Лекция 16: Политики безопасности и соответствие

Тема: Управление рисками, политики и соответствие

Технический университет Молдовы

Лектор: Максим Масютин

Введение

Добро пожаловать на лекцию 16, заключительную лекцию нашего курса. Сегодня мы рассмотрим политики безопасности и соответствие — то, как организации формализуют требования безопасности через политики и демонстрируют соблюдение нормативных актов, стандартов и договорных обязательств.

Политики и соответствие могут казаться бюрократическими, однако они выполняют важнейшие функции. Политики преобразуют принципы безопасности в конкретные требования, которым могут следовать сотрудники. Соответствие обеспечивает выполнение организацией законодательных обязательств и ожиданий клиентов. Вместе они создают подотчётность и последовательность в программах безопасности.

Нормативно-правовая среда кардинально изменилась в последние годы. Европейский союз принял несколько нормативных актов по кибербезопасности: Директиву NIS2 (Network and Information Security Directive 2, Директива о сетевой и информационной безопасности 2), Закон о цифровой операционной устойчивости (DORA, Digital Operational Resilience Act), Закон об ИИ и Закон о киберустойчивости. Соединённые Штаты ввели новые правила SEC (Securities and Exchange Commission, Комиссия по ценным бумагам и биржам) по раскрытию информации о кибербезопасности. Отраслевые фреймворки, такие как NIST и CIS, продолжают развиваться. Организации должны ориентироваться в этой всё более сложной среде.

В течение следующих двух часов мы рассмотрим иерархию политик, Систему менеджмента информационной безопасности ISO 27001, Фреймворк кибербезопасности NIST 2.0, контроли CIS, управление безопасностью и аудит, планирование реагирования на инциденты, а также основные нормативные акты ЕС и международные стандарты.

Часть 1: Иерархия политик безопасности

Назначение политик безопасности

Политики безопасности документируют управленческие решения в области безопасности. Они устанавливают, что требует организация, почему она это требует и кто отвечает за выполнение этих требований.

Политики служат нескольким целям:

Они доносят ожидания до сотрудников. Без письменных политик ожидания непоследовательны и неисполнимы. Политики информируют каждого о предъявляемых требованиях.

Они демонстрируют должную осмотрительность перед регуляторами и судами. Когда происходят инциденты, организации должны доказать, что они применяли разумные меры безопасности. Документированные политики служат доказательством.

Они обеспечивают единообразное внедрение. Политики гарантируют, что все подразделения организации следуют одним и тем же требованиям, избегая пробелов и противоречий.

Они поддерживают подотчётность. Когда требования задокументированы, можно привлечь к ответственности конкретных лиц за их выполнение.

Иерархия документов политик

Организации обычно поддерживают иерархию документов безопасности:

Политики — это высокоуровневые заявления о намерениях и требованиях руководства. Они отвечают на вопросы "что" и "почему", но не "как". Политики утверждаются высшим руководством или советом директоров. Они редко меняются — обычно пересматриваются ежегодно.

Пример формулировки политики: "Все информационные активы должны быть классифицированы в соответствии с их чувствительностью и критичностью."

Стандарты определяют конкретные обязательные требования, реализующие политики. Они отвечают на вопрос "что конкретно", но всё ещё не на детальный вопрос "как". Стандарты носят более технический характер, чем политики, но остаются требованиями, а не инструкциями.

Пример стандарта: "Все пароли должны содержать не менее 14 символов, включать заглавные и строчные буквы, цифры и специальные символы и меняться каждые 90 дней."

Процедуры — это пошаговые инструкции по выполнению задач. Они отвечают на вопрос "как именно". Процедуры являются операционными документами,

используемыми персоналом, выполняющим конкретные функции.

Пример процедуры: "Для сброса пароля Active Directory: 1) Откройте Active Directory Users and Computers. 2) Найдите учётную запись пользователя. 3) Щёлкните правой кнопкой мыши и выберите Reset Password. 4) Введите временный пароль, соответствующий требованиям сложности. 5) Установите флажок 'User must change password at next logon'."

Руководства (рекомендации) — это рекомендации, а не обязательные требования. Они содержат советы для ситуаций, где допустима гибкость. В руководствах используются формулировки вроде "рекомендуется" вместо "обязательно".

Базовые конфигурации определяют минимальные настройки безопасности для конкретных систем или технологий. Они представляют собой технические стандарты, применяемые при развёртывании систем.

Основные политики безопасности

Каждая организация нуждается в определённых ключевых политиках:

Политика информационной безопасности — это основная политика, устанавливающая приверженность организации безопасности, определяющая область применения и цели, а также задающая общую структуру.

Политика допустимого использования определяет разрешённое использование организационных систем и данных. Она охватывает личное использование, запрещённые действия, мониторинг и последствия нарушений.

Политика управления доступом устанавливает принципы предоставления, пересмотра и отзыва доступа к системам и данным. Она рассматривает вопросы минимальных привилегий, разделения обязанностей и требования к пересмотру доступа.

Политика классификации данных определяет уровни классификации и требования к обращению с данными каждого уровня. Она устанавливает, кто может классифицировать данные и как обозначаются уровни классификации.

Политика реагирования на инциденты устанавливает требования к обнаружению, реагированию и восстановлению после инцидентов безопасности. Она определяет роли, порядок эскалации и требования к отчётности.

