SGRC

ОТ «ГАЛОЧКИ» К УПРАВЛЕНИЮ КИБЕРУСТОЙЧИВОСТЬЮ

Татьяна КЛЯУС
системный аналитик R-Vision

Валерий ГОРБАЧЕВ
руководитель группы внедрения систем мониторинга АО «ДиалогНаука»

Финансовый сектор традиционно первым сталкивается с новыми киберугрозами и регуляторными изменениями. Банки и страховые компании уже в начале 2010-х осознали, что без системного подхода к управлению безопасностью, рисками и соответствием невозможно обеспечить надежность операций. Так начался путь развития решений, которые сегодня известны как SGRC-платформы (Security Governance, Risk & Compliance). За последние 15 лет они прошли эволюцию от «бумажной безопасности» и формальной отчетности перед регуляторами до полноценного инструмента проактивного управления киберустойчивостью.

ТРАНСФОРМАЦИЯ ПОДХОДОВ

Период начала 2010-х характеризовался преимущественно формальным подходом к информационной безопасности и управлению рисками. Для финансового сектора он зачастую сводился к выполнению минимальных требований регуляторов: исполнению требований 152-ФЗ «О персональных данных» и соблюдению приказов ФСТЭК. Основная задача заключалась в подготовке отчетности для проверок и аудита. Учёт рисков и контролей велся вручную в Excel или в рамках систем электронного документооборота. При этом реальные бизнес-риски оставались в стороне, а безопасность воспринималась как обязанность, а не как управляемый процесс.

С середины десятилетия ситуация изменилась. Центробанк усилил надзор, вступили в силу Положение 382-П, СТО БР ИББС-1.0–2014, новые ГОСТ 57580.1–2017 и ГОСТ 57580.2–2018. Банки вынуждены были систематизировать процессы и искать автоматизацию. Так появились первые российские SGRC-системы. Одно из их преимуществ заключалось в наличии встроенной нормативной базы и методик отечественных регуляторов. Например, R-Vision SGRC позволяет сразу работать с актуальными требованиями нормативной базы и встраивать их в процессы без длительной адаптации.

Пандемия, массовый переход на удаленные каналы обслуживания и ускоренная цифровизация банковских сервисов резко увеличили нагрузку на ИТ и ИБ-подразделения. Количество киберугроз многократно возросло, одновременно усиливались и регуляторные требования: был выпущен ряд Положений Банка России, устанавливающих требования к обеспечению защиты информации для финансовых организаций, утверждены документы, регулирующие управление операционными рисками — Положение 716-П и стандарты ГОСТ 57580.3–2022 и ГОСТ 57580.4–2022.

Сегодня SGRC перестал восприниматься исключительно как комплаенс-инструмент и становится частью стратегии цифровой устойчивости. Компании постепенно переходят к риск-ориентированному подходу: оценивают не только факт инцидента, но и его бизнес-последствия. Фокус смещается от обеспечения соответствия к управлению устойчивостью бизнеса, и системы SGRC как раз становятся тем ядром, вокруг которого выстраивается архитектура управления рисками и ИБ-процессами.

SGRC В ДЕЛЕ: ВОЗМОЖНОСТИ, КОТОРЫЕ МЕНЯЮТ ПРОЦЕСС

Управление политиками и защитными мерами. SGRC предоставляет инструменты, упрощающие процедуры оценки соответствия требованиям:

- ведение единой базы нормативных документов, политик и стандартов, а также реестра внутренней документации по ИБ в рамках организации;
- проведение аудитов на соответствие требованиям регуляторов (ЦБ РФ, ФСТЭК, ФСБ, отраслевые стандарты и др.);
- учет перечня защитных мер и статус их реализации в отношении проверяемых активов;
- составление реестра замечаний и формирование плана по их обработке;
- автоматизация подготовки отчетности по итогу проверок для предоставления регуляторам или топ-менеджменту;
- управление жизненным циклом политик: от разработки до согласования и контроля исполнения.

