АССОЦИАЦИЯ ФИНТЕХ X COMPLIANCE CONTROL

SECURITY RESILIENCE

подходы к оценке зрелости информационной безопасности

Февраль 2026

ОБ ИССЛЕДОВАНИИ

МАРИАННА ДАНИЛИНА

Руководитель управления стратегии, исследований и аналитики, АФТ

В настоящем исследовании представлены результаты аналитической работы, проведенной в рамках оценки применимости международных фреймворков информационной безопасности в специфических условиях российского финтех-сектора[1].

Особенность финтех-рынка заключается в том, что требования к информационной безопасности здесь интегрированы с требованиями к финансовым процессам, Открытым API, цифровым финансовым активам, комплексу законов, правил и процедур, направленных на пресечение легализации доходов, полученных преступным путем (AML/CFT), противодействию мошенничеству, что создает дополнительный уровень сложности.

Проведенное исследование показывает, что финтех-организации в России сталкиваются с большим количеством требований: с одной стороны, нормативные стандарты Банка России и других регуляторов Российской Федерации, часть из которых основана на лучших международных практиках и принципах BCBS (Basel Committee on Banking Supervision), с другой стороны, накладываются общие ограничения по локализации данных, использованию отечественного ПО и текущей геополитической обстановке, которые делают невозможным прямое применение зарубежных стандартов без их адаптации.

В рамках исследования были проанализированы международные фреймворки и стандарты по информационной безопасности (NIST CSF 2.0, ISO/IEC 27001/27002, CIS Controls v8.1, ISACA COBIT 2019), проведена оценка их применимости в специфических условиях российского финтех-сектора и отмечены особенности внедрения зарубежных стандартов в финансовых организациях в России.

Также в исследовании предложен адаптированный фреймворк для проведения самостоятельной оценки зрелости кибербезопасности в российских финансовых организациях.

[1] *На основании деятельности выборки организаций-заказчиков группы компаний Compliance Control & Rakasta.*

АССОЦИАЦИЯ
ФИНТЕХ

Ассоциация ФинТех *основана в конце 2016 г. по инициативе Банка России и ключевых участников отечественного финансового рынка. Это уникальная площадка для конструктивного диалога регулятора с представителями бизнеса. Здесь формируется экспертная оценка инновационных технологий с учетом международного опыта, а также разрабатываются концепции финансовых технологий и подходы к их внедрению.*

АЛЕКСАНДР ТОВСТОЛИП

Руководитель Управления информационной безопасности, АФТ

В условиях высокой регуляторной нагрузки, технологической сложности и постоянной эволюции киберугроз информационная безопасность организации не может строиться на фрагментарных мерах или разрозненных практиках. Применение формализованных фреймворков информационной безопасности позволяет перейти от реактивного управления рисками к системному и воспроизводимому подходу, обеспечивая сопоставимость, масштабируемость и управляемость процессов.

Для финтех-организаций, работающих на стыке финансовых и цифровых экосистем, выбор, адаптация и применение международных фреймворков ИБ становится не просто методологическим решением, а стратегическим фактором устойчивости и доверия.

АЛЕКСЕЙ ОСИПОВ

Руководитель направления экспертного консалтинга, Compliance Control

Для нашей команды возможность делиться опытом, накопленным на международных проектах - это не просто обмен знаниями, а реальный вклад в развитие более устойчивой системы кибербезопасности в российском финтехе. Работая с разными международными фреймворками, мы проанализировали, как они используются в реальной практике финтех-бизнеса, и собрали собственную матрицу их применимости.

Мы верим, что благодаря нашим совсместным усилиям, финтех-компании смогут выстраивать ИБ-стратегию более эффективно, с учетом чужих ошибок и опыта.

Надеемся, что Вам будет полезно.

СОДЕРЖАНИЕ

ОБЗОР ПРИМЕНИМОСТИ МЕЖДУНАРОДНЫХ ПОДХОДОВ

МЕТОДОЛОГИЧЕСКИЙ ПОДХОД К АНАЛИЗУ ДОМЕНОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

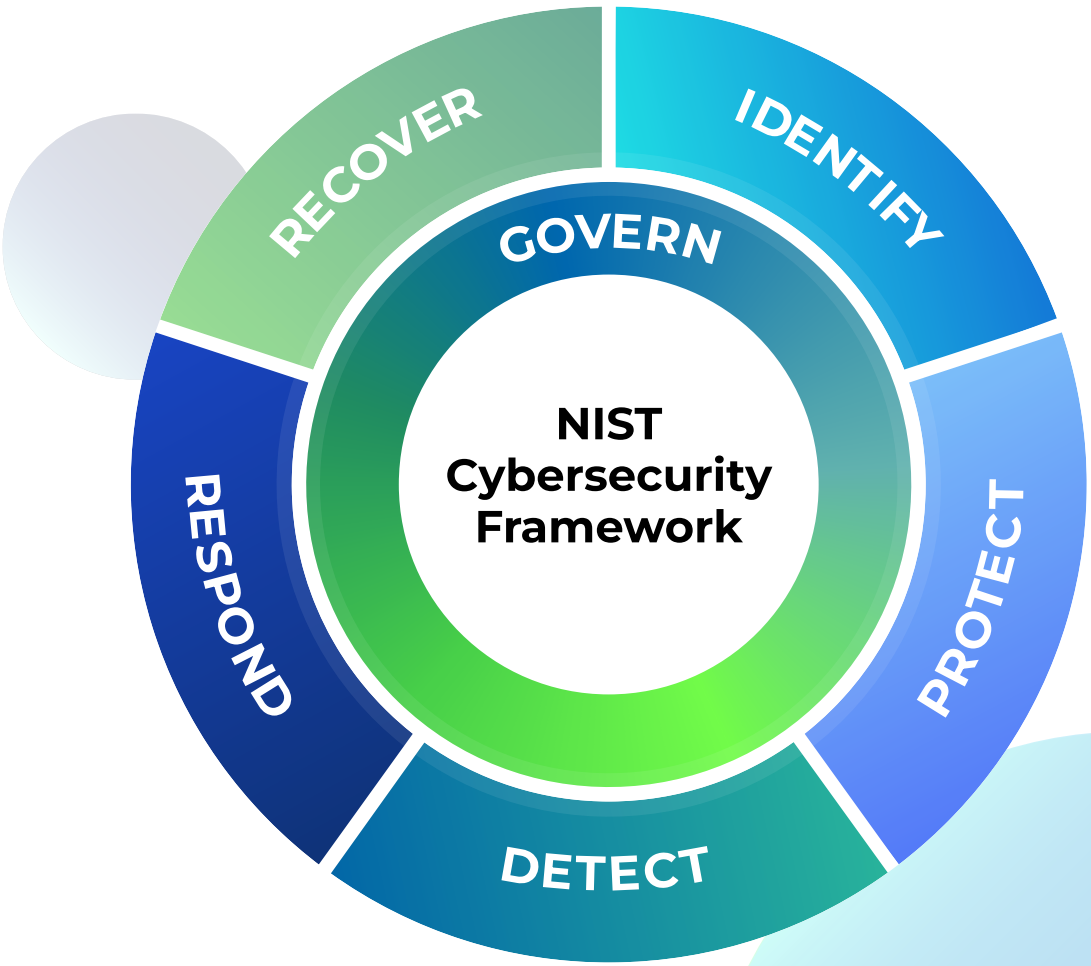
В рамках настоящего отчёта анализ применения международных фреймворков информационной безопасности выполнен на основе доменной модели **NIST Cybersecurity Framework (NIST CSF) версии 2.0.**

Выбор NIST CSF обусловлен тем, что **данный фреймворк предоставляет универсальную доменную структуру**, позволяющую системно рассматривать требования в области информационной безопасности как на управленческом, так и на техническом уровне, а также применять риск-ориентированный подход, интегрированный в бизнес-процессы организации.

При этом в Российской Федерации для финансовых организаций ключевым отраслевым стандартом в области информационной безопасности и операционной надёжности является серия стандартов **ГОСТ Р 57580**, который устанавливает обязательные требования и служит базисом для построения системы ИБ. Структура и направленность ГОСТ Р 57580 ориентированы преимущественно на оценку реализации и достаточности мер защиты информации, что определяет его прикладной и нормативный характер и ограничивает его использование в качестве универсальной архитектурной модели для комплексного доменного анализа.

Использование доменной модели NIST CSF в рамках данного исследования позволило:

- обеспечить сопоставимость и целостность анализа
- унифицировать сравнение требований различных международных фреймворков
- выявить пересечения и различия в подходах
- оценить степень применимости управленческих и технических практик с учётом их адаптации к российскому финтех-рынку и требованиям ГОСТ Р 57580



ДОМЕНЫ NIST CSF

И АНАЛИТИКА ПРИМЕНЕНИЯ В ФИНТЕХ-ОРГАНИЗАЦИЯХ

01 GOVERNANCE
(СТРАТЕГИЯ И УПРАВЛЕНИЕ)

ОПИСАНИЕ ДОМЕНА

Governance – это домен, определяющий стратегическое и организационное управление информационной безопасностью организации. Он охватывает формирование целей и принципов ИБ, разработку и утверждение политик и процедур, распределение ролей и ответственности, а также контроль выполнения требований в области информационной безопасности.

В рамках домена Governance также формируются управленческие подходы к контролю рисков, связанных с использованием программного обеспечения, аппаратных средств и услуг третьих лиц. Это включает установление требований информационной безопасности к поставщикам, интеграцию вопросов управления цепочкой поставок в систему корпоративного управления рисками и принятие решений о допустимом уровне зависимостей от внешних решений.

ЦЕЛИ ДОМЕНА

- обеспечить стратегическое выравнивание подходов к информационной безопасности с бизнес-целями организации
- определить четкое распределение ролей и ответственности за информационную безопасность
- установить политики и стандарты для защиты информационных активов
- обеспечить эффективное управление человеческими, финансовыми и технологическими ресурсами в целях реализации инициатив информационной безопасности
- обеспечить соответствие нормативным и законодательным требованиям в области информационной безопасности
- установить требования по информационной безопасности к поставщикам и включать их в договорные отношения и критерии выбора
- обеспечить управление рисками информационной безопасности, связанными с поставщиками, подрядчиками и использованием решений/услуг третьих лиц

ПРИМЕНЕНИЕ ДОМЕНА GOVERNANCE В МЕЖДУНАРОДНЫХ ФРЕЙМВОРКАХ

NIST CSF 2.0 — Govern function	Функция Govern определяет стратегию ИБ, допустимый уровень риска и распределение ответственности. Подход ориентирован на гибкость и может использоваться как архитектурная основа системы управления ИБ.
ISO/IEC 27001:2022	Функции Governance реализуются через систему менеджмента ИБ (ISMS - Information Security Management System), требования к роли руководства и процесс управления рисками. Формализованный характер стандарта делает его удобным для регулируемых отраслей.
ISO/IEC 27002:2022	Стандарт предоставляет набор организационных контролей, поддерживающих управленческие процессы ИБ, и используется как методологическая база для реализации Governance.

ISACA COBIT 2019	Фреймворк корпоративного управления ИТ, в рамках которого информационная безопасность рассматривается как часть системы управления целями, рисками и ответственностью. Используется для формализации ролей органов управления и принятия управленческих решений в области ИБ.
NIST SP 800-161 Rev.1	Документ развивает положения Governance в части управления рисками цепочки поставок, детализируя управленческие практики оценки и мониторинга поставщиков. Рассматривается как расширение корпоративной модели управления рисками ИБ.
CIS Controls v8.1	Контроли описывают управление рисками поставщиков как элемент системы управления и контроля ИБ. Supply Chain Risk Management поддерживает цели Governance на уровне организации.

ОСОБЕННОСТИ ВНЕДРЕНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Реализация домена Governance в российских финтех-организациях, использующих международные фреймворки информационной безопасности, осуществляется с учётом требований национального регулирования. Это влияет на формирование стратегической модели управления ИБ, включая управление внешними зависимостями и рисками цепочки поставок, которые рассматриваются как часть корпоративного управления.

01

Требование использования отечественного программного обеспечения

Запрет на использование иностранного ПО на объектах критической информационной инфраструктуры требует выстраивания стратегии импортозамещения в рамках Governance. Это затрагивает как архитектурные решения, так и управление рисками, связанными с выбором поставщиков, ограниченной зрелостью отечественных решений и необходимостью адаптации персонала.

02

Повышенная роль регуляторов в формировании приоритетов ИБ

В российском финтех-секторе ключевые приоритеты информационной безопасности, включая требования к поставщикам и используемым технологиям, во многом задаются регуляторами. В результате Governance ориентирован преимущественно на нормативное соответствие, что снижает гибкость в управлении рисками и выборе стратегических инициатив, в том числе в части цепочки поставок.

03

Требования к локализации данных и инфраструктуры

Обязательная локализация персональных данных и приоритет использования отечественной инфраструктуры ограничивают применение зарубежных облачных сервисов и глобальных цепочек поставок. Эти ограничения учитываются в Governance при формировании стратегии ИБ и долгосрочных планов развития ИТ- и ИБ-архитектуры.

04

Ограниченная зрелость управления рисками цепочки поставок

Различия в степени формализации подходов к управлению рисками цепочки поставок и особенности оценки поставщиков обуславливают необходимость адаптации международных практик к национальному контексту. В рамках домена Governance это усиливает роль внутренних политик, компенсирующих управленческих мер и экспертной оценки рисков, связанных с внешними зависимостями.

02 IDENTIFY
(ИДЕНТИФИКАЦИЯ АКТИВОВ, РИСКОВ И УГРОЗ)

ОПИСАНИЕ ДОМЕНА

Identify – это домен, охватывающий процессы выявления, инвентаризации и классификации информационных активов, оценки рисков информационной безопасности и анализа актуального ландшафта угроз. Он формирует понимание того, какие активы подлежат защите и с каким уровнем риска функционирует организация, при этом угрозы в рамках данного домена рассматриваются как методологическая основа для оценки рисков и обоснования управленческих и архитектурных решений, а не как события в реальном времени.

ЦЕЛИ ДОМЕНА

- сформировать полный и актуальный реестр информационных активов
- классифицировать активы с точки зрения их критичности для бизнеса
- оценить риски реализации информационных угроз
- выявить потенциальные уязвимости и зоны повышенного риска
- обеспечить соответствие требованиям законодательства и отраслевых стандартов
- обеспечить руководство информацией для принятия решений по управлению рисками

ПРИМЕНЕНИЕ ДОМЕНА IDENTIFY В МЕЖДУНАРОДНЫХ ФРЕЙМВОРКАХ

NIST CSF 2.0 — Identify function	Функция Identify охватывает управление активами, оценку рисков и анализ угроз на уровне организации и формирует основу для последующих доменов NIST CSF.
ISO/IEC 27001:2022	Домен Identify реализуется через риск-ориентированный подход, в рамках которого активы и угрозы используются для обоснования выбора мер ИБ.
CIS Controls v8.1	Домен Identify реализован в CIS Controls v8.1 через практики инвентаризации активов и управления уязвимостями, обеспечивая операционную детализацию.
ISACA COBIT 2019	Рассматривает процессы идентификации рисков и активов в контексте корпоративного управления и управления ИТ-рисками, обеспечивая связь между оценкой рисков информационной безопасности и целями организации.

ОСОБЕННОСТИ ВНЕДРЕНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Реализация домена Identify в российских финтех-организациях характеризуется ограничениями, влияющими на процессы анализа угроз и оценки рисков.

01

Отсутствие официального и широкодоступного механизма обмена информацией об угрозах (Cyber Threat Intelligence, CTI)

В Российской Федерации отсутствует единая широкодоступная и централизованная платформа обмена информацией об угрозах, сопоставимая с международными инициативами (US-CERT, ENISA). Существующие механизмы обмена CTI ориентированы преимущественно на отдельные отрасли и имеют ограниченную применимость для широкого круга организаций.

Как пример, в стране развивается национальная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, включая деятельность НКЦКИ (Национальный координационный центр по компьютерным инцидентам Федеральной службы безопасности) и инфраструктуру ГосСОПКА, а также отраслевые механизмы обмена информацией об угрозах, такие как ФинЦЕРТ Банка России. Указанные механизмы формируют основу для централизованного обмена информацией об угрозах и инцидентах, однако на текущем этапе в большей степени ориентированы на взаимодействие с государственными органами, объектами критической инфраструктуры и финансовыми организациями, что ограничивает их использование. Для большинства организаций вне указанных категорий доступ к таким механизмам либо отсутствует, либо носит ограниченный характер.

02

Требование обязательного уведомления государственных органов

Национальные требования предусматривают обязательное уведомление уполномоченных государственных органов и пострадавших лиц о произошедших инцидентах информационной безопасности. Данные требования накладывают дополнительные ограничения на процессы идентификации и классификации инцидентов и требуют формализации критериев значимости инцидентов уже на этапе Identify. Отказ от внедрения или некорректное внедрение средств «уведомления» регуляторов об инцидентах может привести к существенным штрафам, финансовым и репутационным потерям.

03 PROTECT
(РЕАЛИЗАЦИЯ МЕР ЗАЩИТЫ)

ОПИСАНИЕ ДОМЕНА

Домен **Protect** фокусируется на реализации организационных и технических мер, направленных на предотвращение несанкционированного доступа и снижение вероятности реализации угроз информационной безопасности. В рамках данного домена формируются и применяются меры по управлению доступом, защите данных и обеспечению безопасности инфраструктуры и пользовательских сред, направленные на снижение уровня риска до момента возникновения инцидента в соответствии с результатами оценки рисков и принятыми управленческими решениями.