Политика непрерывности бизнеса требует наличия планов для продолжения деятельности при сбоях. Она устанавливает требования к целевому времени восстановления (RTO) и целевой точке восстановления (RPO), а также периодичность тестирования.

Политика безопасности третьих сторон определяет требования безопасности для поставщиков, партнёров и поставщиков услуг, имеющих доступ к системам или данным организации.

Политика физической безопасности затрагивает вопросы безопасности помещений, управления посетителями и физической защиты оборудования.

Разработка и поддержание политик

Разработка эффективных политик требует:

Вовлечения заинтересованных сторон: политики затрагивают всех. Включайте в разработку представителей бизнес-подразделений, отдела кадров, юридического отдела и ИТ-службы.

Ясности формулировок: пишите для своей аудитории. Избегайте технического жаргона в политиках, распространяющихся на всех сотрудников.

Реалистичности требований: политики, которым невозможно следовать, не будут соблюдаться. Убедитесь, что требования выполнимы.

Согласованности: политики должны быть согласованы друг с другом и с нормативными актами. Противоречивые требования создают пробелы в соответствии.

Утверждения: политики требуют формального утверждения на соответствующем уровне — обычно высшим руководством или советом директоров для политик верхнего уровня.

Информирования: политики бесполезны, если сотрудники о них не знают. Обучайте сотрудников политикам. Обеспечьте лёгкий доступ к политикам.

Пересмотра: политики устаревают. Пересматривайте их ежегодно и обновляйте при изменениях в бизнесе или нормативной среде.

Часть 2: Система менеджмента информационной безопасности ISO/IEC 27001

Что такое СМИБ?

Система менеджмента информационной безопасности (СМИБ, ISMS — Information Security Management System) — это системный подход к управлению конфиденциальной информацией. Она охватывает людей, процессы и технологии с целью защиты конфиденциальности, целостности и доступности информации.

ISO/IEC 27001 — это международный стандарт, устанавливающий требования к созданию, внедрению, поддержанию и постоянному совершенствованию СМИБ. Впервые опубликованный в 2005 году, он был существенно пересмотрен в 2013 и

затем в 2022 году. Версия 2022 года отражает современные практики безопасности и содержит реструктурированные контроли.

Сертификация по ISO 27001 демонстрирует клиентам, партнёрам и регуляторам, что организация внедрила комплексную систему менеджмента безопасности. Сертификация требует оценки аккредитованными органами по сертификации.

Структура ISO 27001

Стандарт следует структуре Annex SL, общей для стандартов ISO на системы менеджмента. Это позволяет интегрировать его с другими стандартами, такими как ISO 9001 (качество) и ISO 22301 (непрерывность бизнеса).

Разделы 4-10 определяют требования к СМИБ:

Раздел 4: Контекст организации требует понимания внутренних и внешних факторов, заинтересованных сторон и определения области применения СМИБ.

Раздел 5: Лидерство требует приверженности высшего руководства, установления политики безопасности и определения ролей и ответственности.

Раздел 6: Планирование рассматривает оценку и обработку рисков, цели безопасности и планирование изменений.

Раздел 7: Поддержка охватывает ресурсы, компетенции, осведомлённость, коммуникацию и требования к документированной информации.

Раздел 8: Функционирование требует реализации планов обработки рисков и управления процессами.

Раздел 9: Оценка результатов деятельности требует мониторинга, измерения, внутреннего аудита и анализа со стороны руководства.

Раздел 10: Улучшение требует устранения несоответствий и осуществления постоянного улучшения.

Контроли Приложения А

Приложение А содержит справочные контроли безопасности, организованные в четыре темы в версии 2022 года:

Организационные контроли (37 контролей) охватывают политики, роли, управление активами, управление доступом, взаимоотношения с поставщиками и соответствие.

Контроли персонала (8 контролей) охватывают проверку перед наймом, условия трудоустройства, осведомлённость, обучение и дисциплинарные процедуры.

Физические контроли (14 контролей) охватывают физические периметры, контроль входа, безопасность оборудования и безопасную утилизацию.

Технологические контроли (34 контроля) охватывают права доступа, аутентификацию, криптографию, защиту от вредоносного ПО, резервное копирование, журналирование, сетевую безопасность и безопасность разработки.

Организации должны определить, какие контроли применимы, на основе оценки рисков. Заявление о применимости документирует, какие контроли внедрены, и обосновывает любые исключения.

Обновления ISO 27001:2022

Пересмотр 2022 года привнёс несколько изменений:

Реструктуризация контролей: контроли реорганизованы из 14 доменов в 4 темы с новой нумерацией.

Новые контроли: 11 новых контролей учитывают современные угрозы и практики, включая аналитику угроз, безопасность облачных сервисов, готовность ИКТ к непрерывности бизнеса, мониторинг физической безопасности, управление конфигурацией, удаление информации, маскирование данных, предотвращение утечки данных, деятельность по мониторингу, веб-фильтрацию и безопасное кодирование.

Таблицы атрибутов: контроли помечены атрибутами (тип контроля, свойства безопасности, концепции кибербезопасности, операционные возможности, домены безопасности), что обеспечивает гибкое соотнесение с потребностями организации.

Организации, сертифицированные по ISO 27001:2013, должны перейти на версию 2022 до октября 2025 года.

Подход к внедрению

Внедрение ISO 27001 обычно включает:

Анализ разрывов: сравнение текущего состояния с требованиями стандарта. Выявление того, что уже имеется и что необходимо разработать.

