей (87,5%) фиксируют слабую способность к обоснованию. Самые распространенные ответы: «не умеет объяснить, что и на что повлияет», «часто говорят общими лозунгами», «нет, не умеет». Еще один CEO описывает, что коммуникационные задачи на себя берет CIO.

Технические директора, как правило, мягче оценивают работу CISO. Они глубже понимают ограничения работы с вероятностными моделями: «на вопрос в духе «если бы потратили на сто рублей больше, предотвратили бы инцидент?» в реальности невозможно ответить прямо».

Часть CTO высоко оценивают коммуникационные навыки CISO: «по софт-скиллам это часто 9–10 из 10», «умеют говорить с бизнесом и договариваться», и одновременно подчеркивают сложность перевода рисков в деньги: «чтобы за один день посчитать все риски в денежном выражении, нужно глубоко понимать бизнес-процессы», «без этого любые цифры будут условными».

В итоге многие отмечают, что текущая практика остается ограниченной: «большинство CISO не дают бизнес-метрик», «говорят на уровне имеющихся систем и инструментов», «до полноценной связки с бизнесом доходят немногие».

Около 70% CISO в той или иной степени стремятся привязывать метрики к бизнес-показателям, однако «единого формата отчетности» возникнуть не может – в силу разницы специфик компаний и индустрий. При этом, как сформулировал один из опрошенных нами CISO: «История с тем, чтобы делиться метриками информационной безопасности с бизнесом — тупиковая. Я считаю, что количество отраженных или обнаруженных атак важны лишь как внутренние метрики ИБ. ИБ стремилась стать бизнес-ориентированной, а в итоге наоборот отгородилась».

БАРЬЕР 2: КИБЕРБЕЗОПАСНОСТЬ И БИЗНЕС ГОВОРЯТ НА РАЗНЫХ ЯЗЫКАХ

В ответах CISO рефреном звучит оценка: взаимодействие с бизнесом улучшается, если удается перейти с технического диалекта на язык руководителей. Примерно у 50% спикеров прямо звучит слово «язык»: «говорить на одном языке», «объяснить просто», «переводить с «птичьего» на русский».

При этом часть опрошенных подчеркивает, что с топами не дает результата как разговор на уровне «технических аббревиатур», так и на уровне «обсуждения угроз». Один из CISO формулирует предельно прямо: «Разговор об угрозах - это чистая бюрократия. CEO не понимают «пугалок», особенно в российском бизнесе, где высок уровень риск-аппетита. Нужно объяснять языком бизнес-драйверов, показать, как потраченные деньги отразятся на доходе компании». Многие CISO упоминают, как важно встраиваться в управленческий ритм: ежемесячные и квартальные, годовые доклады на правлении, совете директоров, бизнес-департаментами.

В чем сходятся опрошенные CISO — безопасность должна помогать бизнесу, а не тормозить его: «бизнес на первом месте», «ты не контролер и не охранник», «цель не блокировать инициативы, а помогать их реализовывать безопасно». Один из участников описывает свое правило: в разговоре с бизнесом не говорить «нет», а искать безопасный способ сделать то, что нужно компании.

Олег Волков

директор департамента кибербезопасности, банк «Зенит»

— За три месяца я написал стратегию с фокусом на развитие бизнеса и роль доверенного защитника. Это была наша цель — не мешать бизнесу, а прийти к принципу врожденной безопасности. Тогда же я ввел требование в ИБ, не говорить бизнесу «нет», а изучать вопрос и предлагать альтернативы, как сделать безопасно.

Без общих определений разговор не идет, поэтому часть CISO пытаются сформулировать общий с бизнесом словарь: «Мы определили недопустимые события, риски. Через эти призмы оцениваем все инициативы бизнеса». Еще один спикер говорит — важно договориться, что вообще такое риск, потому что «все понимают это по-разному».

CEO подтверждают эту картину. Они хотят от CISO «трансляцию технических концепций на языке бизнеса», «умение обосновывать инвестиции с точки зрения бизнес-ценности», «понимание бизнес-процессов». Также встречаются формулировки «взгляд предпринимателя» или «смотреть через призму выручки». Но по сути это один и тот же запрос: CISO должен овладеть новым языком, то есть научиться переводить технические риски в понятные бизнесу последствия и деньги.

Дмитрий Папин

CEO iiko

— Мы убедились на практике, что без участия CISO стратегическое планирование не работает. Иначе у других менеджеров может не хватать понимания рисков и сложности их митигации, а у CISO— понимания целей бизнеса и наших ожиданий. Чтобы мне, как CEO, не приходилось управлять этим процессом на ежедневной основе, мы разрабатываем стратегию совместно.

БАРЬЕР 3: СИСТЕМА ОБУЧЕНИЯ НЕ УСПЕЛА ЗА РЫНКОМ

Редкий для этого исследования случай, когда CEO, CTO и сами CISO оказались солидарны. По их мнению, специализированные программы по кибербезопасности в нынешнем виде неспособны помочь CISO.

Среди CEO узнаваемость таких программ минимальна. Большинство опрошенных руководителей на вопрос «Вы слышали о программах обучения по кибербезопасности?» отвечали «нет» либо говорили «слышу много, но не откладывается в голове». Один из спикеров проходил внутреннюю программу по кибербезопасности по требованию банка, другой отмечает, что его CISO развивается в рамках общей корпоративной модели, однако про специализированное развитие компетенций не в курсе.