ЦЕЛИ ДОМЕНА

- предотвратить несанкционированный доступ к информационным системам и данным
- обеспечить защиту конфиденциальности, целостности и доступности информации
- снизить вероятность успешной реализации атак
- ограничить потенциальный ущерб при компрометации отдельных компонентов
- обеспечить выполнение требований регуляторов в части защиты данных

ПРИМЕНЕНИЕ ДОМЕНА PROTECT В МЕЖДУНАРОДНЫХ ФРЕЙМВОРКАХ

NIST CSF 2.0 — Protect function	Домен Protect охватывает управление учетными данными и доступом, защиту данных и безопасность окружения, обеспечивая снижение вероятности реализации угроз.
ISO/IEC 27001/27002:2022	Реализация домена Protect осуществляется через выбор и внедрение контролей на основе оценки рисков, включая организационные и технические меры защиты.
CIS Controls v8.1 — Core Safeguards	Домен Protect реализован в фреймворке через набор практических мер защиты активов, управления доступом и защиты данных, дополняя управленческие модели конкретными техническими практиками.
ISACA COBIT 2019	Рассматривает меры защиты информационных активов как часть системы управления ИТ-контролями и рисками, обеспечивая увязку технических и организационных мер защиты с целями и требованиями корпоративного управления.

ОСОБЕННОСТИ ВНЕДРЕНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Практическая реализация домена Protect в российских финтех-организациях осуществляется с учетом требований национального законодательства и регуляторной практики, влияющих на выбор средств защиты и архитектуру решений.

01

Обязательная замена иностранного программного обеспечения на отечественное

Ограничения на использование иностранного программного обеспечения на объектах критической информационной инфраструктуры обуславливают необходимость применения отечественных средств защиты и инфраструктурных решений. Это влияет на архитектуру защитных мер, уровень автоматизации и зрелость реализуемых контролей, а также требует корректировки проектных решений и дополнительных организационных усилий при внедрении мер защиты.

02

Ограничения на использование зарубежных облачных сервисов

Требования к локализации данных исключают использование зарубежных облачных платформ для обработки персональных данных и сервисов безопасности. В результате реализация мер защиты в домене Protect должна опираться на локальных провайдеров или собственную инфраструктуру, что ограничивает применение отдельных облачных моделей безопасности и влияет на масштабируемость и гибкость защитных решений.

04 DETECT
(ОБНАРУЖЕНИЕ УГРОЗ)

ОПИСАНИЕ ДОМЕНА

Домен **Detect** ориентирован на своевременное выявление подозрительной активности, атак и инцидентов информационной безопасности за счет непрерывного мониторинга и анализа событий безопасности, а также выявления признаков компрометации в информационных системах и сетях. В рамках данного домена угрозы рассматриваются как события, подлежащие оперативному обнаружению и подтверждению с целью передачи релевантной информации для последующего реагирования.

ЦЕЛИ ДОМЕНА

- обеспечить своевременное выявление атак и инцидентов информационной безопасности
- сократить время между возникновением инцидента и его обнаружением (MTTD)
- обеспечить видимость событий безопасности в системах и сетях (visibility)
- предоставить данные для оперативного реагирования и расследования
- поддерживать непрерывный мониторинг безопасности и выявление аномалий

ПРИМЕНЕНИЕ ДОМЕНА DETECT В МЕЖДУНАРОДНЫХ ФРЕЙМВОРКАХ

NIST CSF 2.0 — Detect function	Функция Detect охватывает непрерывный мониторинг и анализ неблагоприятных событий, обеспечивая выявление инцидентов и признаков атак.
ISO/IEC 27001 — Monitoring and Testing	В ISO/IEC 27001 домен Detect реализуется через требования к мониторингу, тестированию и оценке эффективности мер защиты и процессов ИБ.
CIS Controls v8.1 — Security Continuous Monitoring	Домен Detect реализован в фреймворке CIS Controls в виде практических рекомендаций по организации непрерывного мониторинга и анализа событий ИБ.
ISACA COBIT 2019	Рассматривает процессы мониторинга и контроля как часть системы управления ИТ и операционными рисками, обеспечивая выявление отклонений и инцидентов информационной безопасности в контексте корпоративного управления.

ОСОБЕННОСТИ ВНЕДРЕНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Практическая реализация домена Detect в российских финтех-организациях определяется требованиями национального законодательства и регуляторных актов, которые влияют на построение и функционирование систем мониторинга и обнаружения, используемые источники аналитики угроз и порядок уведомления о выявленных инцидентах.

01

Требование локального размещения средств мониторинга и хранения логов

Требования по локализации данных и нормативные требования к обработке информации ограничивают использование зарубежных облачных решений мониторинга и предполагают размещение систем сбора и анализа событий безопасности на территории Российской Федерации, включая использование отечественных SIEM и SOC-решений.

02

Ограничения на использование зарубежных платформ Threat Intelligence

В российских условиях ограничено использование ряда международных платформ аналитики угроз (Threat Intelligence), что требует опоры на отечественных провайдеров и внутренние источники информации об угрозах при построении корреляционных и аналитических сценариев.

03

Регламентированные сроки уведомления о выявленных инцидентах

Нормативные требования финансового сектора предусматривают жесткие сроки первичного уведомления о выявленных атаках и инцидентах. Это повышает требования к зрелости процессов мониторинга и требует организации 24/7 наблюдения, формализованных процедур эскалации и автоматизации первичной фиксации и передачи информации.

05 RESPOND
(РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ)

ОПИСАНИЕ ДОМЕНА

Домен **Respond** фокусируется на управлении подтвержденными инцидентами информационной безопасности и координации действий по их обработке. Он охватывает процессы реагирования, классификации инцидентов, анализа причин и последствий, сдерживания и устранения угроз, а также управление коммуникациями и документированием в ходе инцидента. Реализация домена Respond направлена на минимизацию ущерба и предотвращение повторной реализации инцидентов за счет формализованных процедур реагирования и систематического совершенствования процессов.

ЦЕЛИ ДОМЕНА

- обеспечить управляемое и своевременное реагирование на подтвержденные инциденты ИБ
- ограничить масштаб ущерба и предотвратить распространение атаки
- выполнить необходимые действия по сдерживанию и устранению угроз
- обеспечить сбор и фиксацию данных, необходимых для внутреннего расследования и взаимодействия с заинтересованными сторонами
- обеспечить выполнение требований по уведомлению уполномоченных органов и пострадавших лиц
- повысить зрелость процессов реагирования на основе анализа инцидентов и извлеченных уроков

ПРИМЕНЕНИЕ ДОМЕНА RESPOND В МЕЖДУНАРОДНЫХ ФРЕЙМВОРКАХ

NIST CSF 2.0 — Respond function	Функция Respond определяет подходы к управлению инцидентами информационной безопасности, включая их анализ, координацию действий по реагированию, смягчение последствий и организацию коммуникаций и отчетности в ходе реагирования.
ISO/IEC 27001:2022 — Incident Planning and Response	Реализует домен Respond через требования к планированию реагирования на инциденты, формализации процедур их обработки и управлению процессами реагирования в рамках системы менеджмента информационной безопасности.
NIST SP 800-61 Rev.2 — Computer Security Incident Handling	Определяет жизненный цикл обработки инцидентов и практики организации процессов реагирования, включая обнаружение, анализ, сдерживание, ликвидацию последствий и восстановление.
ISACA COBIT 2019	Рассматривает процессы реагирования на инциденты как часть системы управления ИТ-рисками и внутреннего контроля, обеспечивая формализацию ролей, ответственности, процедур эскалации и контроля эффективности реагирования в рамках корпоративного управления.

ОСОБЕННОСТИ ВНЕДРЕНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Практическая реализация домена Respond в российских финтех-организациях определяется регламентированными сроками уведомления, необходимостью взаимодействия с несколькими государственными органами и ограничениями на привлечение зарубежных сервисов расследования и реагирования.

01

Жесткие сроки реагирования и уведомления

Нормативные требования предусматривают необходимость оперативного уведомления регуляторов о выявленном инциденте информационной безопасности в установленные сроки (3/24/72 часа) и последующей отчетности по результатам его обработки и закрытия (как правило, в срок до 30 дней). Это требует наличия подготовленной команды реагирования на инциденты, формализованных процедур реагирования и автоматизации первичных действий (обнаружение, классификация, эскалация и подготовка уведомления) для соблюдения регламентированных временных требований.

02

Требование уведомления регуляторов

В зависимости от характера и последствий инцидента информационной безопасности организация обязана уведомлять соответствующие уполномоченные органы и, в установленных случаях, затронутых лиц.

- Оперативное уведомление об инцидентах, затрагивающих объекты критической информационной инфраструктуры, осуществляется в адрес Национального координационного центра по компьютерным инцидентам (НКЦКИ ФСБ России) в рамках функционирования системы ГосСОПКА.
- В случае инцидентов, связанных с нарушением безопасности персональных данных, организация обязана уведомить Роскомнадзор, а также затронутых субъектов персональных данных в порядке и сроки, установленные законодательством Российской Федерации.
- ФСТЭК России осуществляет регуляторный контроль и надзор за соблюдением требований по обеспечению безопасности критической информационной инфраструктуры, включая оценку полноты и корректности мер реагирования на инциденты.
- Для финансовых организаций дополнительно применяется порядок информирования ФинЦЕРТ Банка России в рамках отраслевого взаимодействия и требований регулятора.

Совокупность указанных требований обусловливает необходимость корректной классификации инцидентов информационной безопасности, выстраивания управляемых коммуникаций с регуляторами и заинтересованными сторонами, а также документирования процессов реагирования и принятых мер.

03

Ограничения на обращение к иностранным сервисам расследования/форензики

В условиях действующих ограничений финтех-организации не могут в полной мере взаимодействовать с международными сервисами по расследованию инцидентов и реагированию. В результате возрастает необходимость наличия собственных компетенций в области цифровой форензики (компьютерной криминалистики) и реагирования на инциденты, либо выстраивания договорных отношений с отечественными специализированными организациями, способными обеспечить проведение расследований и поддержку процессов реагирования в установленные сроки.

06 RECOVER
(ВОССТАНОВЛЕНИЕ И НЕПРЕРЫВНОСТЬ ДЕЯТЕЛЬНОСТИ)

ОПИСАНИЕ ДОМЕНА

Домен **Recover** ориентирован на восстановление и поддержание операционной устойчивости организации после инцидентов информационной безопасности и иных чрезвычайных событий. В рамках данного домена реализуются процессы резервного копирования, аварийного восстановления (Disaster Recovery) и обеспечения непрерывности деятельности (Business Continuity), направленные на снижение последствий инцидентов и восстановление критически важных информационных систем, данных и бизнес-процессов.

ЦЕЛИ ДОМЕНА

- минимизировать время простоя информационных систем при инциденте (RTO - Recovery Time Objective)
- минимизировать потерю данных при инциденте (RPO - Recovery Point Objective)
- восстановить критичные бизнес-процессы и ИТ-сервисы в установленные сроки
- обеспечить непрерывность деятельности организации (Business Continuity)
- снизить финансовые и операционные потери, связанные с простоями и потерей данных
- выполнить требования регуляторов по обеспечению непрерывности критически важных операций

ПРИМЕНЕНИЕ ДОМЕНА RECOVER В МЕЖДУНАРОДНЫХ ФРЕЙМВОРКАХ

NIST CSF 2.0 — Recover function	Функция Recover определяет подходы к восстановлению и поддержанию операционной устойчивости после инцидентов информационной безопасности, включая выполнение плана восстановления и обмен информацией о ходе и результатах восстановительных мероприятий.
ISO/IEC 27001 — Business Continuity	Реализует домен Recover через требования к восстановлению и обеспечению непрерывности деятельности в рамках системы менеджмента информационной безопасности, увязывая мероприятия по восстановлению с управлением рисками.
ISACA COBIT 2019	Рассматривает восстановление и непрерывность деятельности как элементы управления операционной устойчивостью и ИТ-рисками, обеспечивая формализацию ответственности, контроль готовности к восстановлению и оценку эффективности мероприятий по обеспечению устойчивости.

ОСОБЕННОСТИ ВНЕДРЕНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Практическая реализация домена Recover в российских финтех-организациях осуществляется с учетом требований к территориальному размещению данных, применению отечественных технических решений и ограничений на использование зарубежных сервисов резервирования и аварийного восстановления.

01

Территориальные требования к размещению резервных копий

Требования к территориальному размещению данных предусматривают хранение резервных копий на территории Российской Федерации, что исключает использование зарубежных облачных решений для резервирования. Это обуславливает необходимость реализации процессов восстановления на локальной инфраструктуре и влияет на архитектурные решения в части резервного копирования и аварийного восстановления. В результате возрастает нагрузка на собственную инфраструктуру и процессы эксплуатации, что приводит к увеличению затрат на обеспечение резервирования и операционной устойчивости, в среднем на 20–30% от ИТ-бюджета.

02

Ограниченный выбор и зрелость отечественных средств резервного копирования

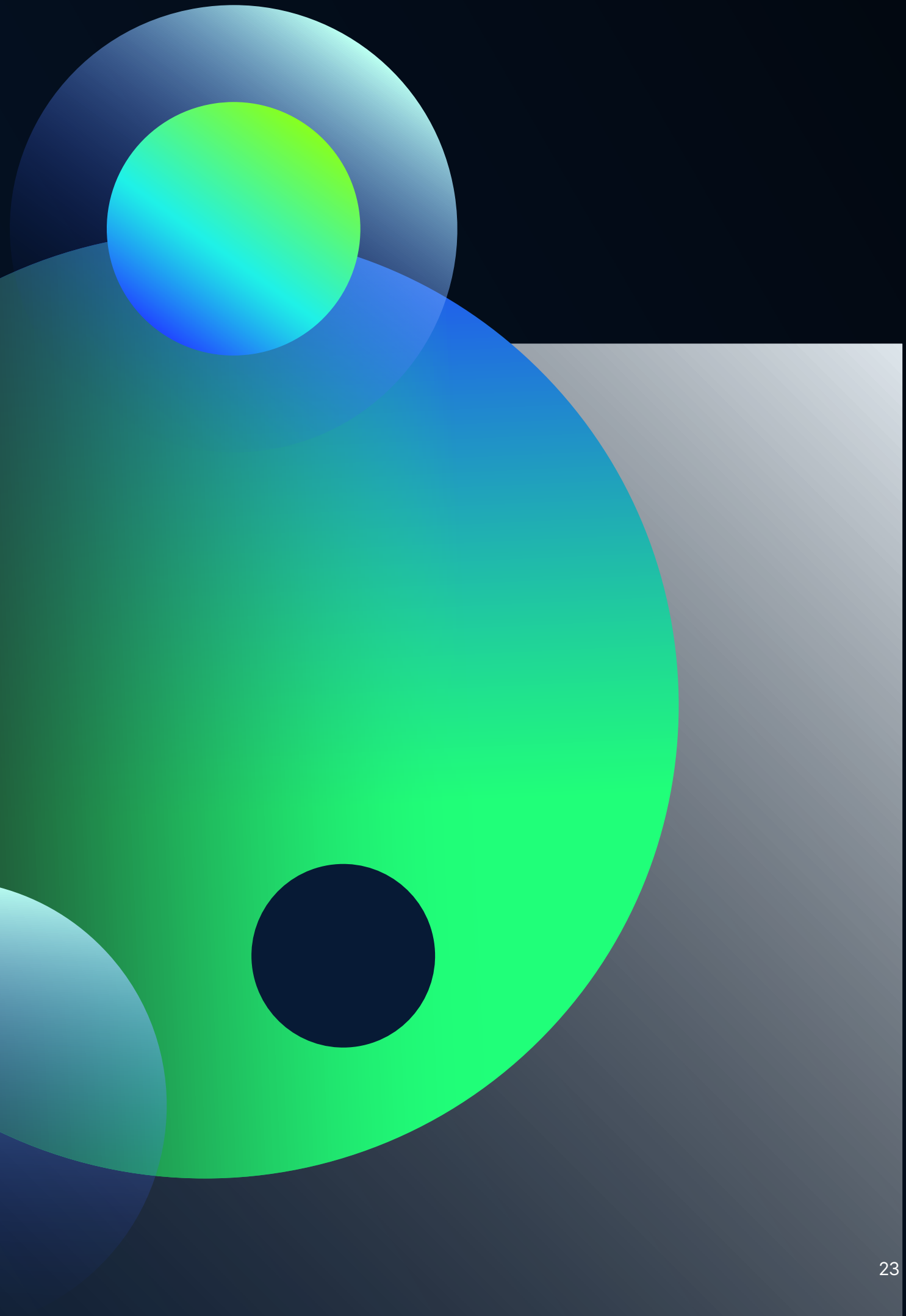
Реализация процессов резервного копирования и восстановления в рамках домена Recover осуществляется с использованием отечественных программных и аппаратных средств. При этом доступные решения могут обладать ограниченной функциональностью по сравнению с зарубежными аналогами и более высокой стоимостью владения, что необходимо учитывать при проектировании и развитии системы восстановления.

03

Ограничения на привлечение зарубежных провайдеров аварийного восстановления

Действующие ограничения исключают возможность использования услуг зарубежных провайдеров аварийного восстановления (Disaster Recovery). В результате организации вынуждены обеспечивать процессы аварийного восстановления за счет собственной инфраструктуры либо выстраивать договорные отношения с отечественными провайдерами, что напрямую влияет на уровень операционной устойчивости и требования к планированию восстановления.