Определение области применения: определение того, какие подразделения организации охвачены. Учёт бизнес-подразделений, локаций и систем.

Оценка рисков: проведение оценки рисков в соответствии с определённой методологией (ISO 27005 содержит соответствующие рекомендации).

Обработка рисков: выбор и внедрение контролей для устранения выявленных рисков.

Документирование: разработка необходимых политик, процедур и записей. ISO 27001 требует документированной информации, но не предписывает форматы.

Обучение: обеспечение понимания персоналом своих обязанностей в области безопасности и требований СМИБ.

Внутренний аудит: оценка эффективности СМИБ посредством внутренних аудитов перед обращением за сертификацией.

Анализ со стороны руководства: высшее руководство анализирует результаты функционирования СМИБ и принимает решения по улучшениям.

Сертификационный аудит: внешние аудиторы оценивают соответствие стандарту в два этапа.

Часть 3: Фреймворк кибербезопасности NIST 2.0

Эволюция CSF

Фреймворк кибербезопасности NIST (CSF, Cybersecurity Framework) был первоначально разработан в 2014 году по указу президента об улучшении кибербезопасности критической инфраструктуры. Он быстро стал наиболее широко принятым фреймворком безопасности в Соединённых Штатах и получил международное признание.

CSF 2.0, выпущенный в феврале 2024 года, представляет собой значительное обновление. Он расширяет область применения с критической инфраструктуры на все организации, добавляет новую функцию "Управление" (Govern) и интегрирует уроки, извлечённые за десятилетие внедрения.

Шесть функций

CSF 2.0 организует деятельность по обеспечению безопасности в шесть основных функций:

Управление (Govern) (новая в версии 2.0) устанавливает и контролирует организационную стратегию кибербезопасности, ожидания и политики. Она охватывает организационный контекст, стратегию управления рисками, роли и ответственность, политики, надзор и управление рисками цепочки поставок.

Идентификация (Identify) формирует организационное понимание рисков кибербезопасности. Категории включают управление активами, оценку рисков и улучшение.

Защита (Protect) разрабатывает и внедряет защитные меры для критически важных сервисов. Категории включают управление идентификацией, обучение по информационной безопасности, безопасность данных, безопасность платформ и устойчивость технологической инфраструктуры.

Обнаружение (Detect) разрабатывает и внедряет возможности обнаружения. Категории включают непрерывный мониторинг и анализ нежелательных событий.

Реагирование (Respond) разрабатывает и внедряет действия по реагированию. Категории включают управление инцидентами, анализ инцидентов, отчётность о реагировании на инциденты и смягчение последствий инцидентов.

Восстановление (Recover) разрабатывает и внедряет действия по восстановлению. Категории включают выполнение плана восстановления после инцидентов и коммуникацию по вопросам восстановления.

Уровни внедрения

CSF определяет четыре уровня внедрения, описывающих степень строгости управления рисками кибербезопасности:

Уровень 1 (Частичный): управление рисками носит ситуативный характер с ограниченной осведомлённостью. Деятельность по кибербезопасности может не учитывать организационные риски.

Уровень 2 (С учётом рисков): практики управления рисками существуют, но могут не быть закреплены в организационной политике. Осведомлённость о рисках кибербезопасности существует, но общеорганизационный подход ограничен.

Уровень 3 (Воспроизводимый): практики управления рисками формально утверждены и выражены в виде политик. Практики регулярно обновляются на основе изменений.

Уровень 4 (Адаптивный): организация адаптирует практики на основе извлечённых уроков и индикаторов. Непрерывное совершенствование с использованием передовых технологий и практик.

Уровни не являются уровнями зрелости — более высокие уровни не обязательно лучше. Организации должны внедрять уровни, соответствующие их среде рисков.

Профили

Профили CSF описывают текущее или целевое состояние кибербезопасности организации. Профиль соотносит функции, категории и подкатегории с бизнес-требованиями, толерантностью к риску и ресурсами.

Текущий профиль описывает существующие результаты кибербезопасности.

Целевой профиль описывает желаемые результаты.

Анализ разрывов сравнивает текущий и целевой профили для определения приоритетов улучшения.

Отраслевые профили предоставляют отраслевые реализации. Примеры существуют для промышленности, морского транспорта, выборов и других

областей.

Ключевые изменения в CSF 2.0

CSF 2.0 привнёс несколько важных изменений:

Функция Управление (Govern) возводит управление в равный статус с техническими функциями. Это отражает важность организационного руководства в сфере кибербезопасности.

Расширенная область применения явно охватывает все организации, а не только критическую инфраструктуру.

Акцент на цепочке поставок усиливает управление рисками цепочки поставок во всём фреймворке.

Улучшенные ресурсы включают краткие руководства по началу работы, примеры внедрения и информативные ссылки на другие фреймворки и стандарты.

Уровни внедрения пересмотрены для лучшей поддержки принятия организационных решений.

Использование CSF совместно с другими фреймворками

CSF разработан для совместного использования с другими стандартами и фреймворками. Организации могут использовать CSF как организующую структуру при реализации конкретных требований из:

ISO 27001 для комплексных требований к системе менеджмента.

Контролей CIS для приоритизированных технических контролей.

NIST SP 800-53 для детальных федеральных контролей безопасности.

Отраслевых стандартов, таких как PCI DSS, HIPAA или отраслевые требования.

Информативные ссылки CSF предоставляют детальные сопоставления с этими фреймворками.