У технических директоров оценки резче. Часть прямо говорит, что специализированных курсов для CISO в стране практически нет. Один формулирует жестко: «курсы для CISO — проблема, потому что всё выглядит как игра в бирюльки». Другой описывает впечатление от услышанного на курсе как «кровь из глаз», указывая на отсутствие доверия к преподавателям. Но встречается и чуть более содержательная критика: CISO часто слабо ориентируются в современном ИТ-стеке, облачной архитектуре, финансах и рисках, а существующие программы этот разрыв не закрывают.

Сами CISO видят подобные программы неоднозначно. Часть опрошенных говорят, что у них сильная инженерная база, есть международные сертификаты, Executive Education в бизнес-школе INSEAD. Другие сознательно дистанцируются от форматов «MBA для CISO», называют их в высшей степени бессмысленными. Встречалось и такое наблюдение: «CISO учиться у CISO бесполезно», поскольку «ценность дает кросс-доменное обучение и выход за пределы собственной функции».

Все респонденты сходятся в одном: современный российский рынок предлагает программы, заточенные под нормативные базы и конкретных вендоров, без общей картины и принципов. Системной программы, которая одновременно давала бы риск-ориентированный подход, навыки приоритизации ИБ-инициатив и понимание бизнес-процессов, участники исследования не встречали. Главная проблема всё та же — технологии редко переводят на язык бизнеса так, чтобы руководители ясно понимали, что именно происходит и как это влияет на их решения. Учиться подобному на системной основе сегодня практически негде.

Александр Лимонов

Независимый эксперт и ex CISO Леруа Мерлен

— **Периодически прохожу курсы, в основном зарубежные. Российский рынок обучения тоже мониторю, но он пока уступает зарубежным аналогам: многие программы сосредоточены на нормативных требованиях и их интерпретации. При этом не хватает системных образовательных программ, которые помогали бы не только понимать требования, но и выстраивать приоритеты, делегирование и контроль в ежедневной управленческой практике. Риск-ориентированный подход как целостная управленческая модель в обучении представлен слабо. У Positive Technologies, например, есть концепция недопустимых событий, но я бы рассматривал ее как более узкий взгляд на тему, а не полноценное обучение риск-ориентированному подходу.**

В итоге картина складывается следующая: сейчас российский EdTech и система образования предлагают различные форматы обучения, однако рынку нужны директора по информационной безопасности, которые одновременно понимают модель киберрисков, ИТ-архитектуру и умеют объяснять совету директоров, сколько стоит та или иная угроза для бизнеса. Ни вуз, ни программы дополнительного профессионального образования ничего подобного еще не предложили. Экспертиза формируется точечно, через личный опыт, самообразование, менторство и постоянную работу.

ВЫВОД: ТРИ БАРЬЕРА, КОТОРЫЕ ВЛИЯЮТ НА РАЗРЫВ В ВОСПРИЯТИИ РОЛИ CISO

В этой главе мы увидели три причины, по которым безопасность остается на периферии управленческого мышления.

Первое — разрыв в метриках. У каждого CISO собственный набор цифр, свой формат отчета и логика презентации. Кто-то считает ROI и влияние на P&L, кто-то показывает зрелость функции через сравнение с конкурентами или покрытие инфраструктуры средствами ИБ, общего формата измерения безопасности рынок не выработал.

Вторая причина — трудности перевода. CISO уже поняли, что разговор про уязвимости и аббревиатуры топ-менеджменту мало что дает, поэтому они учатся новому языку: объяснять работу в таких терминах, как деньги, последствия и влияние на репутацию компании.