ОБЩИЙ ВЫВОД



АНАЛИЗ ДОМЕННОЙ МОДЕЛИ NIST CSF И МЕЖДУНАРОДНЫХ ФРЕЙМВОРКОВ

В рамках исследования была проведена оценка применимости доменов **NIST Cybersecurity Framework (CSF)** к требованиям и структурам **ISO/IEC 27001:2022, CIS Controls v8.1** и **ISACA COBIT 2019**. Результаты оценки представлены в виде унифицированной матрицы соответствия, что позволило наглядно отразить степень согласованности управленческих и операционных подходов указанных стандартов с доменной моделью NIST CSF в условиях российского финтех-сектора.

Таблица оценки применимости международных фреймворков:

ДОМЕН	ФРЕЙМВОРКИ: NIST CSF 2.0	ISO/IEC 27001:2022	CIS Controls v8.1	ISACA COBIT 2019
Governance	4	4	2	4
Identity	3	2	2	3
Protect	4	4	4	4
Detect	3	2	2	3
Respond	4	3	2	3
Recover	3	2	2	3

Шкала оценки: 1 — низкая применимость, 4 — высокая применимость.

Анализ показал, что наибольшей применимостью характеризуются домены **Governance, Protect** и **Respond**, тогда как домены **Identify, Detect** и **Recover** требуют более глубокой адаптации механизмов реализации при сохранении общей методологической основы.

СПЕЦИФИКА ВНЕДРЕНИЯ ДОМЕНОВ NIST CSF В РОССИЙСКОЙ ФЕДЕРАЦИИ

Финтех-организации Российской Федерации применяют международные фреймворки информационной безопасности с учетом действующего нормативного регулирования, включая ограничения на использование иностранного программного обеспечения, требования к локализации данных и необходимость одновременного соблюдения требований нескольких регуляторов. Эти факторы существенно влияют на практику внедрения доменов NIST CSF.

Дополнительную сложность создают регламентированные сроки и порядок уведомления о киберинцидентах, использование национальных механизмов обмена информацией об угрозах и ограничения на привлечение зарубежных сервисов реагирования и расследования. В совокупности данные условия требуют адаптации архитектурных решений и усиления роли управленческих процессов при построении системы информационной безопасности.

Применение международных фреймворков в финтех-секторе является целесообразным, однако требует глубокой адаптации к российскому законодательству. Эффективность внедрения во многом определяется знанием национального нормативного ландшафта, гибкостью в применении международных практик, долгосрочным планированием и готовностью к инвестициям в инфраструктуру на базе отечественных решений.

РОЛЬ NIST CSF И НАЦИОНАЛЬНЫХ СТАНДАРТОВ

NIST Cybersecurity Framework основан на управлении киберрисками и предназначен для формирования целостной архитектуры процессов, ролей и технических мер защиты. Фреймворк разработан как гибкий и адаптируемый инструмент, предоставляющий обобщённые рекомендации, которые конкретизируются организациями с учётом их профиля рисков, уровня зрелости и организационного контекста. Вместе с тем его практическое внедрение может быть ресурсозатратным и требует поэтапного и осознанного подхода.

Серия ГОСТ Р 57580, в свою очередь, ориентирована на оценку соответствия реализации мер защиты информации в финансовых организациях и устанавливает обязательные регуляторные требования в данной области. Стандарт задаёт формализованные критерии и контрольные требования, направленные на обеспечение проверяемости и воспроизводимости результатов оценки.

Результаты исследования показывают, что международные фреймворки информационной безопасности сохраняют высокую методологическую ценность для российского финтех-сектора, однако их практическое применение возможно только при адаптации к национальным требованиям. В этих условиях целесообразным представляется комбинированный подход, при котором требования серии ГОСТ Р 57580 дополняются архитектурной моделью NIST CSF и лучшими международными практиками управления рисками.

AFT Framework

ЗРЕЛОСТЬ КИБЕРБЕЗО-ПАСНОСТИ

для самостоятельной оценки
в финансовых организациях


АССОЦИАЦИЯ
ФИНТЕХ

ДИСКЛЕЙМЕР

Предлагаемый фреймворк оценки кибербезопасности разработан с учётом особенностей российского финансового рынка и сочетает требования нормативного соответствия с риск-ориентированным управлением.
В его основе лежит понимание того, что устойчивость системы информационной безопасности формируется не только через формальное выполнение установленных мер защиты, но и через системную оценку и управление киберрисками.

Серия ГОСТ Р 57580 и доменная модель NIST CSF в данном контексте рассматриваются как взаимодополняющие подходы. Серия ГОСТ Р 57580 ориентирована на оценку реализации и достаточности мер защиты информации и обеспечивает воспроизводимость и проверяемость результатов, тогда как NIST CSF задаёт качественную архитектуру управления киберрисками, позволяющую оценивать зрелость процессов, управленческих решений и взаимодействия между доменами безопасности.

В рамках методологии отдельно выделена область управления рисками цепочки поставок (Supply Chain - Dependency Management), что обусловлено её возрастающим влиянием на устойчивость финансовых организаций и необходимостью более детальной оценки внешних зависимостей.

В совокупности такой подход формирует целостную модель оценки, в которой количественная проверяемость нормативных требований сочетается с качественной оценкой зрелости кибербезопасности, обеспечивая практическую применимость фреймворка в условиях российского финтех-сектора.

МАРИАННА ДАНИЛИНА

Руководитель управления стратегии, исследований и аналитики, АФТ

В 2025 году российские банки потратили от 330 до 390 млрд рублей на информационную безопасность и, вероятно, превысили запланированные ИБ-бюджеты. Это много по меркам ИБ, но сопоставимо масштабу банковского сектора и рисков: примерно 0,2% совокупных активов рынка и около 10% годовой прибыли.

С учетом появления новых поколений угроз и увеличения числа атак на сектор, рост бюджетов в направление безопасности – это необходимая мера. Однако не всегда покупка нового ИБ-инструмента позволяет выстраивать эффективные барьеры против кибермошенников: порой наращивается «лоскутное одеяло» слабо интегрированных инструментов.

Для того чтобы подойти к вопросу повышения безопасности системно, мы предлагаем организациям оценить зрелость кибербезопасности с помощью **нашего фреймворка** и в зависимости от уровня – совершенствовать процессы комплексно.

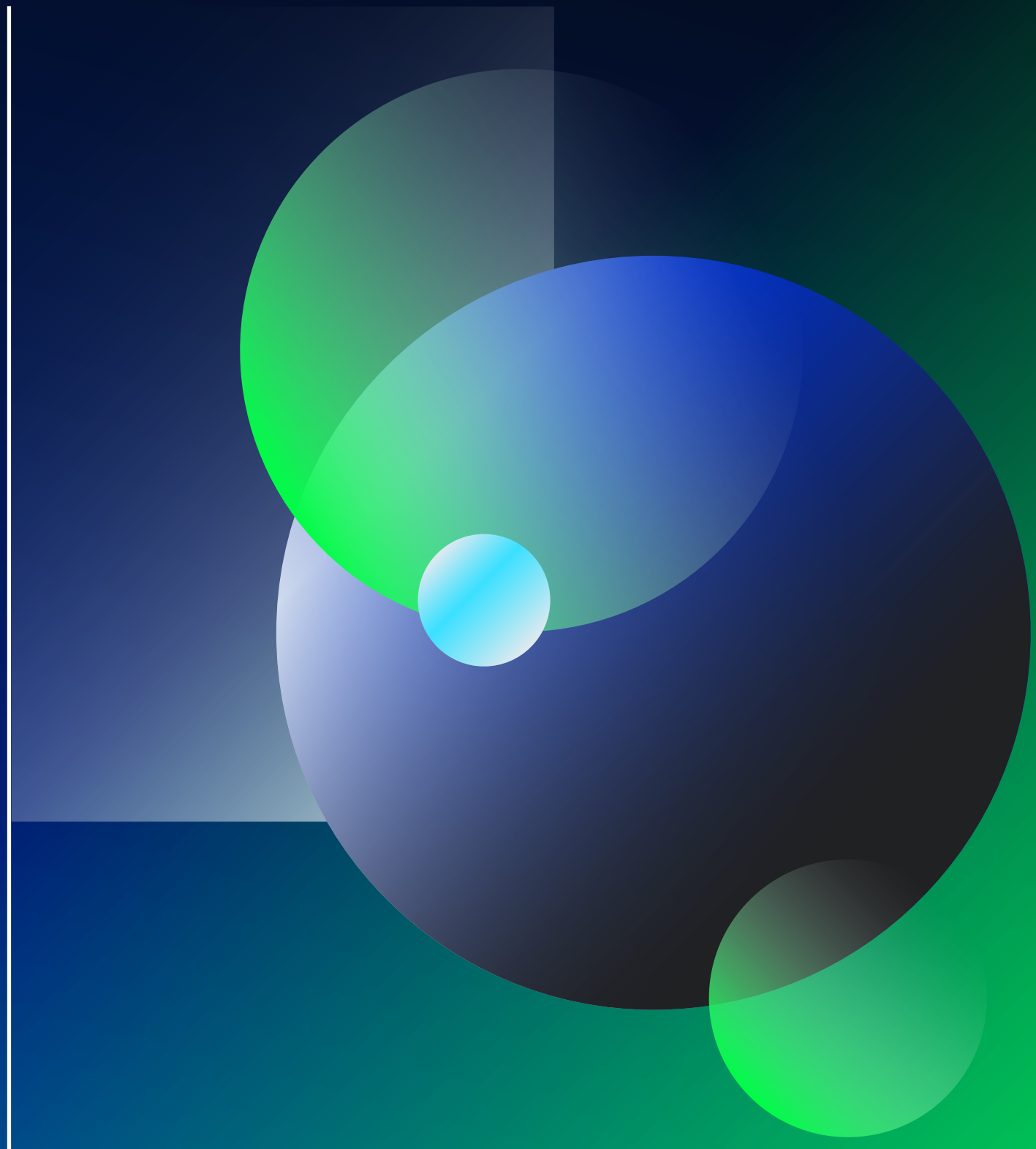
СЕРГЕЙ ДЕМИДОВ

Директор департамента операционных рисков, информационной безопасности и непрерывности бизнеса, Московская биржа

Московская биржа уделяет повышенное внимание информационной безопасности, обрабатывая данные огромного числа пользователей, среди которых только частных инвесторов около 38,6 млн. У нас внедрена система управления информационной безопасностью, соответствующая требованиям российского законодательства и стандарта ISO 27001. Регулярно проводятся организационные и технические мероприятия по обеспечению информационной безопасности, управлению ИТ-инфраструктурой и инцидентами информационной безопасности.

Среди таких мероприятий ранее Московская биржа принимала участие в **международном отраслевом исследовании Cyber Resilience**, которое было построено на доменах NIST CSF. Тогда результаты исследования позволили определить направления для улучшения и сравниться со средними значениями по рынку. С экспертами Управления стратегии, исследований и аналитики АФТ мы решили также обратить внимание коллег финтех-отрасли на вопросы устройства внутренней кибербезопасности и **предлагаем улучшенный подход для самостоятельной оценки** в финансовых организациях.

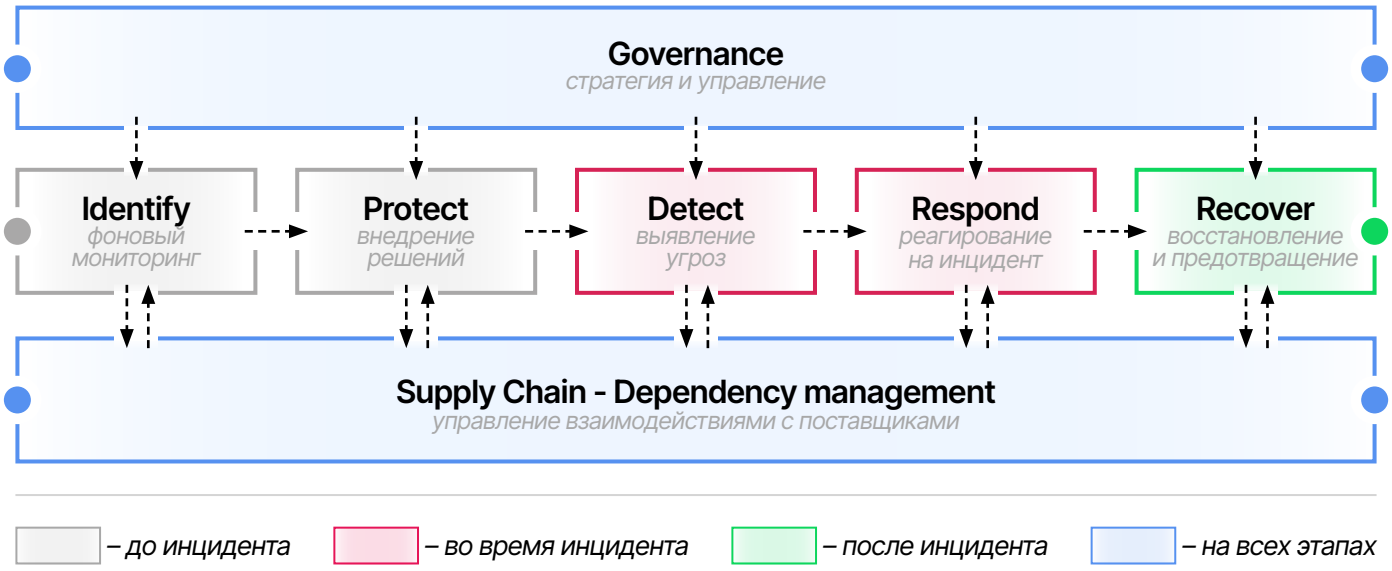
МЕТОДОЛОГИЯ ФРЕЙМВОРКА



ЦЕЛЬ СОЗДАНИЯ ФРЕЙМВОРКА

Содействие повышению уровня зрелости функции кибербезопасности на российском финансовом рынке за счет обеспечения участников АФТ методологией для самостоятельной оценки кибербезопасности по доменам NIST CSF:

Governance	Стратегия & Управление персоналом, ПО, инфраструктурой ИБ
Identify	Мониторинг угроз, управление уязвимостями, рисками и комплаенс
Protect	Внедрение мер защиты и поддержки ИБ (контроль доступа и защита данных)
Detect	Обнаружение угроз безопасности в реальном времени
Respond	Реагирование на инциденты ИБ: экстренные меры и дорожная карта
Recover	Восстановление данных, систем и процессов после инцидента и меры предотвращения
Supply Chain - Dependency management *Добавлено экспертами АФТ*	Управление взаимодействиями с поставщиками



МЕТОДОЛОГИЯ ФРЕЙМВОРКА

За основу подхода были взяты **7 взаимосвязанных доменов кибербезопасности NIST CSF**.
К каждому из доменов Исследования & аналитика и Экспертная группа АФТ предлагают перечень вопросов, ответив на которые можно получить оценку зрелости кибербезопасности организации.

Оценка в зависимости от цели может быть выполнена для определения уровня **ЧАСТНОЙ ЗРЕЛОСТИ** каждого из семи доменов NIST CSF и **ОБЩЕЙ ЗРЕЛОСТИ** кибербезопасности.

01

Уровень общей для всей функции кибербезопасности зрелости предполагается измерять как консолидированную оценку по всем семи доменам NIST CSF.

02

Уровень частной и общей зрелости предполагается измерять как сумму баллов по ответам в опросном листе для самостоятельной оценки.

03

Определены пороговые значения суммы баллов для четырех уровней зрелости кибербезопасности: высокого, среднего, ниже среднего и низкого.

Высокий уровень зрелости:
Governance

Ниже среднего уровень зрелости:
Identify

Низкий уровень зрелости:
Protect

Средний уровень зрелости:
Detect

Высокий уровень зрелости:
Respond

Средний уровень зрелости:
Recover

Средний уровень зрелости:
Supply Chain - Dependency management

↓

ОБЩИЙ уровень зрелости: **средний**

пример

Подход предполагает самостоятельное заполнение опросного листа по фреймворку. Опросник разделен на 7 доменов по NIST SCF. Для каждого из доменов предлагается от 3 до 17 вопросов с вариантами ответов. За каждый вариант ответа можно получить от 0 до 5 баллов.

В зависимости от цели можно заполнить опросный лист по одному, нескольким или всем доменам. Соответственно после суммы баллов по ним будет получена оценка **ОБЩЕЙ** зрелости кибербезопасности (по всем доменам) или **ЧАСТНОЙ** зрелости по конкретному направлению.