Часть 4: Контроли CIS

Обзор контролей CIS

Контроли Центра интернет-безопасности (CIS, Center for Internet Security) — это приоритизированный набор действий для киберзащиты. Разработанные в

процессе консенсуса с участием отраслевых и государственных экспертов, они представляют собой основы гигиены безопасности.

Контроли CIS версии 8, выпущенные в 2021 году, содержат 18 контролей, организованных по приоритету внедрения. Контроли спроектированы как практически применимые, с акцентом на наиболее важных аспектах на основе реальных данных об атаках.

Группы внедрения

CIS признаёт, что организации располагают различными ресурсами и профилями рисков. Группы внедрения (IG, Implementation Groups) помогают организациям расставить приоритеты на основе их характеристик:

IG1 — это базовая кибергигиена для всех организаций, независимо от размера. Она содержит 56 защитных мер, охватывающих базовые практики безопасности. Организациям с ограниченными ресурсами следует начинать именно с этой группы.

IG2 дополняет IG1 для организаций с умеренными ресурсами и несколько более высокими рисками. Она добавляет 74 дополнительных защитных меры. Организации, обрабатывающие конфиденциальные данные или подпадающие под нормативные требования, обычно нуждаются в IG2.

IG3 — это полный набор контролей для организаций со значительными ресурсами в области безопасности, сталкивающихся с изощрёнными угрозами. Она добавляет 23 дополнительных защитных меры.

18 контролей

Рассмотрим 18 контролей CIS:

Контроль 1: Инвентаризация и управление корпоративными активами — знайте, какое оборудование присутствует в вашей сети.

Контроль 2: Инвентаризация и управление программными активами — знайте, какое программное обеспечение авторизовано и работает.

Контроль 3: Защита данных — управляйте данными на протяжении всего их жизненного цикла с надлежащей классификацией и защитой.

Контроль 4: Безопасная конфигурация корпоративных активов и программного обеспечения — установите и поддерживайте безопасные конфигурации.

Контроль 5: Управление учётными записями — управляйте учётными данными и учётными записями авторизованных пользователей.

Контроль 6: Управление доступом — контролируйте доступ на основе принципов необходимости знать и минимальных привилегий.

Контроль 7: Непрерывное управление уязвимостями — выявляйте и устраняйте уязвимости на постоянной основе.

Контроль 8: Управление журналами аудита — собирайте, храните и анализируйте журналы для обнаружения и расследования инцидентов.

Контроль 9: Защита электронной почты и веб-браузеров — защищайтесь от угроз через электронную почту и веб.

Контроль 10: Защита от вредоносного ПО — предотвращайте, обнаруживайте и реагируйте на вредоносное ПО.

Контроль 11: Восстановление данных — поддерживайте возможности резервного копирования и восстановления данных.

Контроль 12: Управление сетевой инфраструктурой — обеспечивайте безопасность сетевых устройств и архитектуры.

Контроль 13: Мониторинг и защита сети — осуществляйте мониторинг и защиту сетевых операций.

Контроль 14: Обучение по информационной безопасности и развитие навыков — обучайте персонал практикам безопасности.

Контроль 15: Управление поставщиками услуг — управляйте рисками безопасности, связанными с поставщиками услуг.

Контроль 16: Безопасность прикладного программного обеспечения — обеспечивайте безопасность собственного и приобретённого программного обеспечения.

Контроль 17: Управление реагированием на инциденты — создайте возможности реагирования на инциденты.

Контроль 18: Тестирование на проникновение — проверяйте защиту с помощью имитации атак.

Стандарты конфигурации CIS

В дополнение к контролям, стандарты конфигурации CIS (CIS Benchmarks) предоставляют подробные рекомендации по безопасной настройке конкретных технологий. Стандарты существуют для операционных систем, облачных провайдеров, приложений, сетевых устройств и других платформ.

Стандарты определяют два профиля: Уровень 1 для базовой безопасности, которая не должна существенно влиять на функциональность, и Уровень 2 для сред, требующих повышенной безопасности, с возможным воздействием на функционирование.

CIS-CAT — это инструмент оценки, автоматически проверяющий системы на соответствие рекомендациям стандартов.

Часть 5: Управление безопасностью и аудит

Управление безопасностью

Управление безопасностью — это система руководства, организационных структур и процессов, обеспечивающих поддержку организационных целей со стороны безопасности и надлежащее управление рисками.

Эффективное управление требует:

Участия совета директоров и высшего руководства: безопасность — это бизнес-риск, а не просто проблема ИТ. Советы директоров должны осуществлять надзор за стратегией безопасности и рисками. Руководители должны принимать решения по рискам и выделять ресурсы.

Чётких ролей и ответственности: кто несёт ответственность за решения в области безопасности? Кто внедряет контроли? Кто контролирует эффективность? Матрицы RACI (Responsible, Accountable, Consulted, Informed — ответственный, подотчётный, консультируемый, информируемый) уточняют роли.

Системы политик: как обсуждалось ранее, документированные политики устанавливают требования и ожидания.

Интеграции с управлением рисками: решения в области безопасности должны основываться на оценке рисков. Управление обеспечивает соблюдение процессов работы с рисками.

Измерения эффективности: метрики и индикаторы отслеживают результативность безопасности. Информационные панели доносят состояние до руководства.

Постоянного улучшения: управление включает механизмы извлечения уроков из инцидентов, аудитов и изменяющихся угроз.