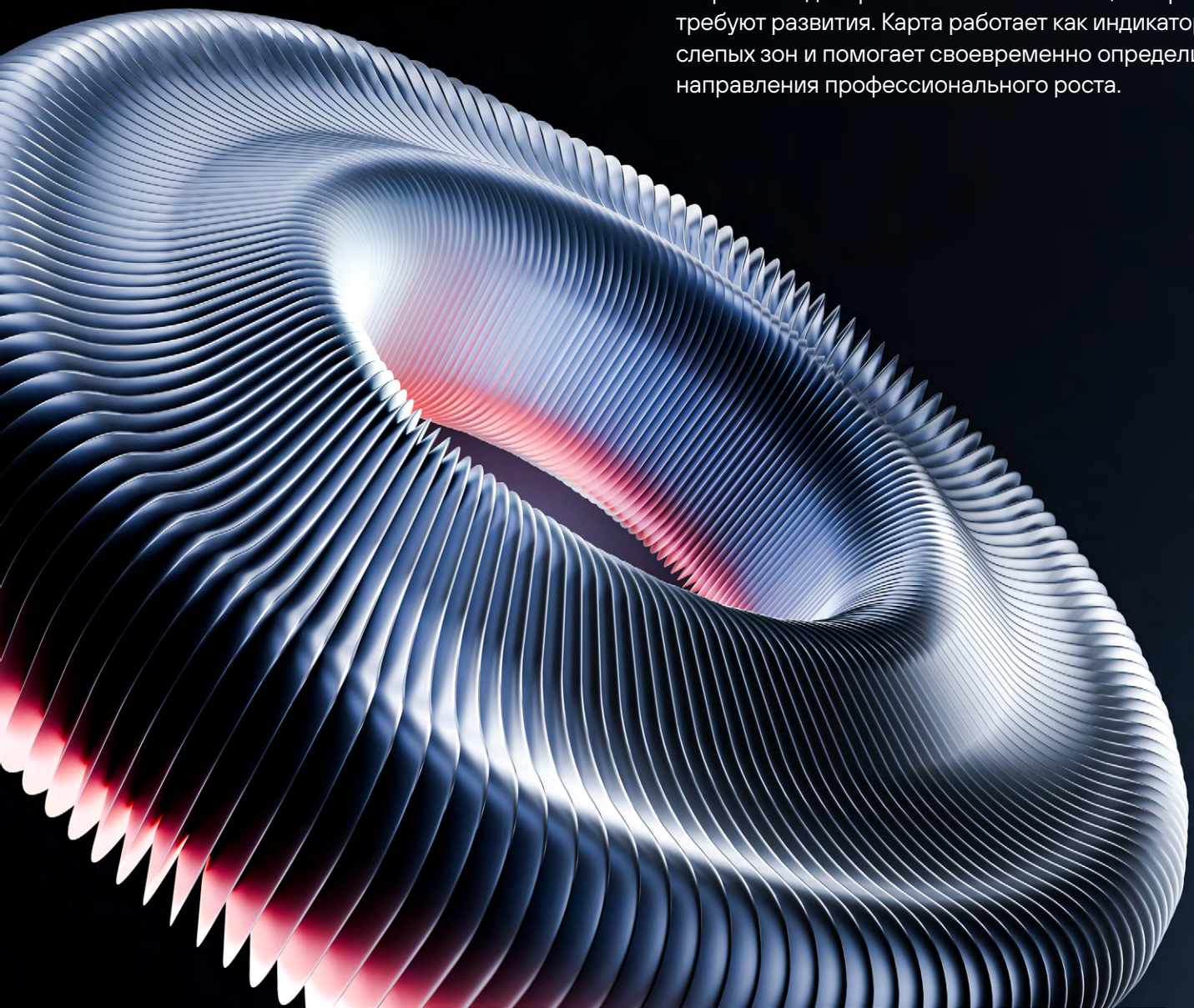
И третье — ограниченность образовательной среды. Современные программы обучения фокусируются на нормативной базе и продуктах конкретных вендоров, поэтому лидерам ИБ приходится формировать свои управленческие компетенции через личный опыт, менторство и самостоятельное изучение финансовых моделей. Целостной программы, которая напрямую связывает стратегию развития компании, цели и ключевые бизнес-процессы с обеспечением киберустойчивости их функционирования и позволяет демонстрировать это через объективные и понятные метрики для бизнеса, участники исследования не встречали.