СУММА БАЛЛОВ ПО ОЦЕНКЕ ЧАСТНОЙ ЗРЕЛОСТИ КИБЕРБЕЗОПАСНОСТИ

ДОМЕН	УРОВЕНЬ ЗРЕЛОСТИ			
	Высокий	Средний	Ниже среднего	Низкий
Governance	75-60	59-44	43-28	≤ 27
Identity	15-12	11-8	7-4	≤ 3
Protect	85-68	67-50	49-32	≤ 31
Detect	35-28	27-20	19-12	≤11
Respond	45-36	35-26	25-16	≤ 15
Recover	20-16	15-11	10-6	≤ 5
Supply Chain	20-16	15-11	10-6	≤ 5

СУММА БАЛЛОВ ПО ОЦЕНКЕ ОБЩЕЙ ЗРЕЛОСТИ КИБЕРБЕЗОПАСНОСТИ

	УРОВЕНЬ ЗРЕЛОСТИ			
	Высокий	Средний	Ниже среднего	Низкий
ОБЩАЯ СУММА	295-236	235-176	175-116	≤ 115

УРОВНИ ЗРЕЛОСТИ КИБЕРБЕЗОПАСНОСТИ NIST CSF

Высокий уровень зрелости:
Адаптивный (Adaptive)

- Процессы кибербезопасности выстроены и регулярно обновляются в ответ на внешние изменения
- Используются передовые технологии и методы для прогнозирования и предотвращения угроз, в том числе машинное обучение
- Кибербезопасность учитывается при формировании общей стратегии организации

Средний уровень зрелости:
Повторяемый (Repeatable)

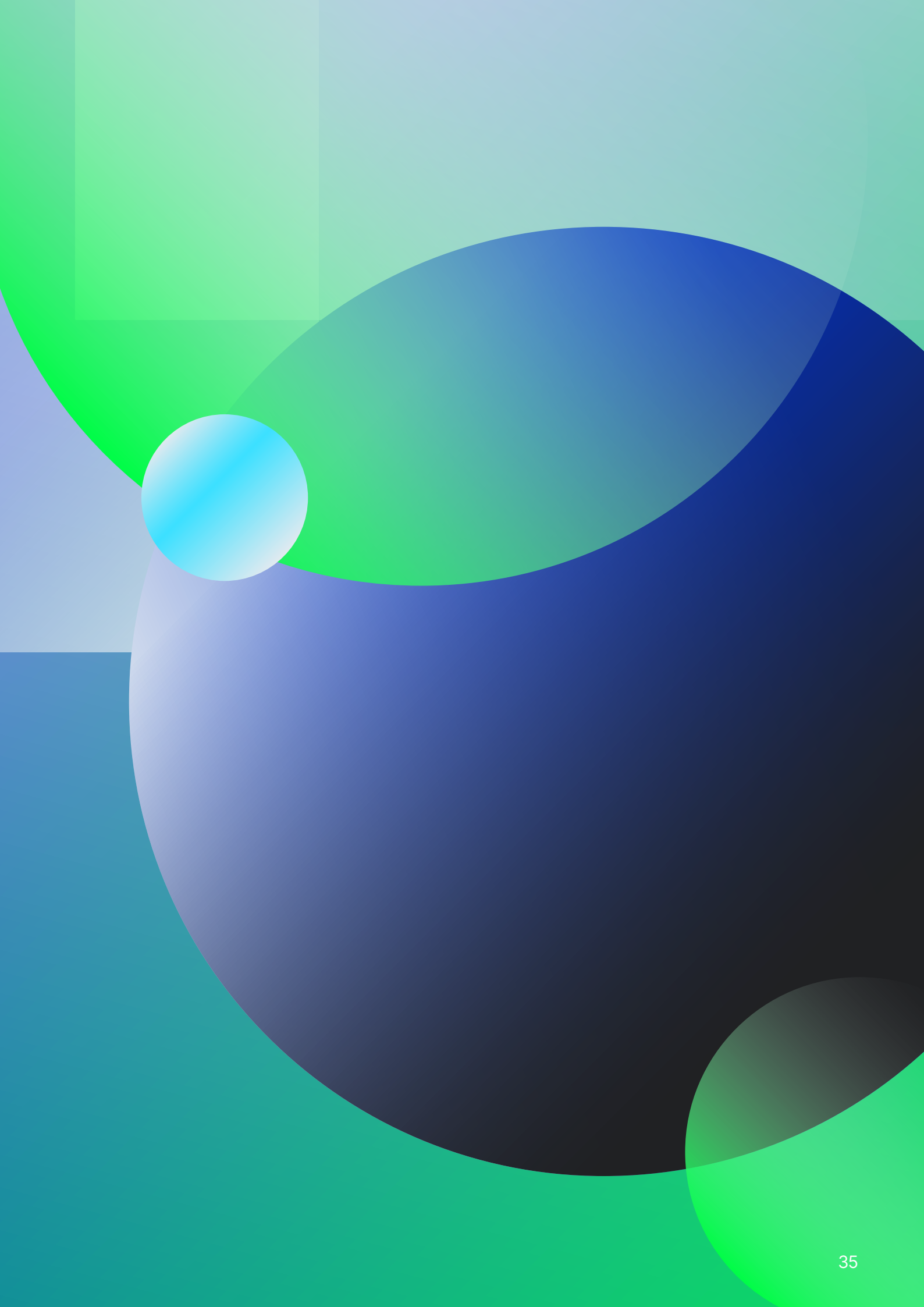
- Процессы кибербезопасности документированы и стандартизированы
- Организация выполняет превентивный мониторинг по инцидентам, меры защитыи планы регулярно обновляются с учетом опыта произошедших инцидентов
- Существует детальное распределение ролей и обязанностей в штатной структуре

Ниже среднего
уровень зрелости:
Формализованный (Risk-Informed)

- Процессы кибербезопасности начинают документироваться и стандартизироваться
- Организация отслеживает произошедшие инциденты и есть планы по их устранению
- Существует базовое понимание ролей и обязанностей по кибербезопасности

Низкий уровень зрелости:
Частичный (Partial)

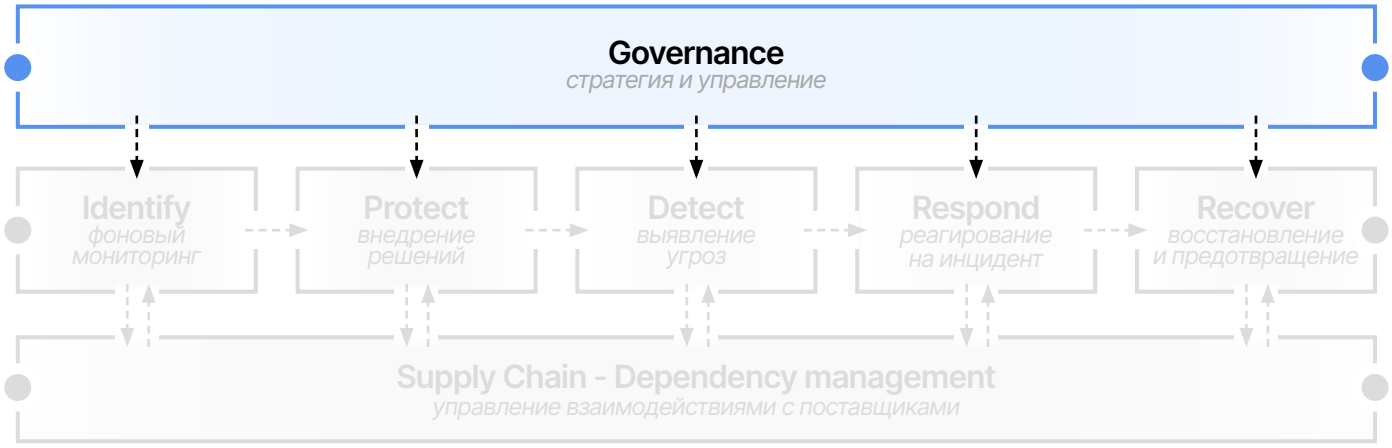
- Процессы кибербезопасности не формализованы и выполняются на ad-hoc основе
- Реагирование на инциденты и управление рисками не систематизированы
- Осведомленность о киберрисках ограничена среди сотрудников



ОПРОСНЫЙ ЛИСТ

01

ДОМЕН GOVERNANCE



GOVERNANCE - СТРАТЕГИЯ & УПРАВЛЕНИЕ ПЕРСОНАЛОМ, ПО, ИНФРАСТРУКТУРОЙ ИБ

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
G.1 Примерный % численности сотрудников ИБ от общей численности организации:	1-10%	1
	11-20%	2
	21-40%	3
	41-60%	4
	>60%	5
	Нет информации/не применимо	0
G.2 Примерный % бюджета ИБ от операционных расходов (OPEX) Организации:	1-10%	1
	11-20%	2
	21-40%	3
	41-60%	4
	>60%	5
	Нет информации/не применимо	0
G.3 Как выделяется функция по контролю за риск-менеджментом (управлением киберрисками)?	Нет такой функции, нет контроля за риск-менеджментом по кибербезопасности (т.е. нет второй линии)	1
	Есть функция, она подчиняется тому же руководителю (например, CIO), что и само управление по киберрискам	2
	Контроль осуществляется управлением корпоративными рисками (ERM) или операционными рисками	3
	Создана 2-я линия - управление по информационным рискам	4
	2-я линия создана и обеспечивает контроль за управлением киберрисками, а также подготовку отчетности по управлению киберрисками; 2-я линия подчиняется директору по управлению рисками (CRO)	5
	Нет информации/не применимо	0

GOVERNANCE - СТРАТЕГИЯ & УПРАВЛЕНИЕ ПЕРСОНАЛОМ, ПО, ИНФРАСТРУКТУРОЙ ИБ

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
G.4 Как часто CIO, CRO, CISO или другой руководитель выступает перед Советом директоров или другим коллегиальным корпоративным органом, принимающим решения, с отчетом по кибербезопасности?	Регулярные отчеты о кибербезопасности перед Советом директоров отсутствуют	**1**
	Только по запросу	**2**
	Один раз в год	**3**
	Один раз в квартал, включая отчеты по обеспечению информационной безопасности (information protection technologies)	**4**
	Каждое заседание Совета директоров, включая отчеты по обеспечению информационной безопасности (information protection technologies)	**5**
	Нет информации/не применимо	**0**
G.5 Какой в вашей организации есть список, реестр или перечень рисков кибербезопасности?	Список рисков отсутствует	**1**
	Неформальный список рисков с некоторой информацией о связанных с ними уязвимостях и затронутом бизнес-процессе или информационном активе (information asset)	**2**
	Принятый формально список основных рисков на корпоративном уровне (top risks at enterprise and business level)	**3**
	Принятый формально полный и консолидированный реестр рисков, охватывающий все бизнес-подразделения и функциональные группы, включая затронутые бизнес-процессы и информационные активы (information assets)	**4**
	Принятый формально полный и консолидированный реестр рисков, охватывающий все бизнес-подразделения и функциональные группы, включая затронутые бизнес-процессы и информационные активы (information assets), официально утвержденный руководителями бизнес-подразделений	**5**
	Нет информации/не применимо	**0**
G.6 Насколько хорошо выполняются сотрудниками вашей организации нормативные требования по кибербезопасности?	Не выполняются	**1**
	Выполняются нерегулярно, а только в ситуациях, связанных с нормативными рисками	**2**
	Выполняются проактивно с целью митигации потенциальных рисков среди внутренних сотрудников	**3**
	Выполняются проактивно с целью митигации потенциальных рисков как среди внутренних, так и привлеченных сотрудников	**4**
	Выполняются проактивно с целью митигации потенциальных рисков как среди внутренних, так и привлеченных сотрудников; проведенные корпоративные опросы отмечают высокий уровень осведомленности о киберрисках среди сотрудников	**5**
	Нет информации/не применимо	**0**

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
G.7 Насколько четко определены должности и обязанности сотрудников, руководства и третьих сторон по кибербезопасности (особенно информационной безопасности)?	Отсутствуют должности и обязанности по кибербезопасности	**1**
	Есть должности и обязанности для некоторых функций (например, только руководящей - CISO)	**2**
	Есть должности и обязанности для большинства функций (как руководящей, так и среднего управленческого звена)	**3**
	Есть должности и обязанности для всех уровней функций	**4**
	Е сть должности и обязанности для всех уровней функций, регулярно обновляемые с учетом перераспределения обязанностей между различными группами (например, с учетом привлечения подрядчиков)	**5**
	Нет информации/не применимо	**0**
G.8 Как политики и стандарты кибербезопасности доводятся до сведения сотрудникам вашей организации?	Нет корпоративной коммуникации по политикам и стандартам по кибербезопасности	**1**
	Политики и стандарты по кибербезопасности доступны для ознакомления сотрудникам через корпоративный портал (например, the intranet)	**2**
	Есть коммуникация по политикам и стандартам по кибербезопасности для но вых сотрудников при приеме на работу, а также документы доступны через корпоративный портал (например, the intranet)	**3**
	Есть коммуникация по политикам и стандартам по кибербезопасности для новых сотрудников при приеме на работу, а также регулярно в течение работы (например, может требоваться прохождение тренингов на периодической основе)	**4**
	Есть коммуникация по политикам и стандартам по кибербезопасности для новых сотрудников при приеме на работу, регулярно в течение работы (например, может требоваться прохождение тренингов на периодической основе), а также документы доступны через корпоративный портал (например, the intranet)	**5**
	Нет информации/не применимо	**0**
G.9 Каким образом операционные команды (например, служба клиентской поддержки) учитывают конфиденциальность обрабатываемой информации?	Процесс работы с клиентами и их информацией всегда одинаковый, уровень конфиденциальности информации не определяется и не учитывается	**1**
	Выполняются нерегулярно, а только в ситуациях, связанных с нормативными рисками	**2**
	Контроль обеспечения защиты информации повышается с уровнем конфиденциальности этой информации	**3**
	Приняты регламентом «безопасные пути» (secure paths) - специальные процессы, используемые для работы с клиентами и информацией, содержащей высокочувствительные данные	**4**
	Для работы с клиентами и информацией, содержащей высокочувствительные данные, используются не только принятые регламентом «безопасные пути» (secure paths) - выстроенные процессы, но и привлекаются эксперты из специального отдела	**5**
	Нет информации/не применимо	**0**

GOVERNANCE - СТРАТЕГИЯ & УПРАВЛЕНИЕ ПЕРСОНАЛОМ, ПО, ИНФРАСТРУКТУРОЙ ИБ

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
G.10 Как осуществляется подбор и обучение специалистов по кибербезопасности?	Нет программы по управлению талантами по кибербезопасности, набор проводится хаотично (ad-hoc)	1
	Нет программы по управлению талантами по кибербезопасности, сотрудники службы безопасности в основном работают неполный рабочий день или являются подрядчиками	2
	Есть сотрудники на основных ролях по кибербезопасности, проводится систематическое отслеживание профессионального соответствия основным сертификациям	3
	Проводится систематический мониторинг всего набора профессиональных знаний и навыков среди всех специалистов по кибербезопасности, выявление пробелов и проведение обязательных к участию тренингов для восполнения пробелов в компетенциях	4
	Проводится систематический мониторинг соответствия всем профессиональным сертификациям среди всех специалистов по кибербезопасности, внесение в реестр рисков выявленных систематических пробелов и проведение обязательных к участию тренингов для восполнения пробелов в компетенциях, а также разработка и внедрение политики и процессов в области управления специалистами по кибербезопасности, поощрение команды кибербезопасности к самообучению/исследованию актуальных практик по профессиональной тематике	5
	Нет информации/не применимо	0
G.11 Как определяются допустимые уровни киберриска?	Организация не приемлет какие-либо киберриски	1
	Есть неформально принятые нормы, что считать допустимым киберриском	2
	Есть устная коммуникация от сотрудников по управлению киберрисками, что считать допустимым киберриском	3
	Есть количественные пороги по допустимым киберрискам и привязка к отчетности по рискам	4
	Есть количественные пороги по допустимым киберрискам и привязка к отчетности по рискам, а также КПЭ	5
	Нет информации/не применимо	0
G.12 Кто, согласно регламенту или руководству высшего звена, несет ответственность за киберриски в организации?	Нет ответственного лица за киберриски	1
	Управление по кибербезопасности несет ответственность за устранение киберрисков	2
	Каждый сотрудник организации несет ответственность за возникновение киберриска по его вине, управление по кибербезопасности несет ответственность за устранение обнаруженных киберрисков	3
	Бизнес-подразделение несет ответственность за возникновение киберрисков, управление по кибербезопасности несет ответственность за устранение киберрисков	4
	Бизнес-подразделение несет ответственность за возникновение киберрисков, управление по кибербезопасности несет ответственность за устранение и содействие снижению киберрисков, управление корпоративными рисками (ERM) осуществляет контроль за управлением киберрисками	5
	Нет информации/не применимо	0