Модель трёх линий

Модель трёх линий (ранее — модель трёх линий защиты) описывает структуру управления:

Первая линия: операционное руководство владеет рисками и управляет ими. Бизнес-подразделения и ИТ-подразделения внедряют контроли и обеспечивают повседневную безопасность.

Вторая линия: функции управления рисками и соответствия осуществляют надзор, устанавливают стандарты и контролируют первую линию. Здесь обычно действуют подразделения менеджмента информационной безопасности и команды по соответствию.

Третья линия: внутренний аудит обеспечивает независимую гарантию. Аудиторы оценивают, правильно ли спроектированы контроли и эффективно ли они

функционируют.

Внешние аудиторы и регуляторы обеспечивают дополнительный надзор за пределами организации.

Аудит безопасности

Аудит безопасности оценивает, правильно ли спроектированы контроли и эффективно ли они функционируют.

Внутренние аудиты проводятся собственной службой аудита организации. Они обеспечивают постоянную уверенность и выявляют области для улучшения. Внутренний аудит должен быть независимым от ИТ-службы и подразделения безопасности.

Внешние аудиты проводятся независимыми аудиторами. Они могут требоваться для регулятивного соответствия, сертификации (ISO 27001) или обеспечения уверенности клиентов (SOC 2).

Типы аудитов включают:

Аудит соответствия оценивает соблюдение конкретных требований: нормативных актов, стандартов или политик.

Аудит контролей оценивает, спроектированы ли контроли для устранения рисков и функционируют ли они в соответствии с замыслом.

ИТ-аудит фокусируется на технологических контролях и процессах.

Операционный аудит проверяет эффективность и результативность операций безопасности.

Отчёты SOC

Отчёты SOC (Service Organization Control) — это аудиторские отчёты для сервисных организаций:

SOC 1 охватывает контроли, значимые для финансовой отчётности. Используется преимущественно для услуг, влияющих на финансовую отчётность клиентов.

SOC 2 охватывает безопасность, доступность, целостность обработки, конфиденциальность и конфиденциальность данных. Широко используется для демонстрации безопасности клиентам.

Отчёты Типа I оценивают дизайн контролей на определённый момент времени.

Отчёты Типа II оценивают дизайн контролей и эффективность их функционирования за период (обычно 6-12 месяцев).

Отчёты SOC 2 Типа II особенно ценны для оценки безопасности третьих сторон. Они обеспечивают независимую проверку эффективности контролей на протяжении времени.

Подготовка к аудиту

Подготовка к аудитам снижает стресс и улучшает результаты:

Поддерживайте документацию: аудиторы требуют доказательства. Поддерживайте политики, процедуры и записи в актуальном и доступном состоянии.

Фиксируйте функционирование контролей: сохраняйте свидетельства постоянного функционирования контролей — журналы, отчёты и согласования.

Проводите самооценки: выявляйте и устраняйте проблемы до того, как их найдут аудиторы.

Понимайте область проверки: знайте, что будут проверять аудиторы, и убедитесь, что соответствующие контроли готовы.

Назначьте ответственных: определите лицо для координации работы с аудиторами и сбора доказательств.

Устраняйте предыдущие замечания: аудиторы всегда проверяют устранение ранее выявленных замечаний. Убедитесь, что исправления завершены.

Часть 6: Планирование реагирования на инциденты

Почему планирование важно

Инциденты безопасности будут происходить, несмотря на лучшие превентивные меры. То, как организации реагируют, определяет серьёзность последствий. Плохое реагирование продлевает простои, увеличивает затраты и наносит ущерб репутации. Эффективное реагирование ограничивает ущерб и ускоряет восстановление.

Реагирование на инциденты невозможно импровизировать во время кризиса. Давление, неполная информация и временные ограничения затрудняют принятие правильных решений. Планирование обеспечивает целенаправленную подготовку в условиях более низких ставок.

Нормативные требования всё чаще предписывают наличие возможностей реагирования на инциденты. GDPR, NIS2, DORA, PCI DSS и многие отраслевые нормативные акты требуют документированных процедур реагирования на инциденты.

Фазы реагирования на инциденты

NIST SP 800-61 определяет четыре фазы реагирования на инциденты:

Подготовка осуществляется до наступления инцидентов. Она включает разработку политик и процедур, формирование группы реагирования, приобретение инструментов и ресурсов, а также обучение персонала.

Обнаружение и анализ выявляет факт произошедшего инцидента и определяет его характер и масштаб. Эта фаза включает мониторинг, сортировку оповещений и первичное расследование.

Сдерживание, устранение и восстановление останавливает распространение инцидента, устраняет присутствие злоумышленника и восстанавливает нормальную работу. Эта фаза включает изоляцию, сохранение доказательств, очистку и восстановление систем.

Постинцидентная деятельность извлекает уроки из инцидентов для улучшения будущего реагирования. Она включает анализ первопричин, документирование и внедрение улучшений.

Содержание плана реагирования на инциденты

План реагирования на инциденты должен охватывать:

Цель и область применения: какие инциденты охвачены? Что запускает план?

Роли и ответственности: кто что делает во время инцидентов? Включите роли ИТ, безопасности, юристов, коммуникации и руководства.

Процедуры коммуникации: как координируется работа группы? Кто осуществляет внешние коммуникации — с клиентами, регуляторами, СМИ?

Критерии классификации: как инциденты категоризируются и приоритизируются?

Процедуры реагирования: какие шаги предпринимаются для различных типов инцидентов?