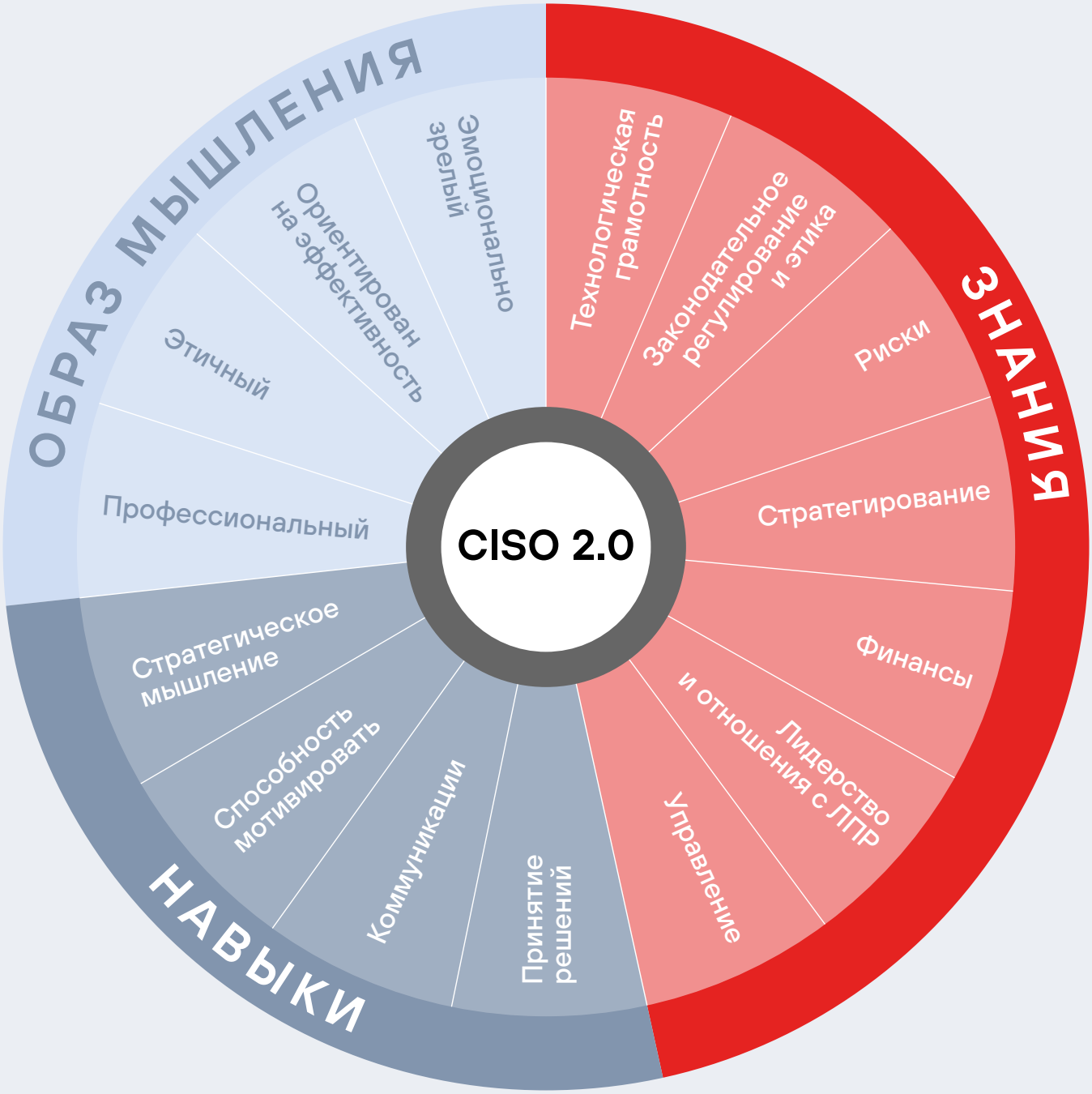
ГЛАВА 3
ПРОФИЛЬ CISO 2.0

В предыдущих главах мы зафиксировали проблему и причины ее появления. Третья глава отвечает на вопрос: какие компетенции нужны CISO, чтобы стать бизнес-партнером. Мы проиллюстрируем это с помощью карты компетенций, построенной по аналогии с международной моделью компетенций члена совета директоров, используемой «Ассоциацией независимых директоров» — поскольку задачи CISO включают выстраивание диалога с бизнесом, обоснование инвестиций и обеспечение стабильности ключевых процессов, а значит, требуют сопоставимого уровня управленческого и стратегического мышления. Карта включает три блока: «Знания», «Навыки» и «Образ мышления».

Предложенная карта компетенций представляет собой один из возможных способов описания роли современного CISO. В разных компаниях баланс между знаниями, навыками и образом мышления может различаться, на него влияют отрасль, стадия развития бизнеса, уровень цифровизации и место кибербезопасности в управленческом контуре. При этом комплексный подход, основанный на синергии всех трех блоков компетенций, формирует основу для выхода CISO на уровень полноценного участника управленческой команды и стратегического диалога.

Предложенный круг компетенций удобно использовать как инструмент самооценки. Он позволяет увидеть собственные сильные стороны и одновременно выявить зоны, которые требуют развития. Карта работает как индикатор слепых зон и помогает своевременно определить направления профессионального роста.




CISO 2.0
ЗНАНИЯ
Технологическая грамотность
Законодательное регулирование и этика
Риски
Стратегирование
Финансы
Лидерство и отношения с ЛПР
Управление
НАВЫКИ
Принятие решений
Коммуникации
Способность мотивировать
Стратегическое мышление
ОБРАЗ МЫШЛЕНИЯ
Профессиональный
Этичный
Ориентирован на эффективность
Эмоционально зрелый

ЗНАНИЯ

Технологическая грамотность	Понимает технологический стек систем и средств защиты, их влияние на специфику инфраструктуры и бизнеса компании, понимает актуальные цифровые инструменты и новые технологии, их влияние на инновации и развитие организации. Обеспечивает и повышает киберустойчивость и защищенность активов в соответствии со стратегическими решениями по развитию организации
Законодательное регулирование и этика	Понимает законодательное регулирование и этические принципы, принятые на уровне государства и транслируемые топ-менеджментом. Видит их влияние на киберзащищенность организации
Риски	Понимает корпоративное управление рисками как единый подход, включая риск-культуру, риск-аппетит и роль риска в росте и создании ценности, встраивает процессы управления киберрисками в корпоративную среду
Стратегирование	Знает как устроен стратегический процесс развития бизнеса и обеспечивает устойчивость компании, встраивая безопасность в стратегию
Финансы	Понимает взаимосвязь и влияние киберустойчивости на финансовую надежность организации, знает как оценить возврат инвестиций в обеспечение непрерывности бизнеса
Лидерство и отношения с ЛПР	Знает, как обеспечивать эффективное лидерство, выстраивать отношения со стейкхолдерами и развивать стратегически согласованную культуру, основанную на ценностях
Управление	Погружен в принципы корпоративного управления и встраивает кибербезопасность в достижение корпоративных целей, обеспечивая эффективную и устойчивую деятельность