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
G.13 Какая структура у функции кибербезопасности?	Нет управления кибербезопасности или аналогичного подразделения; предполагается, что кибербезопасность обеспечивают ИТ-сотрудники	**1**
	Вопросы кибербезопасности могут быть переданы для решения CIO, однако четкого ответственного лица за их решение нет	**2**
	Есть руководитель по кибербезопасности (например, должность CISO); CISO подчиняется генеральному директору или Совету директоров; нет отдельной должности по кибербезопасности в каждом бизнес-подразделении (ответственность за киберриски лежит только на CISO)	**3**
	Есть руководитель по кибербезопасности (например, должность CISO); CISO подчиняется генеральному директору или Совету директоров; есть отдельная должность по кибербезопасности в каждом бизнес-подразделении (общая ответственность за киберриски)	**4**
	Есть руководитель по кибербезопасности (например, должность CISO); CISO подчиняется CRO; есть отдельная должность по кибербезопасности в каждом бизнес-подразделении (общая ответственность за киберриски); за киберриски также несут ответственность менеджеры проектов и продуктов	**5**
	Нет информации/не применимо	**0**
G.14 Как ваши должность и обязанности учитываются для определения допустимых уровней киберриска?	Уровень допустимого киберриска не связан с должностью и выполняемыми обязанностями	**1**
	Должность (например, руководитель отдела) и обязанности (например, провайдер критической инфраструктуры - critical infrastructure provider) редко учитываются при определении допустимого уровня киберриска	**2**
	Должность (например, руководитель отдела) и обязанности (например, провайдер критической инфраструктуры - critical infrastructure provider) обычно учитываются при определении допустимого уровня киберриска	**3**
	Должность (например, руководитель отдела) и обязанности (например, провайдер критической инфраструктуры - critical infrastructure provider) всегда учитываются при определении допустимого уровня киберриска, но только для руководящих должностей	**4**
	Должность (например, руководитель отдела) и обязанности (например, провайдер критической инфраструктуры - critical infrastructure provider) всегда учитываются при определении допустимого уровня киберриска, а также регулярно пересматриваются с учетом обновления перечня киберрисков	**5**
	Нет информации/не применимо	**0**
G.15 Какие действия предпринимаются в отношении сотрудников вашей организации, если сотрудники нарушают требования по кибербезопасности, а именно - не проходят тестирование или пропускают обучение?	Не предпринимаются никакие действия	**1**
	Иногда в крайних случаях (например, отсутствие даже старта прохождения тренингов, провал всех тестов), принимаются неформальные меры (прямая коммуникация/напоминание)	**2**
	Введен официальный дисциплинарный процесс в случае нарушения сотрудниками политик безопасности	**3**
	Введен официальный дисциплинарный процесс в случае нарушения сотрудниками политик безопасности, доступ к рабочим программам и данным ограничивается до тех пор, пока сотрудник не пройдет тренинг или нужное обучение	**4**
	Введен официальный дисциплинарный процесс в случае нарушения сотрудниками политик безопасности, доступ к рабочим программам и данным ограничивается до тех пор, пока сотрудник не пройдет тренинг или нужное обучение, вводится усиленный мониторинг за действиями пользователя в системах до тех пор, пока сотрудник не пройдет тренинг или нужное обучение	**5**
	Нет информации/не применимо	**0**

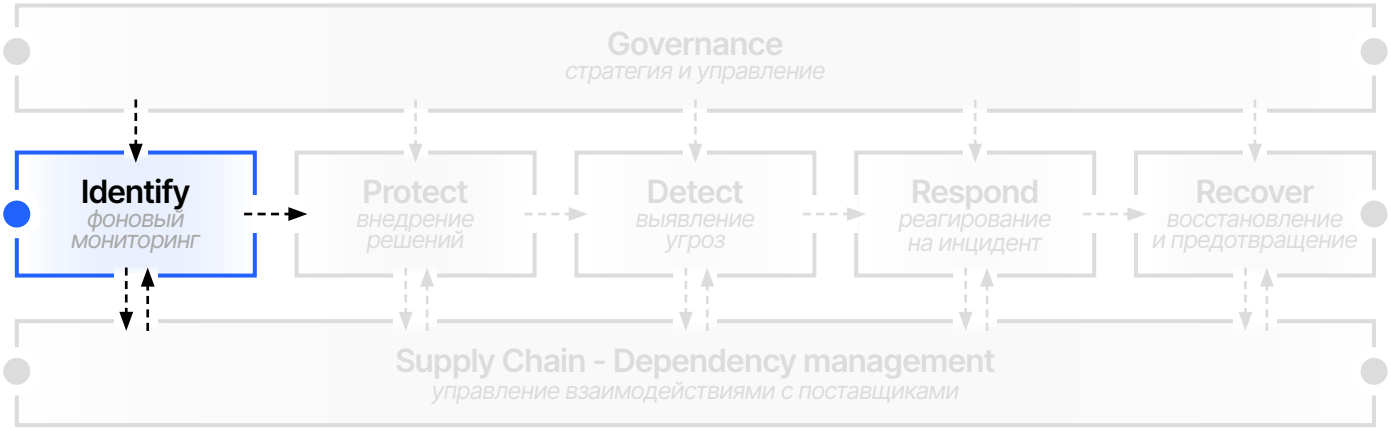
CASE STUDY: GOVERNANCE

Согласно опросу Национальной ассоциации корпоративных директоров (NACD) в США, проведенному в 2025 году, 77% директоров публичных компаний заявили, что за последний год на заседаниях совета обсуждались потенциальные финансовые убытки от возможного киберинцидента. Для сравнения, двумя годами ранее таких организаций было менее половины. Также около 72% членов советов директоров прошли в 2025 году хотя бы один специальный обучающий курс или семинар по киберрискам. Ранее руководители такого уровня редко лично участвовали в подобных мероприятиях. Менеджмент признает, что киберугрозы, например, ransomware, утечки данных, сбои из-за атак, могут поколебать позиции бизнеса не меньше, чем традиционные финансовые или операционные риски.

Источники: NACD Public Company, АО «Позитив Текнолоджиз»

02

ДОМЕН IDENTIFY



IDENTIFY - МОНИТОРИНГ УГРОЗ, УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ, РИСКАМИ И КОМПЛАЕНС

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
I.1 Какой список или реестр информационных активов ведется в вашей организации (т.е. чувствительных данных и/или систем, которые хранят или обрабатывают данные)?	Нет списка или реестра информационных активов - не проводится их инвентаризация	1
	Есть неформальный список информационных активов	2
	Есть неформальный список информационных активов, основанный на информации о применении	3
	Есть полная база данных по всем информационным активам; определены на бизнес-функциональном уровне, а не на основании цепочки создания коммерческой ценности	4
	Есть полная база данных по всем информационным активам; активы определены на основании цепочки создания коммерческой ценности; у каждого информационного актива есть владелец	5
	Нет информации/не применимо	0
I.2 Как распределяются информационные активы в соответствии с коммерческой ценностью и рисками?	Нет приоритизации информационных активов по коммерческой ценности и рискам	1
	Проводится неформальная классификация информационных активов в соответствии с коммерческой ценностью и рисками	2
	Собирается информация о киберугрозах на разовой основе, и в организации нет определенного набора источников	3
	Проводится неформальная классификация информационных активов в соответствии с коммерческой ценностью и рисками	4
	Проводится формальная классификация информационных активов в соответствии с коммерческой ценностью и рисками	5
	Нет информации/не применимо	0
I.3 Какие источники используются в вашей организации для получения информации о киберугрозах?	Собирается информация о киберугрозах на разовой основе, и в организации нет определенного набора источников	1
	В организации регулярно собирается информация о киберугрозах из утвержденных по внутренним процедурам источников, но все эти источники открыты (например, новостные сообщения и блоги)	2
	В организации регулярно собирается информация о киберугрозах из утвержденных по внутренним процедурам открытых и платных источников (например, от поставщиков средств обеспечения безопасности)	3
	В организации регулярно собирается информация о киберугрозах из утвержденных по внутренним процедурам открытых и платных источников, а также специализированных поставщиков аналитических данных о киберугрозах	4
	В организации регулярно собирается информация о киберугрозах из утвержденных по внутренним процедурам открытых и платных источников, а также специализированных поставщиков аналитических данных о киберугрозах и партнеров по отрасли (например, через участников ISAC и соглашения об обмене данными)	5
	Нет информации/не применимо	0

CASE STUDY: IDENTIFY

РТК ИТ Плюс РСХБ

Внедрение отечественной платформы «Диво» в Россельхозбанке продемонстрировало, как учет ИТ-активов напрямую усиливает информационную безопасность.

В рамках проекта по импортозамещению ITSM-системы был создан сервисный каталог, который охватил более 700 сервисов, включая ИТ-услуги, административно-хозяйственные задачи, процессы централизованного обслуживания и другие ключевые функции. При реализации проекта в новую систему были перенесены более 150 000 пользовательских записей, 6 376 записей агентов, 4 500 рабочих групп и свыше 200 000 значений из справочников. Переход на новую платформу прошел практически бесшовно – благодаря продуманным интеграциям, синхронизации старых и новых связей, а также заранее выстроенной логике переноса и настройки. Переход на платформу «Диво» также стал важной точкой отказа от традиционного подхода к разработке – теперь процессы настраиваются через визуальный интерфейс и принципы low-code. Это позволило в четыре раза сократить сроки внедрения изменений и запускать новые процессы, которые ранее были невозможны в старой системе.

Источник: АО «Россельхозбанк».

MOEX МОСКОВСКАЯ БИРЖА

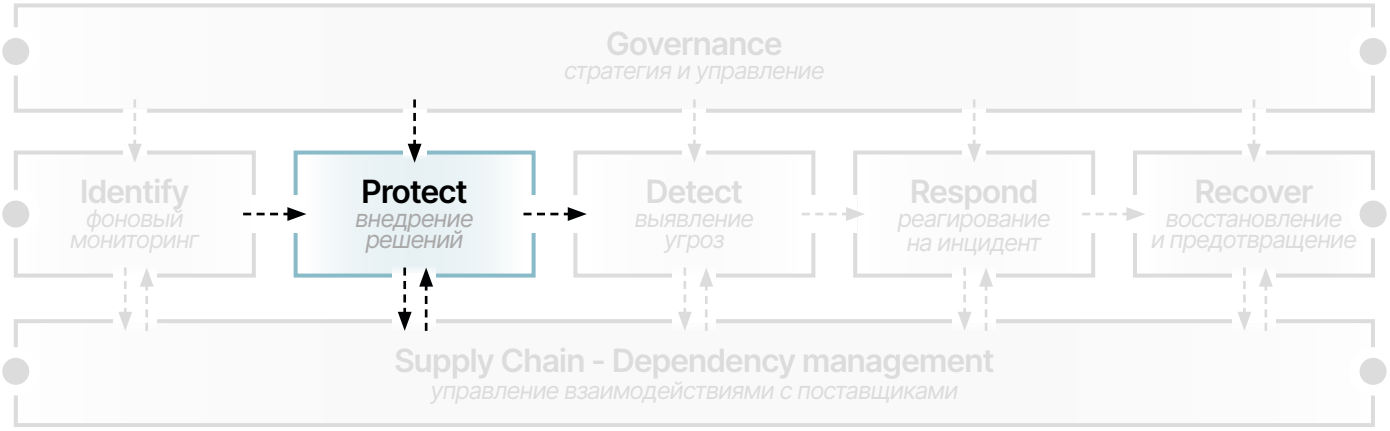
В октябре 2025 года Московская биржа запустила платформу Compliance Tool: комплексное решение для эмитентов и профессиональных участников рынка для построения эффективной системы внутреннего контроля, выполнения регуляторных требования и взаимодействия с биржевой инфраструктурой.

Платформа включает 4 сервиса: система учета инсайдеров, взаимодействие, контроль сделок инсайдеров и проверку совпадения контрагента. Благодаря Compliance Tool, можно формировать списки инсайдеров с защитой данных по стандартам ИБ и выстраивать коммуникацию комплаенс-подразделений участников торгов и биржи при проверке торговых операций. Платформа позволяет осуществлять контроль за соблюдением инсайдерами условий совершения операций с финансовыми инструментами, до 95% сокращая трудозатраты по выявлению рисков.

Источник: ПАО «Московская Биржа ММВБ-РТС».

03

ДОМЕН PROTECT



PROTECT - ВНЕДРЕНИЕ МЕР ЗАЩИТЫ И ПОДДЕРЖКИ ИБ (КОНТРОЛЬ ДОСТУПА И ЗАЩИТА ДАННЫХ)

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
P.1 Как в вашей организации адаптируется коммуникация и обучение по вопросам кибербезопасности для различных групп сотрудников?	Коммуникация не адаптируется, обучения по кибербезопасности в организации нет	**1**
	Все сотрудники получают одинаковую коммуникацию и проходят одинаковое обучение	**2**
	Только для высокорисковых групп (например, разработчиков приложений и высшего руководства) проводится определенная адаптация коммуникации и обучений по таким темам, как резервное копирование, настройка конфигурации данных, соблюдение политики и нормативных требований к операционной среде, уничтожение данных	**3**
	Проводится индивидуальное обучение и направляется индивидуальная коммуникация для отдельных групп сотрудников, регулярная рассылка информации и обновлений по информационной безопасности для всей организации с целью информирования об изменениях в области рисков и соответствия требованиям, направляется дополнительная информация о соблюдении политики безопасности на основе матрицы ролей по рискам, наиболее связанным с ролью в организации	**4**
	Проводится индивидуальное обучение и направляется индивидуальная коммуникация для отдельных групп сотрудников, регулярная рассылка информации и обновлений по информационной безопасности для всей организации с целью информирования об изменениях в области рисков и соответствия требованиям, направляется дополнительная информация о соблюдении политики безопасности на основе матрицы ролей по рискам, наиболее связанным с ролью в организации; мотивация для сотрудников кибербезопасности во время программ обучения внести свой вклад (например, обучение сотрудников первой линии выявлять подозрительное поведение пользователей и сообщать о нем в SOC)	**5**
	Нет информации/не применимо	**0**
P.2 Как осуществляется управление активами, которые хранят или обрабатывают информацию?	В организации отсутствует формализованная программа управления активами, которые хранят или обрабатывают информацию	**1**
	Активы, которые хранят или обрабатывают информацию, идентифицируются, инвентаризируются и управляются на ad-hoc основе (по запросу)	**2**
	Существует формализованная программа по управлению активами, которые хранят или обрабатывают информацию; нет уверенности в том, что все активы включены в программу	**3**
	Существует формализованная программа по управлению активами, которые хранят или обрабатывают информацию; большинство активов (более 50%) включены в программу	**4**
	Существует формализованная программа по управлению активами, которые хранят или обрабатывают информацию; все активы организации идентифицируются, инвентаризируются и управляются в соответствии с политикой и процедурами управления активами	**5**
	Нет информации/не применимо	**0**

PROTECT - ВНЕДРЕНИЕ МЕР ЗАЩИТЫ И ПОДДЕРЖКИ ИБ (КОНТРОЛЬ ДОСТУПА И ЗАЩИТА ДАННЫХ)

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
P.3 Как управляются базовые (baseline) конфигурации программ и систем?	У нас отсутствуют базовые (baseline) конфигурации для приложений и систем	**1**
	Используются базовые (baseline) конфигурации для высокорисковых систем и программ (например, контроллеров домена и веб-серверов), но управление по кибербезопасности не является владельцем конфигураций и не управляет ими (конфигурации настройки были получены из внешнего источника)	**2**
	Используются базовые (baseline) конфигурации для высокорисковых систем и программ (например, контроллеров домена и веб-серверов), и базовые (baseline) конфигурации были разработаны управлением по кибербезопасности или по заказу управления по кибербезопасности	**3**
	Используются базовые (baseline) конфигурации для большинства или всех систем и программ и проверяется их соответствие утвержденным базовым конфигурациям на ad-hoc основе	**4**
	Используются базовые (baseline) конфигурации для большинства или всех систем и программ, также есть автоматизированный регулярный мониторинг соответствия утвержденным базовым конфигурациям	**5**
	Нет информации/не применимо	**0**
P.4 Как в вашей организации обеспечивается кибербезопасность в программах или системах, которые работают в корпоративном (private) облаке?	У нас нет программ или систем, работающих в private облаке	**1**
	Только стандартные средства безопасности, предусмотренные провайдером корпоративного (private) облака организации	**2**
	Разработана и внедрена программа кибербезопасности, продуманная для основных корпоративных (private) облаков, которые использует организация, и проведено нагрузочное тестирование инструментов программы	**3**
	Разработана и внедрена программа кибербезопасности, продуманная для основных корпоративных (private) облаков, которые использует организация, и проведено нагрузочное тестирование инструментов программы, а также предусмотрено снижение рисков при удалении/ перемещении активов	**4**
	Разработана и внедрена программа кибербезопасности, продуманная для основных корпоративных (private) облаков, которые использует организация, и проведено нагрузочное тестирование инструментов программы, а также предусмотрено снижение рисков при удалении/ перемещении активов и внедрена защита от утечки данных	**5**
	Нет информации/не применимо	**0**
P.5 Как в вашей организации о беспечивается кибербезопасность в программах или системах, которые работают в публичном (public) облаке?	У нас нет программ или систем, работающих в публичном (public) облаке	**1**
	Только стандартные средства безопасности, предусмотренные провайдером публичного (public) облака организации	**2**
	Разработана и внедрена программа кибербезопасности, продуманная для основных публичных (public) облаков, которые использует организация, и проведено нагрузочное тестирование инструментов программы	**3**
	Разработана и внедрена программа кибербезопасности, продуманная для основных публичных (public) облаков, которые использует организация, и проведено нагрузочное тестирование инструментов программы, а также предусмотрено снижение рисков при удалении/перемещении активов	**4**
	Разработана и внедрена программа кибербезопасности, продуманная для основных публичных (public) облаков, которые использует организация, и проведено нагрузочное тестирование инструментов программы, а также предусмотрено снижение рисков при удалении/перемещении активов и внедрена защита от утечки данных	**5**
	Нет информации/не применимо	**0**