Критерии эскалации: когда уведомляется высшее руководство? Когда привлекаются внешние стороны?

Обращение с доказательствами: как сохраняются доказательства для возможных судебных разбирательств?

Внешние ресурсы: какие поставщики, правоохранительные органы или другие стороны могут быть привлечены?

Группа реагирования на инциденты

Группа реагирования на инциденты компьютерной безопасности (CSIRT, Computer Security Incident Response Team) или группа реагирования на

инциденты (IRT, Incident Response Team) координирует действия по реагированию.

Основные участники группы обычно включают аналитиков безопасности, персонал ИТ-операций и менеджера инцидентов. Они обрабатывают большинство инцидентов напрямую.

Расширенные участники группы привлекаются по мере необходимости: юрисконсульт для решения нормативных вопросов и вопросов ответственности, подразделение коммуникаций для внешних сообщений, отдел кадров при инцидентах с участием инсайдеров, руководство для принятия стратегических решений.

Внешние ресурсы могут включать специалистов по форензике, юристов, специализирующихся на правовых вопросах, компании по кризисным коммуникациям и правоохранительные органы. Установите контакты и выстройте отношения до наступления инцидентов.

Тестирование и учения

Планы необходимо тестировать для проверки их работоспособности и обучения персонала.

Кабинетные учения моделируют сценарии в формате совещания. Группа обсуждает, как бы она реагировала. Это малозатратный и эффективный метод выявления пробелов.

Функциональные учения реально выполняют процедуры реагирования без фактического инцидента. Группы могут отрабатывать процедуры форензики, протоколы коммуникации или процессы восстановления.

Полномасштабные учения имитируют реалистичные инциденты максимально полно. Они затратны, но выявляют слабые места, которые не обнаруживаются другими тестами.

Проводите тестирование не реже одного раза в год. Тестируйте при каждом существенном изменении в системах, составе группы или процедурах.

Часть 7: Нормативные акты ЕС — NIS2, DORA, Закон об ИИ, Закон о киберустойчивости

Нормативно-правовой ландшафт ЕС

Европейский союз принял амбициозную программу регулирования кибербезопасности. Многочисленные регламенты и директивы устанавливают требования для организаций, действующих в Европе. Понимание этих требований необходимо для любой организации, присутствующей на рынке ЕС или обслуживающей клиентов из ЕС.

Директива NIS2

Директива NIS2 о сетевой и информационной безопасности вступила в силу в январе 2023 года, с требованием транспозиции в национальное законодательство до октября 2024 года. Она значительно расширяет первоначальную Директиву NIS 2016 года.

Расширение области применения: NIS2 охватывает значительно больше секторов, включая энергетику, транспорт, банковскую деятельность, здравоохранение, цифровую инфраструктуру, государственное управление, космическую отрасль, почтовые услуги, управление отходами, производство, пищевую промышленность и цифровых провайдеров. Организации классифицируются как основные или важные в зависимости от размера и сектора.

Требования включают:

Меры по управлению рисками: организации должны внедрять надлежащие технические, операционные и организационные меры, охватывающие анализ рисков, обработку инцидентов, непрерывность бизнеса, безопасность цепочки поставок, сетевую безопасность, управление доступом, криптографию и обучение по информационной безопасности.

Отчётность об инцидентах: о значительных инцидентах необходимо сообщать властям в течение 24 часов (раннее предупреждение), 72 часов (первоначальное уведомление) и одного месяца (итоговый отчёт).

Безопасность цепочки поставок: организации должны учитывать риски кибербезопасности, связанные с поставщиками и поставщиками услуг.

Корпоративная ответственность: органы управления должны утверждать и осуществлять надзор за мерами кибербезопасности. Они должны проходить обучение и могут нести ответственность за несоблюдение требований.

Правоприменение: штрафы для основных субъектов могут достигать 10 миллионов евро или 2% глобального оборота. Для важных субъектов — 7 миллионов евро или 1,4% оборота.

Закон о цифровой операционной устойчивости (DORA)

DORA устанавливает единые требования к цифровой операционной устойчивости финансового сектора. Он применяется с января 2025 года к банкам, страховым компаниям, инвестиционным фирмам, платёжным провайдерам и другим финансовым субъектам.

Основные требования включают:

Управление рисками ИКТ: финансовые субъекты должны поддерживать комплексные фреймворки управления рисками ИКТ, охватывающие идентификацию, защиту, обнаружение, реагирование, восстановление и обучение.

Управление инцидентами, связанными с ИКТ: субъекты должны классифицировать и сообщать о крупных инцидентах, связанных с ИКТ, используя стандартизированные критерии.

Тестирование цифровой операционной устойчивости: регулярное тестирование, включая тестирование на проникновение на основе модели угроз для значимых субъектов.

Управление рисками третьих сторон в области ИКТ: требования к управлению рисками, связанными с поставщиками услуг ИКТ, включая контрактные положения, надзор и стратегии выхода.

Надзор за критическими третьими сторонами в области ИКТ: регуляторы могут напрямую осуществлять надзор за критическими сторонними провайдерами (такими как крупные облачные провайдеры), обслуживающими финансовый сектор.

Обмен информацией: поощрение обмена аналитикой об угрозах между финансовыми субъектами.

DORA гармонизирует то, что ранее регулировалось разрозненными национальными нормами и отраслевыми руководствами.