НАВЫКИ

Принятие решений	Принимает решения, в том числе в ситуации неопределенности и недостатка информации, опираясь на данные и учитывая риски в контексте стратегии организации и бизнес-юнита
Коммуникации	Оказывает влияние через построение прочной сети отношений как внутри организации, так и за ее пределами. Умеет слушать и коммуницировать, адаптируя стиль коммуникации под задачи, аудиторию, ситуацию
Способность мотивировать	Способен мотивировать и вдохновлять собственную команду и сотрудников организации. Демонстрирует гибкость в ситуации изменений и киберкризисов, конструктивно взаимодействует в сложных и конфликтных ситуациях
Стратегическое мышление	Смотрит на функцию кибербезопасности с точки зрения перспектив бизнеса, выходя за рамки насущных проблем и собственной сферы экспертизы, предвосхищает будущие сценарии и вызовы, видит возможности и угрозы, предлагает альтернативные решения для руководства

ОБРАЗ МЫШЛЕНИЯ

Профессиональный	Поддерживает профессиональный уровень свой и команды, инвестирует время в развитие себя и команды, ответственно относится к собственной роли. Отстаивает интересы бизнес-юнита и организации
Этичный	Задает пример высоких стандартов этики в подходах и поведении для обеспечения киберустойчивости организации. Участвует в установлении правил и принятии решений по чувствительным вопросам — предоставлению доступа, раскрытию информации, контролю операций и эскалации санкций при инцидентах на разных уровнях компании. В этих ситуациях действует, опираясь на корпоративные стандарты, законодательство и принципы этики. Идентифицирует и раскрывает конфликты интересов для их корректного разрешения
Ориентирован на эффективность	Задает высокие стандарты эффективности, фокусируется на целях и приоритетах бизнеса и обеспечении его непрерывного функционирования. Идентифицирует недопустимые события в области кибербезопасности и новые возможности
Эмоционально зрелый	Осознает и контролирует собственные эмоции и модели поведения, проявляет эмпатию к чувствам и реакциям других людей

ВЫВОД: CISO 2.0 ЭВОЛЮЦИОНИРУЕТ ОТ ТЕХНИЧЕСКОГО ЭКСПЕРТА К СТРАТЕГИЧЕСКОМУ ПАРТНЕРУ

Сейчас у большинства CISO есть несколько барьеров, которые проявляются во время общения с топ-менеджментом — особенно когда нужно обосновать и защитить инвестиции в цифровую безопасность.

Один из ключевых барьеров — язык. Во≈взаимодействии с топ-менеджментом директора по информационной безопасности часто используют профессиональный «птичий язык»: нормативные требования, специализированные термины, аббревиатуры и перечни уязвимостей. Для CEO зачастую подобные аргументы звучат как техническая детализация, оторванная от бизнеса или слабо с ним связанная.

Не все понимают, что компетенции CISO давно вышли за пределы технологий. Понимание бизнес-процессов, логики прибыли, финансовой диагностики и стратегических приоритетов компании сегодня не менее важно, чем техническая экспертиза. Только соединив эти знания, директор по информационной безопасности может по-настоящему встроить киберустойчивость в стратегию развития и участвовать в управленческом диалоге на равных.

И третья проблема в том, что сформировать подобный профиль непросто: сочетание технологической экспертизы, бизнес-мышления и управленческих навыков практически негде получить системно.

Предлагаемая карта описывает новый набор компетенций CISO 2.0. Она показывает, какие знания, навыки и элементы образа мышления формируют современный профиль директора по информационной безопасности. Технологическая экспертиза остается фундаментом профессии, однако роль CISO также включает в себя понимание бизнеса, финансовой логики и стратегического контекста.

ГЛАВА 4

РЕКОМЕНДАЦИИ ДЛЯ КАЖДОЙ СТОРОНЫ

Предыдущие главы зафиксировали расхождение в восприятии роли CISO, три системных барьера и профиль компетенций CISO 2.0, который только начинает формироваться. Теперь мы готовы предложить конкретные рекомендации для каждой из сторон этого процесса, которые помогут сократить имеющийся разрыв.

1. Для CISO — личная дорожная карта трансформации: как целенаправленно развивать бизнес-компетенции и выстраивать диалог с топ-менеджментом.

2. Для CEO — конкретные шаги к выстраиванию взаимодействия с директором по информационной безопасности, которое сегодня либо не работает, либо не происходит вовсе.

3. Для рынка образования — ориентиры того, какие программы нужны индустрии прямо сейчас, чтобы закрыть разрыв между технической экспертизой и управленческими компетенциями.

ДЛЯ CISO: ЛИЧНАЯ ДОРОЖНАЯ КАРТА ТРАНСФОРМАЦИИ

Согласно данным исследования 62,5% CEO не ожидают активного участия CISO в стратегическом планировании компании и видят его роль в контроле рисков с подключением по необходимости, лишь 37,5% прямо говорят о включении в стратегию на раннем этапе. У CTO и CIO картина сопоставимая: 40% ожидают активного участия, в остальных случаях безопасность воспринимается как встроенная технологическая функция. Это означает, что стратегическое присутствие CISO в управленческом контуре в большинстве компаний заранее не закреплено и требует целенаправленных действий со стороны самого директора по информационной безопасности.

Шаг №1:
Поймите ключевые векторы развития бизнеса

Треть руководителей в исследовании заявляют о том, что CISO находится слишком глубоко в технических деталях и не слишком хорошо погружен в вопросы бизнеса. Директор по информационной безопасности должен знать ключевые направления бизнеса компании. Также он обязан понимать стратегические направления развития, включая технологии, которые обеспечивают рост компании, влияют на прибыль и поддерживают развитие организации.