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
P.6 Какой процент корпоративной инфраструктуры (hardware) полностью обновлен патчами или отстает от них всего на один патч?	Менее 20%	**1**
	Более 21%, но менее 50%	**2**
	Более 51%, но менее 80%	**3**
	Более 81%, но менее 90%	**4**
	Более 91%	**5**
	Нет информации/не применимо	**0**
P.7 Какие механизмы проверки целостности аппаратного и программного обеспечения используются?	Нет механизмов проверки целостности	**1**
	Проводятся специальные проверки внешней и функциональной целостности (например, на уровне файловой системы и пользователя)	**2**
	Проводятся множественные проверки физической и функциональной целостности (например, зеркалирование, проверка RAID) регулярно в определенных подразделениях организации и нерегулярно в других (например, используются последовательно с оборудованием и драйверами, но не на уровне файловой системы или пользователя)	**3**
	Проводятся множественные проверки физической и функциональной целостности (например, зеркалирование, проверка RAID) регулярно в большинстве подразделений организации и нерегулярно в других (например, используются последовательно с оборудованием и драйверами, но не на уровне файловой системы или пользователя)	**4**
	Проводятся множественные проверки физической и функциональной целостности (например, зеркалирование, проверка RAID) во всех подразделениях организации; методы включают ведение журнала проверок, криптографические файловые системы, CRC и проверки целостности диска	**5**
	Нет информации/не применимо	**0**
P.8 Какой процент разработчиков в вашей организации прошли обучение по безопасной разработке?	Менее 20%	**1**
	Более 21%, но менее 50%	**2**
	Более 51%, но менее 80%	**3**
	Более 81%, но менее 90%	**4**
	Более 91%	**5**
	Нет информации/не применимо	**0**
P.9 Как обеспечивается безопасность удаленного доступа (например, VPN и удаленного рабочего стола)?	Безопасность удаленного доступа не контролируется (например, сотрудникам разрешается использовать собственные решения)	**1**
	Есть политики, регулирующие безопасность удаленного доступа, но они не подкреплены средствами безопасности	**2**
	Есть политики и некоторые средства контроля для мониторинга, но нет доп. контролей	**3**
	Есть средства безопасности и политики ИБ, но привилегированным пользователям не запрещено использовать собственные решения	**4**
	Есть средства безопасности, политики ИБ и доп. контроли, которые запрещают использование несогл. решений или настройку конфигураций	**5**
	Нет информации/не применимо	**0**

PROTECT - ВНЕДРЕНИЕ МЕР ЗАЩИТЫ И ПОДДЕРЖКИ ИБ (КОНТРОЛЬ ДОСТУПА И ЗАЩИТА ДАННЫХ)

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
P.10 Какая сегментация сети (network segmentation) в вашей организации против злоумышленников?	В организации плоская сеть (flat) с небольшим количеством сегментов	1
	Выполнена сегментация сети tired для снижения риска для критических информационных активов, идентификация всех потоков данных по запросам сотрудников и автоматических запросов с серверов	2
	Выполнена сегментация сети, при этом она сегментирована по регионам или бизнес-подразделениям	3
	Выполнена сегментация сети, при этом наиболее чувствительная информация хранится в более защищенных сегментах сети	4
	Выполнена сегментация сети, при этом разделение сетевых ресурсов выполнено в зависимости от должности; выполняется мониторинг, идентификация и оповещение о межфункциональных доступах	5
	Нет информации/не применимо	0
P.11 Как осуществляется управление сущностями, учетными данными и доступами?	Менее 20% сущностей, учетных данных и доступов активно управляются (например, с учетом принципа наименьших привилегий, разделения доступов и минимальной функциональности)	1
	Активное управление сущностями, учетными данными и доступами осуществляется менее чем для 50%, но более чем для 21%	2
	Активное управление сущностями, учетными данными и доступами осуществляется менее чем для 80%, но более чем для 51%; управление доступами включает в себя и удаленный доступ	3
	Активное управление сущностями, учетными данными и доступами осуществляется менее чем для 90%, но более чем для 81%; управление доступами выполнено в соответствии с сегментацией сети	4
	Более 91% сущностей, учетных данных и доступов активно управляется; управление доступами выполнено в соответствии с сегментацией сети	5
	Нет информации/не применимо	0
P.12 Какой процент программ и систем использует централизованное решение для обеспечения идентификации пользователя и обеспечения доступами?	Отсутствует централизованное решение для идентификации и предоставления доступов	1
	1-25% программ и систем используют централизованное решение для идентификации и предоставления доступов	2
	26-50% программ и систем используют централизованное решение для идентификации и предоставления доступов	3
	51-75% приложений и систем используют централизованное решение для идентификации и предоставления доступов	4
	Более 75% программ и систем используют централизованное решение для идентификации и предоставления доступов	5
	Нет информации/не применимо	0
P.13 Какой процент систем и программ проходит проверку для уточнения/обновления списка авторизованных пользователей и связанных с ними доступов не реже одного раза в год?	Проверка проводится реже одного раза в год	1
	1-25% программ и систем проходит проверку не реже одного раза в год для уточнения/обновления списка авторизованных пользователей и связанных с ними доступов	2
	26-50% программ и систем проходит проверку не реже одного раза в год для уточнения/обновления списка авторизованных пользователей и связанных с ними доступов	3
	51-75% программ и систем проходит проверку не реже одного раза в год для уточнения/обновления списка авторизованных пользователей и связанных с ними доступов	4
	Более 76% программ и систем проходит проверку не реже одного раза в год для уточнения/обновления списка авторизованных пользователей и связанных с ними доступов	5
	Нет информации/не применимо	0

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
P.14 Как в вашей организации используется многофакторная аутентификация (MFA)?	Не используется многофакторная аутентификация для доступа к информационным активам	**1**
	Многофакторная аутентификация используется только для удаленного доступа	**2**
	Многофакторная аутентификация используется для удаленного доступа и доступа к системам, которые хранят и/или обрабатывают чувствительные данные	**3**
	Многофакторная аутентификация используется для контроля доступа ко всем высокорисковым системам	**4**
	Многофакторная (двух- и более факторная) аутентификация используется для доступа ко всем программам и системам	**5**
	Нет информации/не применимо	**0**
P.15 Как в цикле разработки новых продуктов и услуг учитываются требования к обеспечению кибербезопасности?	Требования к обеспечению кибербезопасности не учитываются	**1**
	Требования к обеспечению кибербезопасности одинаковые для всех продуктов и услуг	**2**
	Требования к обеспечению кибербезопасности учитываются на усмотрение менеджера проекта или менеджера продукта	**3**
	Цикл разработки продуктов и услуг предусматривает проверку соответствия требованиям кибербезопасности, но нет уверенности в актуализация перечня киберрисков	**4**
	Цикл разработки продуктов и услуг предусматривает проверку соответствия требованиям кибербезопасности с дополнительной проверкой наиболее важных/критических проектов	**5**
	Нет информации/не применимо	**0**
P.16 Как контролируется удаленное подключение третьих сторон – поддержки/ вендоров?	Разрешено ad-hoc предоставление удаленного доступа третьим сторонам поддержке/вендорам	**1**
	Предоставление удаленного доступа в каждом случае определяется индивидуально в соответствии с политиками ИБ	**2**
	Предоставление удаленного доступа в каждом случае определяется индивидуально в соответствии с политиками ИБ, MFA необходима	**3**
	Предоставление удаленного доступа в каждом случае определяется индивидуально в соответствии с политиками ИБ, MFA необходима, сегментация сети	**4**
	Предоставление удаленного доступа в каждом случае определяется индивидуально в соответствии с политиками ИБ, MFA необходима, сегментация сети, полное ведение журнала сеансов	**5**
	Нет информации/не применимо	**0**
P.17 Как анализируется информация для выявления атак/детекции киберриска?	Не отслеживается информация для выявления атак	**1**
	Анализируется только информация из программ по обеспечению безопасности (SIEM) и генерируемым оповещениям	**2**
	Анализируется информация из программ по обеспечению безопасности (SIEM), генерируемым оповещениям и расширенной аналитики для выбранных доменов (например, сетевой форензик)	**3**
	Анализируется информация из программ по обеспечению безопасности (SIEM), генерируемым оповещениям, расширенной аналитики для выбранных доменов (например, сетевой форензик), а также лог-мониторингу и IP-трафику	**4**
	Проводится анализ и оценка корреляции по информации из программ по обеспечению безопасности (SIEM), генерируемым оповещениям, расширенной аналитики для выбранных доменов (например, сетевой форензик), а также лог-мониторингу и IP-трафику	**5**
	Нет информации/не применимо	**0**

CASE STUDY: PROTECT

Приложение Яндекс ID (ранее – Яндекс Ключ) теперь полноценный центр управления аккаунтом на Яндексе: с его помощью можно держать под контролем все данные и настройки. В Яндекс ID можно просмотреть список всех устройств, с которых выполнен вход, а также настроить способы восстановления доступа. Приложение также сообщает пользователю о каждом входе в его аккаунт в пуш-уведомлении.

Яндекс ID генерирует одноразовые коды (RFC TOTP) для входа на ресурсы, где есть двухфакторная аутентификация, например «Госуслуги». Подход к безопасности с Яндекс ID с оответствует лучшим мировым практикам, что подтверждает сертификат ISO/IEC 27001.

Источник: ООО «Яндекс»

Крупнейшая страховая компания Ирландии Vhi Healthcare внедрила биометрическую аутентификацию от HYPR для более 1 млн клиентов. Решение повышает безопасность предоставления сервисов, снижает операционные расходы и улучшает пользовательский опыт. Внедрение беспарольной технологии позволило полностью отказаться от затрат на сброс паролей, одновременно остановив атаки с использованием украденных учётных данных. Это решение не только обеспечило соответствие строгим требованиям PSD2 для сильной аутентификации клиентов (SCA), но и значительно повысило удобство для пользователей всех возрастов, включая пожилых людей с телефонами без современных защитных технологий.

В результате Vhi Healthcare добилась существенного повышения продуктивности службы поддержки и качества обслуживания клиентов, создав безопасную и интуитивно понятную цифровую экосистему для здоровья.

Источник: Vhi Healthcare

CASE STUDY: PROTECT

Альфа Банк + T1 Облако

Альфа-Банк и T1 Облако запустили гибридную облачную инфраструктуру на базе графических ускорителей для тестирования и внедрения генеративного ИИ, где ключевой приоритет - это защита данных.

Платформа адаптирована под строгие банковские стандарты с усиленным логированием, мониторингом, безопасными API и защищенными каналами между дата-центрами, обеспечивая надежность и масштабируемость для внутренней ИИ-платформы AlfaGen. Решение позволяет быстро прототипировать сервисы вроде ИИ-ассистентов для разработчиков и аналитики.

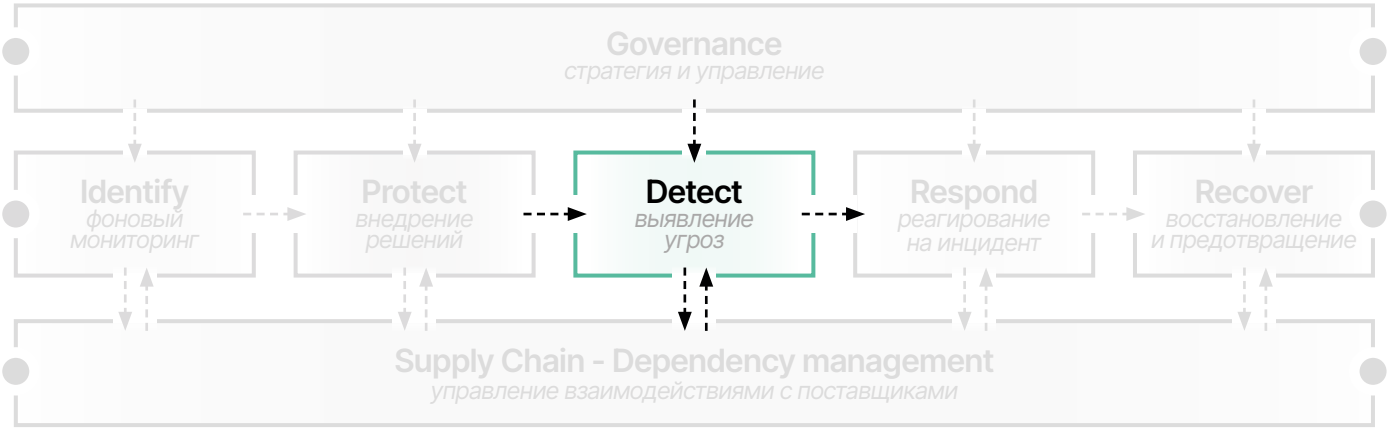
Источник: АО «Альфа-Банк», ООО «Т1Клауд»

АНТОН СТЕПАНОВ
Генеральный директор, T1 Облако

Сегодня оперативное подключение высокопроизводительных вычислительных ресурсов через облако — частый запрос крупного бизнеса. Нашей задачей было – помочь Альфа-Банку в создании информационной платформы, которая позволит гибко и, самое главное, безопасно внедрять инструменты генеративного ИИ. Команда T1 Облако провела серьезную работу над созданием надежной гибридной инфраструктуры, соответствующей стандартам безопасности, а экспертиза Альфа-Банка в комплексной поддержке ИТ-систем позволила плавно интегрировать ее в процессы компании.

04

ДОМЕН DETECT



DETECT - ОБНАРУЖЕНИЕ УГРОЗ БЕЗОПАСНОСТИ В РЕАЛЬНОМ ВРЕМЕНИ

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
D.1 Как выявляется аномальное поведение пользователя?	SIEM не отслеживает поведение пользователей	**1**
	SIEM мониторит поведение пользователя на основе лог-записей с сетевых устройств и систем; предусмотрены оповещения, за которыми следят сотрудники службы безопасности	**2**
	SIEM мониторит поведение пользователя на основе лог-записей с сетевых устройств и систем; предусмотрены оповещения, за которыми следят сотрудники службы безопасности определены роли и обязанности по обнаружению подозрительной активности	**3**
	SIEM мониторит поведение пользователя на основе лог-записей с сетевых устройств и систем; предусмотрены оповещения, за которыми следят сотрудники службы безопасности определены роли и обязанности по обнаружению подозрительной активности; есть расширенная аналитика по поведению пользователей для прогнозирования; есть автоматическое обнаружение аномальных событий в действиях пользователя и возможность внесения изменений/обновлений в программу	**4**
	SIEM мониторит поведение пользователя на основе лог-записей с сетевых устройств и систем; предусмотрены оповещения, за которыми следят сотрудники службы безопасности определены роли и обязанности по обнаружению подозрительной активности; есть расширенная аналитика по поведению пользователей для прогнозирования; есть автоматическое обнаружение аномальных событий в действиях пользователя и возможность внесения изменений/обновлений в программу; роли и обязанности по обнаружению подозрительной активности постоянно обновляются/дополняются	**5**
	Нет информации/не применимо	**0**
D.2 Какие шаги предпринимаются управлением кибербезопасности для обнаружения вредоносного кода (вирусов/червей)?	Управление кибербезопасности не применяет средства/методы для обнаружения вирусов/червей	**1**
	Используются антивирусы для мониторинга сети и рабочих мест (end-points)	**2**
	Используются антивирусы для мониторинга сети и рабочих мест (end-points), а также специализированные решения для обнаружения вредоносных программ (malware)	**3**
	Используются антивирусы для мониторинга сети и рабочих мест (end-points), а также специализированные решения для обнаружения вредоносных программ (malware), которые обновляются на периодической основе	**4**
	Используются антивирусы для мониторинга сети и рабочих мест (end-points), а также специализированные решения для обнаружения вредоносных программ (malware), которые обновляются на периодической основе, а также используются передовые методы, такие как машинное обучение для обнаружения ранее неизвестных образцов вредоносных программ	**5**
	Нет информации/не применимо	**0**

DETECT - ОБНАРУЖЕНИЕ УГРОЗ БЕЗОПАСНОСТИ В РЕАЛЬНОМ ВРЕМЕНИ

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
D.3 Какой процент ИТ-ландшафта активно мониторится?	Отслеживается менее 20% сетей и систем	**1**
	Менее 50%, но более 21% сетей и систем	**2**
	Менее 80%, но более 51% сетей и систем	**3**
	Менее 90%, но более 81% сетей и систем	**4**
	Более 90% сетей и систем находятся под активным мониторингом, а также ведется непрерывная работа по постоянному совершенствованию/обновлению средств мониторинга	**5**
	Нет информации/не применимо	**0**
D4 Как обеспечивается кибербезопасность мобильных устройств сотрудников?	Нет программы обеспечения безопасности мобильных устройств сотрудников	**1**
	Проводится мониторинг кибербезопасности мобильных устройств, предоставляемых организацией, и связанных с ними данных	**2**
	Проводится мониторинг кибербезопасности мобильных устройств, предоставляемых организацией, и связанных с ними данных, а также собственных мобильных устройств сотрудников (BYOD), если устройства используются для выполнения рабочих задач; на них устанавливаются VPN и инструменты мониторинга использования данных и приложений	**3**
	Есть служба управления мобильными устройствами (MDM), которая обеспечивает удаленную очистку и защиту от потери данных; отслеживание потерянных устройств и отслеживание оборудования, имеющего доступ к чувствительным данным; настроена изолированная среда (sandbox) для корпоративных приложений на собственных устройствах сотрудников для выполнения рабочих задач	**4**
	Есть служба управления мобильными устройствами (MDM), которая обеспечивает удаленную очистку и защиту от потери данных; отслеживание потерянных устройств и отслеживание оборудования, имеющего доступ к чувствительным данным; выполнено 100% шифрование рабочих данных; возможно использование корпоративных приложений или данных на собственных устройствах сотрудников для выполнения рабочих задач без изолированной среды	**5**
	Нет информации/не применимо	**0**
D.5 Как работает служба форензика в управлении по кибербезопасности?	Нет службы форензика в управлении по кибербезопасности	**1**
	Форензик проводится интуитивно и нерегулярно на добровольной основе сотрудниками в управлении по кибербезопасности - нет обученных специалистов или специализированных инструментов службы форензика	**2**
	Есть специализированные инструменты форензика, и некоторые участники нашей команды знают, как ими пользоваться, но нет специально выделенной команды форензика	**3**
	Есть полный набор инструментов для форензика и команда специалистов, которая совмещает обязанности по обеспечению кибербезопасности и форензику	**4**
	Есть полный набор инструментов для форензика и отдельная команда специалистов; регулярно проводятся тренинги и обучения по повышению знаний и навыков, следуя продуманной программе или стратегии развития форензика	**5**
	Нет информации/не применимо	**0**