Закон об ИИ

Закон ЕС об ИИ, вступивший в силу в августе 2024 года с поэтапным внедрением до 2027 года, устанавливает риск-ориентированную систему регулирования систем искусственного интеллекта.

Категории рисков:

ИИ с неприемлемым риском запрещён. Сюда входят системы социального рейтинга, биометрическая идентификация в реальном времени в общественных

местах (за исключением установленных случаев) и манипулятивный ИИ.

ИИ высокого риска подпадает под обширные требования, включая управление рисками, управление данными, техническую документацию, прозрачность, человеческий контроль, точность, надёжность и оценку соответствия. Категории включают ИИ в критической инфраструктуре, образовании, занятости, основных услугах, правоприменении и биометрических системах.

ИИ ограниченного риска подлежит обязательствам по прозрачности. Пользователи должны знать, что они взаимодействуют с ИИ.

ИИ минимального риска не подпадает под конкретные требования помимо действующего законодательства.

Последствия для безопасности:

Системы ИИ высокого риска должны быть защищены от несанкционированного изменения.

ИИ, используемый в инструментах кибербезопасности, может относиться к различным категориям рисков.

Организации, использующие ИИ, должны понимать, к какой категории рисков относятся их системы.

Кибератаки с использованием ИИ создают новые аспекты угроз.

Закон о киберустойчивости

Закон о киберустойчивости (CRA), принятый в 2024 году с поэтапным введением требований до 2027 года, устанавливает требования кибербезопасности для продуктов с цифровыми элементами — аппаратных и программных продуктов.

Основные требования:

Безопасность на этапе проектирования: продукты должны проектироваться и разрабатываться с надлежащей кибербезопасностью на протяжении всего жизненного цикла.

Управление уязвимостями: производители должны выявлять и устранять уязвимости, предоставляя обновления безопасности в течение не менее пяти лет.

Документация по безопасности: продукты должны содержать понятную информацию о кибербезопасности для пользователей.

Отчётность об инцидентах: об активно эксплуатируемых уязвимостях и серьёзных инцидентах необходимо сообщать в ENISA (European Union Agency for Cybersecurity, Агентство ЕС по кибербезопасности) в течение 24 часов.

Оценка соответствия: продукты должны пройти оценку соответствия до вывода на рынок. Критические продукты подлежат оценке третьей стороной.

Область применения включает: программное обеспечение (включая компоненты SaaS), аппаратные устройства (IoT — Internet of Things, интернет вещей; сетевое

оборудование) и продукты, импортируемые в ЕС.

Последствия для организаций:

Поставщики программного обеспечения должны внедрить практики безопасной разработки и поддерживать продукты на протяжении всего жизненного цикла.

Организации, закупающие продукты, должны учитывать соответствие CRA при выборе поставщиков.

Для открытого программного обеспечения предусмотрены специальные положения, в целом исключающие некоммерческую разработку.

Часть 8: GDPR, PCI DSS и HIPAA

Общий регламент по защите данных (GDPR)

GDPR (General Data Protection Regulation, Общий регламент по защите данных), действующий с мая 2018 года, регулирует обработку персональных данных. Будучи прежде всего нормативным актом о конфиденциальности, он имеет значительные последствия для безопасности.

Требования безопасности (Статья 32):

Внедрять надлежащие технические и организационные меры.

Учитывать уровень развития технологий, стоимость внедрения, характер и объём обработки, а также риски.

Меры могут включать псевдонимизацию, шифрование, обеспечение конфиденциальности/целостности/доступности, возможность восстановления и тестирование.

Уведомление о нарушениях (Статьи 33-34):

Уведомить надзорный орган в течение 72 часов после обнаружения нарушения, которое может привести к рискам.

Уведомить затронутых лиц без неоправданной задержки при наличии высокого риска.

Подотчётность (Статья 5(2)):

Контролёры должны демонстрировать соответствие.

Требуется документирование действий по обработке данных, мер безопасности и оценок воздействия на защиту данных.

Правоприменение:

Максимальные штрафы — 20 миллионов евро или 4% глобального оборота.

Надзорные органы действуют всё активнее, налагая значительные штрафы в 2024-2025 годах.

Стандарт безопасности данных индустрии платёжных карт (PCI DSS, Payment Card Industry Data Security Standard)

PCI DSS обязателен для организаций, обрабатывающих, хранящих или передающих данные платёжных карт. Версия 4.0, выпущенная в 2022 году, стала обязательной в марте 2024 года, при этом для некоторых требований установлены продлённые сроки соответствия до 2025 года.

PCI DSS 4.0 содержит 12 требований в рамках 6 целей:

Построение и поддержание безопасной сети и систем (Требования 1-2): межсетевые экраны, безопасные конфигурации.

Защита данных учётных записей (Требования 3-4): защита хранимых данных, шифрование передачи.

Поддержание программы управления уязвимостями (Требования 5-6): защита от вредоносного ПО, безопасная разработка.

Внедрение строгих мер управления доступом (Требования 7-9): ограничение доступа, аутентификация пользователей, ограничение физического доступа.

Регулярный мониторинг и тестирование сетей (Требования 10-11): журналирование, тестирование безопасности.

Поддержание политики информационной безопасности (Требование 12): политики безопасности, процедуры, осведомлённость.

Изменения в версии 4.0 включают:

Индивидуальный подход, позволяющий использовать альтернативные контроли, достигающие целей безопасности.

Усиленные требования к аутентификации, включая многофакторную аутентификацию.

Усиленные требования к шифрованию.