Шаг №2:
Измерьте пользу кибербезопасности в бизнес-показателях

Большинство CISO измеряют успех техническими метриками, и это фундаментальная проблема коммуникации с топ-менеджментом. Количество закрытых уязвимостей, время реакции на инцидент, охват мониторингом событий ИБ — всё это важно внутри функции, но CEO ждет другого.

Совет — необходимо перестать измерять успех кибербезопасности техническими метриками. Переведите свою работу в количественные показатели, понятные на уровне правления: сколько стоит час простоя ключевого сервиса? Какой штраф грозит за утечку персональных данных? Какой финансовый эффект дает снижение вероятности критического инцидента? Если кибербезопасность научится говорить на таком языке — разговор с CEO изменится.

Шаг №3:
Выделите критичные активы, оцените их защищенность и согласуйте приоритеты

У каждой компании есть активы и процессы, от которых напрямую зависит устойчивость бизнеса: клиентские базы, производственные системы, интеллектуальная собственность, цифровые платформы. Для каждого из них нужно определить недопустимые события, оценить текущую степень защищенности и устойчивости, описать финансовые, репутационные и юридические последствия. После чего обязательно согласовать этот список с топ-менеджментом.

Шаг №4:
Постройте регулярный диалог с топ-менеджментом

Безопасность воспринимается как стратегическая функция в том случае, если она встроена в управленческие процессы на регулярной основе: квартальные доклады совету директоров, стратегические сессии, обсуждения при запуске продуктов или выходе на новые рынки. Разовые встречи по запросу CEO работают плохо.

Поэтому заранее определите темы и периодичность таких встреч, говорите на языке денег, бизнеса, стратегии, ценности и обеспечения киберустойчивости: риски в привязке к стратегическим целям, инвестиции в безопасность в привязке к финансовым последствиям.

Шаг №5:
Системно развивайте компетенции

Для CISO критически важно постоянно обучаться из-за стремительного развития киберугроз, появления новых технологий и усложнения нормативных требований. Эффективный директор по информационной безопасности должен совершенствовать как технические навыки, так и управленческие компетенции, чтобы обеспечивать безопасность данных, защиту от атак и непрерывность бизнес-процессов.

В исследовании мы подготовили карту компетенций CISO 2.0, состоящую из трех основных блоков: «Знания», «Навыки» и «Образ мышления» — сверьтесь с ней и честно оцените, где находитесь сейчас. В таком случае вы поймете, какие ваши компетенции требуют усиления, и сможете разработать соответствующий план собственного развития.

Должен ли CISO участвовать в стратегическом планировании

ДЛЯ CEO: КАК ПРАВИЛЬНО ВЗАИМОДЕЙСТВОВАТЬ С CISO

Более 50% опрошенных нами CEO либо затрудняются оценить своего CISO, либо не общаются с ним напрямую и там, где должен идти регулярный стратегический диалог о рисках и ответственности, возникает вакуум. Мы предлагаем четыре конкретных шага, которые помогут выстроить взаимодействие с директором по информационной безопасности и определить его место в компании. Каждый шаг потребует определенных действий, но результат стоит того: CISO перестанет работать вслепую, а вы получите понятные критерии для оценки его эффективности.

Шаг №1: Определите недопустимые события

Существуют конкретные события, которые компания не может себе позволить: остановка производства, утечка данных клиентов, компрометация нового продукта до анонса — каждый бизнес ранжирует этот перечень самостоятельно. Например, в банковском секторе утечка ноу-хау к конкуренту может привести к падению продаж на 50% из-за раздела рынка. А в технологических компаниях появление информации о продукте до официального заявления сильно ударит по продажам.

Создать подобный список для конкретной компании — задача топ-менеджмента бизнеса, в том числе при участии CISO. Последствия оцениваются по нескольким измерениям: финансовые потери, репутационный ущерб, юридические риски. И когда перечень будет готов, оценивать работу собственного CISO станет на порядок проще

Шаг №2: Сформулируйте ожидания явно

Треть руководителей компаний в нашем исследовании фиксируют, что CISO «не видел рисков и слишком много вовлекался в задачи ИТ-сегмента», другие отмечают «не хватает погружения в бизнес» и неспособность «стратегически взглянуть на картинку». Это масштабная проблема, например в исследовании Института изучения мировых рынков (Росконгресс, июнь 2025) лишь 40% CEO компаний сказали, что их директор по информационной безопасности достаточно вовлечен в бизнес-процессы. Успешные примеры интеграции встречаются в технологических компаниях, где специалисты по безопасности изначально вовлечены в бизнес: «Он активно участвует в проектах, понимает бизнес-цели и свое место в компании».

Большинство руководителей ждут от CISO умения управлять размером риска и трейд-оффами, находить баланс между затратами и уровнем риска, делать cost-benefit анализ. Звучат формулировки «трансляция технических концепций на языке бизнеса», «умение обосновывать инвестиции с точки зрения бизнес-ценности», «понимание бизнес-процессов».