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
D. 6 Какой процент ИТ-ландшафта проверяется (по крайней мере, ежемесячно) на наличие уязвимостей?	Менее 20% сетей и систем	**1**
	Менее 50%, но более 21% сетей и систем	**2**
	Менее 80%, но более 51% сетей и систем	**3**
	Менее 90%, но более 81% сетей и систем	**4**
	Более 90% сетей и систем проверяется на наличие уязвимостей по крайней мере, ежемесячно, а также ведется непрерывная работа по постоянному совершенствованию/обновлению средств контроля	**5**
	Нет информации/не применимо	**0**
D.7 Как тестируются решения по обнаружению уязвимостей?	Нет программы испытаний для формальной проверки решений по обнаружению уязвимостей	**1**
	Решения по обнаружению уязвимостей время от времени тестируются на специальной основе во время запланированных тестов и киберучений (т.е. тестирование решения по обнаружению уязвимостей является побочным эффектом киберучений, а не целью)	**2**
	Проводятся запланированные испытания решений по обнаружению уязвимостей путем моделирования реалистичных сценариев угроз для систем (например, тестирование на внешние/внутренние угрозы) в отдельных частях ИТ-ландшафта; испытания проводятся реже, чем раз в год	**3**
	Проводятся запланированные испытания решений по обнаружению уязвимостей путем моделирования реалистичных сценариев угроз для систем (например, тестирование на внешние/внутренние угрозы) в отдельных частях ИТ-ланашафта; испытания проводятся не реже одного раза в год, и не менее 50% решений по обнаружению уязвимостей тестируются каждый год	**4**
	Проводятся запланированные испытания решений по обнаружению уязвимостей путем моделирования реалистичных сценариев угроз для систем (например, тестирование на внешние/внутренние угрозы) в отдельных частях ИТ-ландшафта; тесты проводятся чаще одного раза в год, и более 75% решений по обнаружению уязвимостей тестируются каждый год	**5**
	Нет информации/не применимо	**0**

CASE STUDY: DETECT

СОЛАР Ростелеком

Центр противодействия кибератакам Solar JSOC – это первый и крупнейший коммерческий SOC в России. Входит в ТОП-5 европейских MSSP (Managed Security Service Provider) по объему бизнеса. Под защитой центра более 300 организаций из разных секторов экономики, а штат специалистов по кибербезопасности превышает 750 человек. Правила, индикаторы компрометации и сигнатуры SOC непрерывно обогащаются данными центра исследования киберугроз Solar 4RAYS, который сегодня аккумулирует крупнейшую в России базу знаний о кибератаках. Таким образом, экспертиза Solar JSOC позволяет оперативно и своевременно выявлять актуальные угрозы и пресекать атаки даже профессиональных киберпреступников.

Сервис мониторинга и анализа инцидентов ИБ от Solar JSOC предназначен для оперативного обнаружения угроз в инфраструктуре организации. Сервис оказывается на базе SIEM-системы (системы выявления инцидентов ИБ), которая может быть развернута как в облачной инфраструктуре ГК «Солар», так и в инфраструктуре клиента. Сервис оказывается 24/7 за счет 6 филиалов, расположенных в разных часовых поясах: производится сбор и анализ событий ИБ, предоставляются рекомендации по реагированию, оказывается помощь в расследовании.

Источник: АО «СОЛАР СЕКЬЮРИТИ»

билайн kaspersky

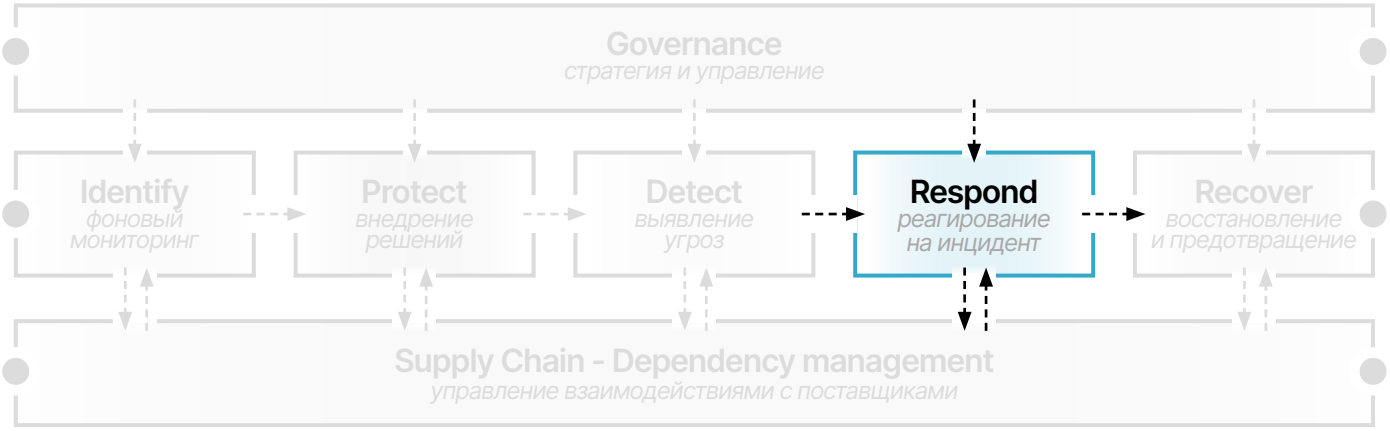
Билайн вместе с «Лабораторией Касперского» запустили сканер киберугроз – он доступен в приложении оператора бесплатно. Клиенты смогут узнать, посещали ли они с устройства потенциально опасные ресурсы, такие как фишинговые или вредоносные сайты. Проверка осуществляется на уровне сети и не требует дополнительного ПО. Оператор проверит данные о трафике за последние 30 дней, сравнит их с базами киберугроз и выдаст результат в виде светофора.

По данным Билайн, телеком-оператор за последние три месяца 2025 года заблокировал 50+ тыс. фишинговых ресурсов, а почти 4 млн клиентов столкнулись с киберугрозами.

Источник: АО «Лаборатория Касперского»

05

ДОМЕН RESPOND



RESPOND - РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИБ: ЭКСТРЕННЫЕ МЕРЫ И ДОРОЖНАЯ КАРТА

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
Res.1 Как часто в вашей организации проводятся учения для сотрудников по реагированию на инциденты?	Программы киберучений отсутствуют	1
	Ежегодно	2
	Чаще, чем ежегодно, но реже, чем ежеквартально	3
	Ежеквартально	4
	Ежеквартально и для всех критических процессов	5
	Нет информации/не применимо	0
Res.2 Как классифицируются инциденты и направляются ответственным сторонам?	Уровни эскалации не определены и нет формального плана действий в зависимости от типа инцидента (например, когда следует созвать оперативный «war room»)	1
	Нет формального плана действий в зависимости от типа инцидента (например, когда следует созвать оперативный «war room»), уровни эскалации определены	2
	Есть неформальное понимание у «сотрудников-старожилов», как следует классифицировать инциденты, и какой план реагирования на инциденты следует задействовать	3
	Есть формальный документ по классификации инцидентов, а также верхнеуровневый план действий по работе с инцидентами	4
	Есть формальный документ по классификации инцидентов, а также верхнеуровневый план действий по работе с инцидентами, включая, как начать работу «war room» и как формировать оперативную отчетность для высшего руководства/Совета директоров	5
	Нет информации/не применимо	0
Res.3 Сколько времени в среднем требуется на устранение уязвимостей после их обнаружения?	6+ месяцев	1
	3-6 месяцев	2
	1-3 месяца	3
	1-4 недели	4
	Меньше, чем неделя	5
	Нет информации/не применимо	0

RESPOND - РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИБ: ЭКСТРЕННЫЕ МЕРЫ И ДОРОЖНАЯ КАРТА

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
Res.4 Как реагирование на киберугрозы интегрируется с обеспечением непрерывности деятельности/ восстановлением работы в аварийных ситуациях?	Нет программы по реагированию на киберугрозы	1
	Есть скорее неформальные рекомендации по обеспечению непрерывности деятельности/восстановления в аварийных ситуациях	2
	План обеспечения непрерывности деятельности/восстановления в аварийных ситуациях (BCP/DR), который включает сценарии, основанные на кибератаках (например, DDoS-атаки)	3
	Есть план обеспечения непрерывности деятельности/восстановления в аварийных ситуациях (BCP/DR), который включает сценарии, основанные на кибератаках (например, DDoS-атаки); а также проводится, по крайней мере, одно учение по реагированию на киберугрозы в 2 года (совместно с бизнес-подразделениями и кибербезопасностью)	4
	Есть план обеспечения непрерывности деятельности/восстановления в аварийных ситуациях (BCP/DR) включает сценарии, основанные на кибератаках (например, DDoS-атаки); а также проводится, по крайней мере, одно учение по реагированию на киберугрозы в 2 года (совместно с бизнес-подразделениями и кибербезопасностью); в учении участвуют все внутренние и внешние сотрудники, задействованные в данном бизнес-процессе	5
	Нет информации/не применимо	0
Res.5 Как план/ программа реагирования на инциденты интегрируется с другими планами действий в кризисных ситуациях/планами действий при нештатной ситуации?	Нет согласованности в действиях и планах	1
	Есть у «сотрудников-старожилов» примерный неформальный перечень действий/шагов для обеспечения согласованности между планами	2
	Есть неформальное понимание у «сотрудников-старожилов», как следует классифицировать инциденты, и какой план реагирования на инциденты следует задействовать	3
	Есть формальный план, который содержит общие рекомендации о том, как процесс IR соотносится с другими планами действий в кризисных ситуациях/планами действий при нештатной ситуации	4
	Есть формальный план реагирования на инциденты, согласованный с наиболее тесно связанными функциями (например, для обеспечения непрерывности деятельности/аварийного восстановления)	5
	Нет информации/не применимо	0
Res.6 Как осуществляется процесс управления уязвимостями?	Нет разработанной программы по управлению уязвимостями	1
	Проводятся мероприятия по идентификации уязвимостей (например, сканирование), но определение приоритетов уязвимостей и их устранение проводятся от случая к случаю	2
	Есть разработанная программа, которая включает в себя элементы для идентификации уязвимостей, определения приоритетов и устранения неполадок	3
	Есть программа по управлению уязвимостями, которая включает элементы для детекции, расстановки приоритетов и устранения, а также формирует отчеты для руководителей по статусу работы с инцидентами	4
	Есть программа по управлению уязвимостями, которая включает элементы для детекции, расстановки приоритетов и устранения, а также формирует отчеты для руководителей по статусу работы с инцидентами, а также она интегрирована со смежными программами в организации (например, разработка решений, производственная поддержка, архитектура и инжиниринг, корпоративные риски)	5
	Нет информации/не применимо	0

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
Res.7 Насколько точно соблюдается существующий план реагирования на инциденты?	План не соблюдается	1
	План соблюдается время от времени или частично (не все шаги выполняются)	2
	Плана придерживаются для устранения большинства инцидентов	3
	Плана придерживаются для всех инцидентов: во время и после его устранения	4
	Плана придерживаются для всех инцидентов (во время и после его устранения, а также план регулярно обновляется на основе результатов последних устраненных инцидентов	5
	Нет информации/не применимо	0
Res.8 Какие автоматические действия предпринимаются в рамках реагирования на инциденты?	Нет автоматических действий	1
	Выполняются только базовые автоматические действия (например, фильтрация вредоносных программ) на рабочих станциях сотрудников (end-points)	2
	Выполняются автоматические действия на границах сети и системных серверах (например, блокировка IP-адреса, выключение компьютера) на основе заранее заданных параметров	3
	Выполняются автоматические действия, основанные на анализе информации о сети, системе и рабочей станции (end-point)	4
	Выполняются автоматические действия, включая мониторинг, сегментацию доступа подозрительных пользователей/систем на основе аналитических данных	5
	Нет информации/не применимо	0
Res.9 Как осуществляется процесс работы уязвимостями, которые не могут быть в моменте устранены?	Уязвимости, которые не могут быть устранены по решению владельцев систем, теряют приоритет и/или исключаются из отслеживания; никаких дальнейших действий не предпринимается	1
	Есть процесс проверки и утверждения уязвимостей, которые не могут быть устранены, и по крайней мере один «владелец риска», который не является владельцем системы (например, риск-менеджер или риск-аналитик) должен одобрить порядок действий «без устранения»	2
	Есть программа управления корпоративными рисками, которая включает рекомендации по работе с уязвимостями, которые не будут устранены; но риски, связанные с уязвимостями, документально не оформляются	3
	Есть программа управления корпоративными рисками, которая включает рекомендации по работе с уязвимостями, которые не будут устранены; риски, связанные с уязвимостями, документально оформляются	4
	Есть программа управления корпоративными рисками, которая включает рекомендации по работе с уязвимостями, которые не будут устранены; риски, связанные с уязвимостями, документально оформляются и рассматриваются совместно с другими рисками (например, юридическими и финансовыми)	5
	Нет информации/не применимо	0

CASE STUDY: RESPOND

Систему безопасности для реагирования на возможные киберинциденты, разработанную инженерами компании VK, внедрили в отечественный мессенджер MAX. Решение содержит больше 10 петабайт данных для кибер-расследований, что повышает скорость реагирования на возможные инциденты, предоставляя проактивную и превентивную охоту за угрозами.

Источник: ООО «ВК»

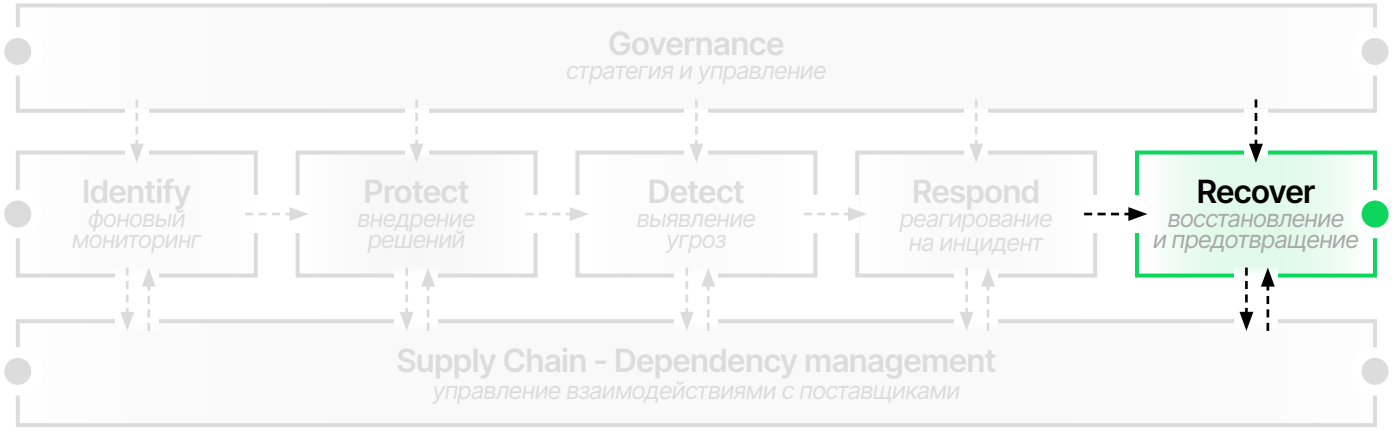
MTC Web Services внедрила решение для управления обращениями и инцидентами в «АШАН». Итоговое решение включает кастомную форму для приема обращений и поддерживает разные сценарии подачи заявок - в том числе полностью анонимные. Для таких запросов создан отдельный защищенный чат, где заявитель может общаться без раскрытия персональных данных. Отдельное внимание было уделено прозрачности коммуникаций: встроенный чат позволяет сотрудникам «АШАН» вести переписку с заявителем и между собой, фиксируя все действия в журнале изменений в соответствии с требованиями ИБ.

Развертывание и адаптация платформы MWS Tables на инфраструктуре заказчика заняли менее 3 месяцев. On-premises-модель обеспечила полный контроль над данными и возможность увеличивать количество лицензий без дополнительной перенастройки.