Решение не только автоматизирует процедуры, но и связывает между собой разные сущности системы (активы, защитные меры, стандарты и т.д.), облегчает сбор доказательств и подготовку отчетности. За счет этого процесс становится более быстрым, эффективным и прозрачным, а у CISO появляется возможность частично освободить ресурсы сотрудников для более приоритетных задач.

Управление рисками. SGRC позволяет создать единый реестр, в котором фиксируются все выявленные риски, учитываются потенциальные источники, уязвимости и их возможное влияние на информационные активы и бизнес-процессы. Обычно он содержит следующую информацию:

- описание каждого риска;
- вероятность его реализации и возможные последствия;
- действующие меры по снижению риска;
- применяемые контроли и политики;
- ответственные лица;
- способ обработки или устранения риска;
- стоимость защитных мер и расчет совокупного бюджета для снижения риска до приемлемого уровня.

Это позволяет организации получить целостное представление о ландшафте угроз, формировать «дорожную карту» развития безопасности на основе бизнес-рисков, а не только технических показателей, и осуществлять постоянный контроль их уровня.

В R-Vision SGRC доступны как встроенные методики оценки, так и возможность создавать собственные формулы и алгоритмы с помощью конструктора. Это важно для крупных компаний, которые разрабатывают внутренние стандарты и экстраполируют их на дочерние организации и подразделения.

Интеграция аудита и риск-менеджмента. Стоит отметить, что четко выстроенный процесс оценки соответствия требованиям помогает в определении мер, необходимых для обеспечения киберустойчивости, поскольку устранение выявленных замечаний может снизить вероятность реализации некоторых угроз.

В случае если для проведения аудита и оценки рисков ИБ в организации используется автоматизированная система класса SGRC, результаты этих двух процессов будут дополнять друг друга. К примеру, R-Vision SGRC автоматически отмечает требования аудита выполненными, если в организации уже задействованы необходимые защитные меры. Если же они не обнаружены, то будут рекомендованы к внедрению. Все реализованные средства защиты автоматически учитываются в оценке вероятности реализации атак на инфраструктуру компании и влияют на расчёт итогового уровня рисков.

ТРЕНДЫ БЛИЖАЙШИХ ЛЕТ

Интеграция с SOC и управлением уязвимостями. Появилась потребность в интеграции SGRC-решений с инструментарием SOC и формировании процессов управления инцидентами и уязвимостями в единой логике. Компании переходят к расчёту рисков на основе реальных данных из внедренных ИБ-продуктов и приоритизации защитных мер с учётом фактической статистики по киберугрозам.

BI и моделирование сценариев. На фоне привлечения в расчёты реальных данных появилась потребность и во внедрении BI-инструментов. Также происходит переход от поиска актуальных угроз из статичных справочников к сценарному моделированию, которое рассматривает реализацию риска разными путями. Фактически SGRC развивается в сторону «дашборда киберустойчивости», доступного для топ-менеджмента в режиме реального времени: он отображает текущее состояние защищенности и уровень рисков и позволяет вовремя увидеть приближение к «красной зоне».

Платформенность. Отсюда вполне закономерно вытекает тренд на платформенные системы, когда смежные ИБ-решения базируются на общем технологическом стеке, органично интегрированы между собой, обогащают друг друга данными и позволяют выстраивать сквозные процессы.

ЗАКЛЮЧЕНИЕ

Финансовый сектор задал стандарт, который уже широко используется и в других отраслях: промышленности, энергетике, телекоме и ритейле. Сегодня SGRC перестал быть инструментом для «галочки». Он вошел в арсенал средств управления киберустойчивостью, позволяющим CISO перейти от «тушения пожаров» к системному управлению киберрисками. Компании используют SGRC для построения «дорожной карты» по развитию ИБ-процессов, обоснования бюджетов и повышения прозрачности управления. Благодаря этому организации более гибко и эффективно реагируют на современные вызовы и угрозы, укрепляя доверие клиентов и партнеров, а также обеспечивая устойчивое развитие бизнеса в условиях растущих цифровых рисков.