Проблема в том, что эти ожидания редко формулируются явно на старте работы. И вероятно директор по информационной безопасности даже не знает, что теперь он обязан досконально знать бизнес-процессы. Со стороны CEO будет разумным зафиксировать новые требования письменно и заодно обсудить с CISO, что именно от него теперь хотят получать.

Шаг №3:
Скажите, что хотите видеть в метриках

Большинство руководителей получают формализованные отчеты, которые сложно интерпретировать без специальных знаний. Сейчас в России редки случаи, когда компании системно связывают между собой данные кибербезопасности и бизнес-показатели. Согласно тому же исследованию Росконгресса, 63% компаний стремятся оценить экономический ущерб от потенциальных инцидентов, применяя разные подходы: от карт рисков до расчета потерь от простоев.

Отчетность для CEO от CISO должна отвечать на важные для бизнеса вопросы: сколько инцидентов было, сколько из них критических, сколько это стоит в деньгах. Итоговый список метрик должен коррелировать с перечнем недопустимых для компании событий.

Шаг №4:
Встройте CISO в стратегию компании

Половина руководителей компаний в нашем исследовании подчеркивает: CISO должен глубоко понимать бизнес; по их мнению хороший CISO проактивно участвует в стратегическом развитии компании. В то же время, прямой вопрос «Ожидаете ли вы, что CISO будет активно участвовать в стратегическом планировании компании?» внес сумятицу — 60% опрошенных заявили «нет, ни в коем случае», а другие 40% сказали «да, конечно». И радикальность формулировок, и незначительная разница между этими полюсами подсказывают, что у CEO в России нет единого мнения, стоит ли допускать директора по информационной безопасности к стратегическим вопросам.

Практика показывает, что взаимодействие улучшается, когда безопасность становится частью регулярного управленческого цикла: квартальные доклады на совет директоров, доклады в правление, квартальные обзоры с бизнес-департаментами. CISO должен присутствовать на стратегических сессиях, когда обсуждается выход на новый рынок, запуск нового продукта, изменение бизнес-модели. Именно в этот момент, до принятия решения, нужно оценить киберриски и заложить бюджет на защиту.

ДЛЯ РЫНКА ОБРАЗОВАНИЯ: НОВАЯ АРХИТЕКТУРА ПРОГРАММ ПО КИБЕРБЕЗОПАСНОСТИ

Представления о роли кибербезопасности внутри управленческой команды заметно различаются. Незначительная часть руководителей видит в CISO стратегического участника обсуждений, но большинство воспринимают безопасность как технологическую функцию. Это означает, что рынок образования должен предложить разные форматы обучения для разных ролей: для топ-менеджмента — понимание влияния киберрисков на устойчивость бизнеса и действий в киберкризисах, для CISO — развитие навыков взаимодействия с топ-менеджментом.

Направление №1: специализированные программы для членов советов директоров

В компаниях всё чаще появляются члены советов директоров, курирующие вопросы цифровой трансформации и кибербезопасности. При этом системной подготовки для такой роли на российском рынке практически нет. В результате стратегические вопросы безопасности обсуждаются на уровне общих презентаций и отчетов, а у членов совета директоров отсутствует общий понятийный аппарат для оценки рисков, инвестиций и устойчивости цифровой инфраструктуры.

Для этой аудитории необходимы специализированные образовательные программы через профильные ассоциации и профессиональные объединения. В рамках таких программ важно разбирать управленческие вопросы, которые возникают у совета директоров при обсуждении киберрисков и инвестиций в защиту бизнеса:

- сценарии киберинцидентов на уровне компании и их влияние на устойчивость бизнеса
- подходы к оценке ущерба и финансовых последствий атак
- контроль киберрисков на уровне совета директоров
- место директора по информационной безопасности в системе корпоративного управления.

Подобная подготовка формирует у членов совета директоров общий язык для обсуждения цифровых рисков и позволяет оценивать, насколько безопасность встроена в стратегию компании.

Направление №2: короткие практикумы для CEO

Для этой аудитории длинные академические программы работают хуже, чем компактные практические форматы, которые позволяют быстро сформировать общее понимание киберугроз и роли руководства в управлении этими рисками. Практика показывает, что такие программы особенно эффективны в формате совместного обучения топ-менеджеров и директоров по информационной безопасности.

Например, в практико-ориентированной программе Positive Education для российской инфраструктурной корпорации, включающей в свой состав более 30 компаний, обучение прошли 27 топ-руководителей и 24 специалиста ИТ и ИБ из десяти предприятий холдинга. Гибридный формат сочетал управленческий интенсив и кибербитву для специалистов по безопасности, что позволило сформировать единое понимание киберугроз на разных уровнях компании.

В рамках программы участники работали с конкретными управленческими задачами:

- обсуждали влияние киберинцидентов на финансовую устойчивость и непрерывность операций
- разбирали реальные сценарии атак и возможные модели реагирования
- анализировали риски, связанные с развитием новых технологий, включая искусственный интеллект
- обсуждали вопросы лидерства в кризисных ситуациях и интеграцию кибербезопасности в бизнес-стратегию компании

По итогам обучения участники отметили, что формат помог им переосмыслить роль информационной безопасности. Теперь они воспринимают ее как элемент корпоративного управления и деловой культуры компании.