Источник: ООО «МВС»

06

ДОМЕН RECOVER



RECOVER - ВОССТАНОВЛЕНИЕ ДАННЫХ, СИСТЕМ И ПРОЦЕССОВ ПОСЛЕ ИНЦИДЕНТА И МЕРЫ ПРЕДОТВРАЩЕНИЯ

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
Rec.1 Каким образом информация о деятельности по восстановлению процесса после инцидента доводится до сведения внутренних и внешних стейкхолдеров?	Проводится ограниченная коммуникация с внутренними и внешними стейкхолдерами	1
	Проводится коммуникация по некоторым мероприятиям по восстановлению процесса после инцидента для определенного регламентом перечня внутренних и внешних стейкхолдеров	2
	Проводится коммуникация по большинству мероприятий по восстановлению процесса после инцидента для большинства внутренних и внешних стейкхолдеров; в организации действует политика, которая определяет, как организация должна доводить до сведения внутренних и внешних сотрудников мероприятия по восстановлению, процедуры и вопросы риск-менеджмента	3
	Проводится коммуникация по большинству мероприятий по восстановлению процесса после инцидента для большинства внутренних и внешних стейкхолдеров; организация также имеет комплексную, документально оформленную политику и процедуры для доведения до сведения Совета директоров (или Правления), иного высшего руководства и всех соответствующих внутренних стейкхолдеров информации о деятельности по восстановлению, принятых процедурах и вопросах риск-менеджмента	4
	Проводится коммуникация по всем мероприятиям по восстановлению процесса после инцидента для всех внутренних и внешних стейкхолдеров; организация также имеет комплексную, документально оформленную политику и процедуры для доведения до сведения Совета директоров (или Правления), иного высшего руководства и всех соответствующих внутренних стейкхолдеров информации о деятельности по восстановлению, принятых процедурах и вопросах риск-менеджмента	5
	Нет информации/не применимо	0
Rec.2 Как анализируются ранее произошедшие киберинциденты?	Некоторые инциденты проверяются	1
	Все инциденты анализируются; зачастую анализ инцидентов проводится без учета влияния произошедшего инцидента на бизнес-цели (КПЭ)	2
	Все инциденты анализируются; зачастую анализ инцидентов проводится без учета влияния произошедшего инцидента на бизнес-цели (КПЭ); определяются уровни инцидентов и SLA для их устранения	3
	Все инциденты анализируются; зачастую анализ инцидентов проводится с учетом влияния произошедшего инцидента на бизнес-цели (КПЭ); определяются уровни инцидентов и SLA для их устранения	4
	Все инциденты анализируются; зачастую анализ инцидентов проводится с учетом влияния произошедшего инцидента на бизнес-цели (КПЭ) с привлечением бизнес-владельца процесса; определяются уровни инцидентов и SLA для их устранения; анализируется выполненный план работ по устранению и выполняется поиск улучшений в предложенном плане	5
	Нет информации/не применимо	0

RESPOND - РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИБ: ЭКСТРЕННЫЕ МЕРЫ И ДОРОЖНАЯ КАРТА

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
Rec.3 Как реализуются программы по восстановлению процесса после инцидента и как ими управляют?	Отслеживание затрат и прогресса в реализации инициатив по устранению критических рисков на best-effort basis	**1**
	Дорожная карта содержит большинство новых инициатив по восстановлению и внедрению систем защиты, а проводится оценка новых программ в течение одного года	**2**
	Документально оформляются основные затраты, ожидаемые и понесенные в ходе реализации инициатив по восстановлению и внедрению систем защиты систем, оценка эффективности систем защиты проводится в течение 6 месяцев после внедрения	**3**
	Документально оформляются все внедряемые технические и нетехнические системы и программы, которые также обновляются не реже одного раза в квартал; для каждой системы или программы регистрируется владелец проекта/продукта; график обновляется регулярно и затраты, понесенные для восстановления большинства систем или программ, заносятся в систему отслеживания прогресса проекта	**4**
	Документально оформляются все внедряемые технические и нетехнические системы и программы, которые также обновляются не реже одного раза в квартал; для каждой системы или программы регистрируется владелец проекта/продукта; график обновляется регулярно и затраты, понесенные для восстановления большинства систем или программ, заносятся в систему отслеживания прогресса проекта; прогресс в реализации включается во все отчеты для совета директоров и высшего руководства; повторная оценка эффективности систем защиты проводится в течение 1 квартала после внедрения и результаты направляются в бизнес-подразделение	**5**
	Нет информации/не применимо	**0**
Rec.4 Как гарантируется безопасность и доступность для сотрудников критически важных для бизнеса данных?	Нет специальных программ по обеспечению безопасности и доступности критически важных для бизнеса данных	**1**
	Есть формализованный план обеспечения непрерывности деятельности, но он ориентирован на доступность объектов инфраструктуры, а не на системы или данные; однакое есть решения для резервного копирования некоторых данных	**2**
	Есть формализованный план обеспечения непрерывности деятельности, но он ориентирован на доступность объектов инфраструктуры, а не на системы или данные; однакое есть решения для резервного копирования большинства или всех критически важных бизнес-данных	**3**
	Есть формализованный план обеспечения непрерывности деятельности, который полностью охватывает объекты инфраструктуры, системы и данные, резервные копии самих данных хранятся в нескольких альтернативных хранилищах, и есть SLA восстановления для всех ресурсов	**4**
	Есть формализованный план обеспечения непрерывности деятельности, который полностью охватывает объекты инфраструктуры, системы и данные, резервные копии самих данных хранятся в нескольких альтернативных хранилищах, и есть SLA восстановления для всех ресурсов, а также обеспечивается переход на другой ресурс в режиме реального времени в случае сбоя основных систем хранения данных	**5**
	Нет информации/не применимо	**0**

CASE STUDY: RECOVER

Банк России

В октябре 2025 года на территории Университета Иннополис Банк России провел международные киберучения «Евразия-2025». В трансграничных киберучениях приняли участие представители финансовых регуляторов и финансовых организаций стран Евразийского экономического союза (ЕАЭС) и одной из стран-наблюдателей.

Участники мероприятия расследовали компьютерный инцидент в банке, который, по легенде, подвергся атаке хакеров. Сценарий был связан с эксплуатацией уязвимостей в программных продуктах, используемых этим банком. Командам требовалось восстановить его инфраструктуру и провести расследование, чтобы выйти на след злоумышленников – пройти весь сценарий Recovery. Всю собранную информацию команды передавали в ФинЦЕРТ Банка России.

Чтобы эффективнее противодействовать глобальным киберугрозам, Банк России продолжит сотрудничество с финансовыми регуляторами из стран ЕАЭС и других заинтересованных государств.

Источник: Центральный банк Российской Федерации

СБЕР УНИВЕРСИТЕТ КИБЕРПРОТЕКТ

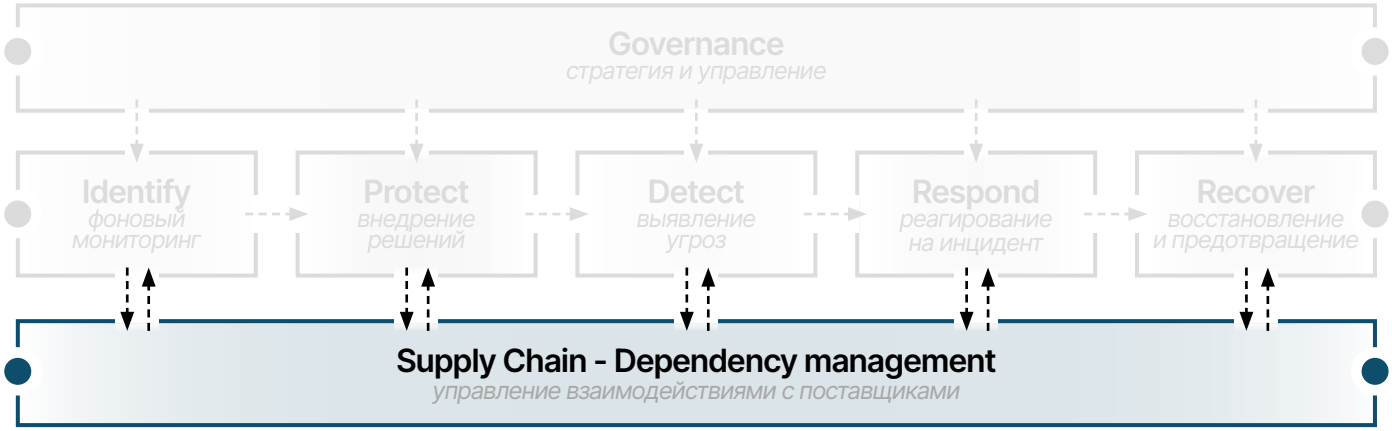
СберУниверситет внедрил новую версию системы резервного копирования и восстановления данных Кибер Бэкап от российской компании «Киберпротект». Решение защищает более 40 ТБ данных СберУниверситета при высокой скорости работы. На обновление системы заказчику потребовался всего 1 день.

Кибер Бэкап также позволяет прогнозировать показатели RTO / RPO, что важно для образовательного центра, в котором ежегодно повышают квалификацию 40+ тысяч топ-менеджеров, госслужащих и предпринимателей.

Источник: ООО «Киберпротект»

07

ДОМЕН SUPPLY CHAIN – DEPENDENCY MANAGEMENT



SUPPLY CHAIN - DEPENDENCY MANAGEMENT - УПРАВЛЕНИЕ ВЗАИМОДЕЙСТВИЕМ С ПОСТАВЩИКАМИ

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
SCh.1 Каким образом требования по кибербезопасности доводятся до сведения поставщиков/ провайдеров решений?	Нет требований по кибербезопасности для третьих лиц, или намеренно не сообщается о требованиях	1
	Требования по кибербезопасности доводятся до сведения поставщиков и третьих лиц на ad-hoc основе (например, устно по запросу)	2
	Требования по кибербезопасности включены в документацию, предоставляемую поставщикам и третьим лицам	3
	Требования по кибербезопасности включаются в договоры, технические задания или другую документацию, в которых устанавливаются обязанности поставщиков и третьих лиц	4
	Требования по кибербезопасности регулярно приводятся в соответствие с отраслевыми стандартами, включаются во всю документацию, предоставляемую третьим лицам до и после продажи, и доводятся до сведения в устной форме для обеспечения понимания на других этапах процесса взаимодействия с третьими лицами	5
	Нет информации/не применимо	0
SCh.2 Как поставщики задействованы в плане реагирования на инциденты?	Поставщики не задействованы	1
	Поставщики могут упоминаться, но без указания конкретных ролей/обязанностей	2
	Есть внутренние правила взаимодействия с поставщиками во время инцидента	3
	Есть внутренние правила взаимодействия с поставщиками во время инцидента, которые согласовываются с поставщиками	4
	Есть внутренние правила взаимодействия с поставщиками во время инцидента, которые согласовываются с поставщиками; поставщики также участвуют в проводимых учениях по реагированию на инциденты	5
	Нет информации/не применимо	0
SCh.3 Как часто управление по кибербезопасности участвует в процессе выбора поставщика?	Менее 20% случаев	1
	От 21% до 50% случаев	2
	От 51% до 80% случаев	3
	От 81% до 90% случаев	4
	Более 91% случаев	5
	Нет информации/не применимо	0

SUPPLY CHAIN - DEPENDENCY MANAGEMENT - УПРАВЛЕНИЕ ВЗАИМОДЕЙСТВИЕМ С ПОСТАВЩИКАМИ

ВОПРОС	ВАРИАНТЫ ОТВЕТА	БАЛЛЫ ЗА ОТВЕТ
SCh.4 Какой процент поставщиков (для которых предусмотрены требования по безопасности) прошли оценку соответствия или аудит соответствия требованиям (например, SOC II) за последние два года?	Менее 20% поставщиков	**1**
	От 21% до 50% поставщиков	**2**
	От 51% до 80% поставщиков	**3**
	От 81% до 90% поставщиков	**4**
	Более 91% поставщиков	**5**
	Нет информации/не применимо	**0**

CASE STUDY: SUPPLY CHAIN

В конце августа 2025 года злоумышленники парализовали ИТ-системы Jaguar Land Rover, что вынудило концерн остановить производство автомобилей на всех 3 британских заводах. Простои продолжались около 6 недель, за которые JLR не выпустила тысячи запланированных машин, понесла прямые убытки почти на 200 млн фунтов и нанесла ощутимый удар по всей отрасли.

В октябре 2025 года выпуск автомобилей в Великобритании просел на 24% в годовом сравнении именно вследствие простоя JLR. В регионе Уэст-Мидлендс более 70% предприятий-подрядчиков сообщили о негативном влиянии атаки на JLR. Британскому правительству пришлось рассматривать вопрос о поддержке пострадавших участников цепочки поставок, а самому JLR в итоге был предоставлен льготный заем на 1,5 млрд фунтов для восстановления деятельности. Этот инцидент показал, как уязвимость одного узла приводит к каскадному сбою всей сети.

Источник: АО «Позитив Текнолоджиз»

В JavaScript в сентябре 2025 был зафиксирован инцидент, объектом которого был Node Package Manager (npm) и ряд широко используемых JavaScript-пакетов, входящих в цепочки программного обеспечения. Злоумышленники получили доступ к учётным данным разработчика npm-пакетов через фишинговую кампанию. Письмо пришло с поддельного домена npmjs.help и выглядело как официальное уведомление об обновлении 2FA.

В результате инцидента были скомпрометированы порядка 150 программных пакетов, включая компоненты, связанные с экосистемой CrowdStrike. Часть затронутых библиотек, имеющих миллионы загрузок в неделю, содержала вредоносный код, предназначенный для хищения токенов и ключей аутентификации. Его особенность - способность распространяться автоматически, заражая другие доступные пакеты. Npm выявили скомпрометированные пакеты и удалили их из реестра. Разработчикам рекомендовали усилить защиту учётных записей, внедрить проверку целостности зависимостей и наладить процессы аудита цепочки поставок на всех этапах жизненного цикла ПО.

Источник: ООО «АМ Медиа»

ВЫВОДЫ

И ДАЛЬНЕЙШИЕ ШАГИ

За последние годы финансовый сектор столкнулся с ростом киберугроз: в 2024 году Банк России зафиксировал не менее 750 целевых кибератак на финансовые организации, большая часть которых была нацелена на выведение из строя ключевой инфраструктуры. В 2025 году тренд только усилился: по данным RED Security SOC, количество атак на финансовый сектор в России выросло в 2,2 раза по сравнению с аналогичным периодом 2024 года, при этом критическими признано свыше 13% инцидентов. По оценке Сбербанка, совокупный ущерб российской экономики от кибератак в 2025 году может достигать более 1,5 трлн рублей, значит, к**ибербезопасность перестала быть задачей исключительно для технических специалистов: это стратегический фактор устойчивости бизнеса, напрямую влияющий на финансовые результаты, репутацию и доверие клиентов.** Фреймворк Ассоциации ФинТех - это практический ответ на системный вызов, с которым сталкиваются сегодня участники финансового рынка.

За основу взят международный стандарт NIST CSF, мы адаптировали его, наполнили вопросами и примерами из российской практики, чтобы руководитель или специалист ИБ мог самостоятельно провести диагностику внутренней функции кибербезопасности.

Фреймворк охватывает не только традиционные защиту и обнаружение, но и **стратегическое управление (Governance)** и **восстановление после возможных инцидентов (Recover)**. Что актуально, мы также рассмотрели **домен по управлению цепочкой поставок (Supply Chain)**, так как современные типы угроз могут проникать и через систему партнеров, даже если меры защиты в вашей организации на высоком уровне зрелости.

ЧТО МЫ ПРЕДЛАГАЕМ СДЕЛАТЬ ДАЛЬШЕ?

01

Проведите самооценку

Ознакомьтесь с методологией и заполните опросные листы, проставив баллы с оценкой по каждому из доменов.

02

Определите приоритеты

Например, высокая зрелость в «Governance» при низкой в «Protect» могут указывать на разрыв между стратегией и тактикой: политика и регламенты функции не дополняются внедренными мерами защиты и их соблюдением. Фреймворк помогает выявить возможные отклонения.

03

Сформируйте дорожную карту

Мы предлагаем использовать полученную оценку для построения практического плана работ для повышения уровня зрелости кибербезопасности на 12-18 месяцев, фокусируясь на ключевых рисках для вашего бизнеса.

04

Делитесь опытом

На площадке АФТ мы организовываем встречи для участников экспертных сообществ, где мы будем рады вашей обратной связи как по сложности и удобству использования фреймворка, так и по практическим кейсам применения – вашим успехам в области кибербезопасности.

Выстраивание устойчивой функции кибербезопасности - это непрерывная системная работа, и мы верим, что фреймворк, который предлагает АФТ, станет дополнительным шагом в построении цифрового и устойчивого финансового рынка России.

НАД ИССЛЕДОВАНИЕМ РАБОТАЛИ

Команда АФТ

МАРИАННА ДАНИЛИНА
Руководитель Управления стратегии, исследований и аналитики, АФТ

АННА АНДРЕЙЧЕВА
Руководитель исследовательских проектов, АФТ

АЛЕКСАНДР ТОВСТОЛИП
Руководитель Управления информационной безопасности, АФТ

СЕРГЕЙ ЛАПИН
Эксперт Управления информационной безопасности, АФТ

Привлеченные эксперты

СЕРГЕЙ ДЕМИДОВ
Директор департамента операционных рисков, информационной безопасности и непрерывности бизнеса, Московская биржа

ЕВГЕНИЙ БАБИЦКИЙ
Сооснователь компании, Compliance Control

АЛЕКСЕЙ ОСИПОВ
Руководитель направления экспертного консалтинга, QSA, Compliance Control

АНДРЕЙ КОНЯХИН
Руководитель департамента международного и российского консалтинга, QSA, Compliance Control

Дизайн

АЛЕКСАНДРА ЩЕДРИНА
Креативный директор, АФТ

ДАРЬЯ ЗИНЬКО
Дизайнер, АФТ

АССОЦИАЦИЯ ФИНТЕХ

ИССЛЕДОВАНИЯ & АНАЛИТИКА

research.analytics@fintechru.org

АССОЦИАЦИЯ ФИНТЕХ

Ассоциация ФинТех *основана в конце 2016 г. по инициативе Банка России и ключевых участников отечественного финансового рынка. Это уникальная площадка для конструктивного диалога регулятора с представителями бизнеса.*

Здесь формируется экспертная оценка инновационных технологий с учетом международного опыта, а также разрабатываются концепции финансовых технологий и подходы к их внедрению.

WWW.FINTECHRU.ORG