Направление №3: практико-ориентированные программы для CISO

Для самих директоров по информационной безопасности образовательный запрос выглядит иначе. Исторически функция ИБ в компаниях формировалась как обеспечивающая и технологическая. Она редко встроена в проектную логику бизнеса, почти не участвует в создании продуктов и часто воспринимается как элемент инфраструктуры.

Поэтому ключевая образовательная задача для CISO состоит в развитии гибридного набора компетенций. Такой набор включает технологическую экспертизу, понимание бизнес-процессов, навыки стратегического анализа, управление рисками, финансовую аргументацию инвестиций и коммуникацию с топ-менеджментом.

Практико-ориентированные программы для этой аудитории должны строиться вокруг реальных управленческих задач:

- интеграция кибербезопасности в ключевые бизнес-процессы компании
- определение критических активов и недопустимых событий
- подтверждение уровня киберустойчивости на языке бизнеса и финансов
- согласование приоритетов защиты с топ-менеджментом

Такие программы помогают директору по информационной безопасности перейти от роли технического эксперта к роли управленца, который отвечает за устойчивость ключевых направлений бизнеса и способен обсуждать эту устойчивость с топ-менеджментом на понятном для них языке.

ВЫВОД: СЕЙЧАС CISO НА ПОРОГЕ УСКОРЯЮЩЕЙСЯ ЭВОЛЮЦИИ

CISO должны пройти трансформацию. Выход на уровень топ-менеджмента требует нового набора компетенций: понимание бизнес-модели компании, умение переводить киберриски в финансовые последствия, способность участвовать в стратегическом диалоге. Карта компетенций CISO 2.0 показывает, что техническая экспертиза важна, но для работы на уровне управления ее одной недостаточно.

Руководителям компаний необходимо выстроить новую модель взаимодействия с функцией безопасности. Большинство CEO сегодня либо затрудняется оценить своего CISO, либо взаимодействует с ним эпизодически. Кибербезопасность становится элементом корпоративного управления лишь в том случае, когда CISO встроен в обсуждение недопустимых событий, финансовых рисков и стратегических решений.

Рынку образования предстоит закрыть разрыв через новую архитектуру программ для трех аудиторий. Членам советов директоров нужны общий словарь для обсуждения цифровых рисков и инструменты оценки этих рисков на стратегическом уровне. CEO нужны короткие практические форматы понимания киберкризисов и роли руководства в управлении ими. CISO нужны практико-ориентированные программы развития гибридного управленческого набора компетенций: 70% практики, разбор кейсов, симуляции переговоров с CEO, построение финансовых моделей для ИБ-проектов, обучение у опытных CISO и бизнес-тренеров.

Только синхронные изменения на всех трех уровнях способны сократить разрыв. Если CISO продолжат говорить на языке технологий, CEO будет воспринимать безопасность как инфраструктуру, а образовательный рынок останется сосредоточенным на технической подготовке, существующее расхождение сохранится.

ЗАКЛЮЧЕНИЕ

ТРАНСФОРМАЦИЯ НЕИЗБЕЖНА. КТО УСПЕЕТ ПЕРЕСТРОИТЬСЯ?

Сейчас роль CISO проходит фазу трансформации и запрос на изменения возникает сразу с двух сторон: от топ-менеджмента компаний и от самих директоров по информационной безопасности. В условиях лавинообразного роста киберугроз руководители бизнеса всё яснее понимают, что цифровая безопасность напрямую влияет на финансовую устойчивость, непрерывность операций и репутацию компании. Поэтому внутри управленческой команды формируется запрос на круг лиц, принимающих решения и говорящих на общем языке при обсуждении цифровых рисков и киберустойчивости.

Однако этот запрос пока удовлетворяется лишь частично. Наблюдения показывают, что значительная часть директоров по информационной безопасности по-прежнему сосредоточена на операционной стороне работы: поддержании систем защиты и реагировании на инциденты. При этом гораздо сложнее оказывается встроить кибербезопасность в стратегический контур развития компании и убедительно показать топ-менеджменту ценность инвестиций в защиту и их влияние на устойчивость бизнеса.

Ключевым условием становится превращение CISO в бизнес-партнера. Речь идет о роли, которая отвечает на запросы топ-менеджмента и участвует в обеспечении развития компании через повышение ее киберустойчивости и готовности к киберкризисам.

Такая трансформация требует новых компетенций. Современному директору информационной безопасности необходимы навыки работы с новыми технологиями и цифровыми трендами, понимание принципов корпоративного и антикризисного управления, развитые коммуникационные навыки и способность оперировать финансовыми показателями.

Образование становится важным инструментом этой трансформации. Свою роль могут сыграть специализированные образовательные программы, а также обмен опытом и переосмысление практик ведущих управленцев из разных отраслей рынка.

КОМАНДА ПРОЕКТА ИССЛЕДОВАНИЯ

THE EDGERS

Ирина Милехина

Леонид Коен

Полина Кухто

Кирилл Каненков

Степан Туркин

Александра Сулейманова

SUPERJOB

Наталья Ильченко

POSITIVE TECHNOLOGIES

Анастасия Федорова

Ольга Иванова

Андрей Велесюк

Татьяна Жданова

Слава Танцоров

The Edgers × SuperJob × positive education