Повышенный акцент на непрерывной безопасности.

Закон о переносимости и подотчётности медицинского страхования (HIPAA)

HIPAA (Health Insurance Portability and Accountability Act) защищает медицинскую информацию в Соединённых Штатах. Правило безопасности

устанавливает требования к электронной защищённой медицинской информации (ePHI, electronic Protected Health Information).

Административные защитные меры: управление безопасностью, безопасность персонала, управление доступом к информации, обучение и процедуры реагирования на инциденты.

Физические защитные меры: контроль доступа к помещениям, безопасность рабочих станций и контроль устройств.

Технические защитные меры: управление доступом, контроль аудита, контроль целостности и безопасность передачи данных.

HIPAA требует анализа рисков и внедрения разумных и надлежащих защитных мер. Согласно данным Управления по гражданским правам Министерства здравоохранения и социальных служб США (HHS Office for Civil Rights), практика правоприменения в 2024-2025 годах демонстрирует увеличение штрафов за недостаточный анализ рисков и управление доступом.

Предложенные в 2024 году обновления направлены на усиление требований Правила безопасности HIPAA, включая обязательное шифрование и усиленный контроль доступа.

Часть 9: Построение программы соответствия

Компоненты программы соответствия

Эффективная программа соответствия включает:

Инвентаризацию требований: знайте, какие нормативные акты, стандарты и контракты применимы. Сопоставьте требования с организационными подразделениями и системами.

Оценку разрывов: сравните текущее состояние с требованиями. Выявите недостатки.

Планирование устранения: приоритизируйте пробелы и разработайте планы их устранения. Выделите ресурсы.

Внедрение контролей: внедрите контроли, отвечающие требованиям. Задокументируйте внедрение.

Мониторинг: отслеживайте соответствие на постоянной основе, а не только во время аудита. Автоматизируйте по возможности.

Управление доказательствами: ведите базу доказательств, подтверждающих соответствие. Организуйте их для быстрого извлечения.

Отчётность: докладывайте о состоянии соответствия руководству и соответствующим заинтересованным сторонам.

Постоянное улучшение: извлекайте уроки из аудитов, инцидентов и нормативных изменений.

Управление множественными фреймворками

Большинство организаций сталкиваются с множественными требованиями соответствия одновременно. Эффективное управление ими требует:

Сопоставления контролей: сопоставьте контроли между фреймворками. Один контроль часто удовлетворяет множественным требованиям. Информативные ссылки NIST CSF предоставляют межфреймворковые сопоставления.

Единой системы контролей: внедрите комплексный набор контролей, охватывающий все требования, а не отдельные контроли для каждого фреймворка.

Интегрированных оценок: по возможности проводите оценки, одновременно охватывающие несколько фреймворков.

Инструментов GRC (Governance, Risk, and Compliance — управление, риски и соответствие): платформы GRC помогают управлять множественными требованиями, отслеживать внедрение контролей и вести базу доказательств.

Соответствие и безопасность

Соответствие и безопасность связаны, но различны:

Соответствие устанавливает минимальные требования. Выполнение стандартов соответствия не гарантирует безопасности. Требования могут быть устаревшими или недостаточными для вашей среды угроз.

Безопасность адресует фактические риски. Эффективная безопасность выходит за рамки соответствия, устраняя конкретные организационные риски.

Безопасность, движимая соответствием, распространена, но проблематична. Организации, выполняющие только требования соответствия, часто имеют пробелы в безопасности.

Соответствие, движимое безопасностью, предпочтительнее. Стройте безопасность на основе оценки рисков, затем демонстрируйте, как контроли удовлетворяют требованиям соответствия.

Нарушения соответствия часто указывают на нарушения безопасности. Но соответствие не доказывает безопасность.

Часть 10: Современные тенденции и перспективы

Конвергенция и дивергенция регулирования

Нормативно-правовой ландшафт демонстрирует как конвергенцию, так и дивергенцию:

Конвергенция: общие концепции присутствуют в разных нормативных актах — риск-ориентированный подход, отчётность об инцидентах, безопасность цепочки поставок, подотчётность. Фреймворки всё чаще ссылаются друг на друга.

Дивергенция: юрисдикционные различия сохраняются. Нормативные акты ЕС делают акцент на конфиденциальности и основных правах. Нормативные акты США различаются по отраслям. Национальные реализации директив ЕС отличаются.

Глобальные организации должны ориентироваться в этой сложности, потенциально применяя различные подходы для разных юрисдикций.

Автоматизация и непрерывное соответствие

Ручные процессы обеспечения соответствия не масштабируются. Тенденции в направлении автоматизации включают:

Политика как код: политики безопасности, выраженные в машиночитаемых форматах, обеспечивающие автоматизированное применение.

Непрерывный мониторинг: инструменты, непрерывно оценивающие соответствие, а не проводящие точечные аудиты.

Автоматизированный сбор доказательств: системы, автоматически фиксирующие и организующие доказательства соответствия.

Соответствие как код: конфигурации инфраструктуры, обеспечивающие выполнение требований соответствия.

Инвестиции в регуляторные технологии (RegTech, Regulatory Technology) растут по мере того, как организации стремятся к эффективности.

Кибербезопасность на уровне совета директоров

Нормативные требования и реалии бизнеса поднимают кибербезопасность на уровень совета директоров:

Правила SEC требуют от публичных компаний раскрытия существенных инцидентов кибербезопасности и описания надзора со стороны совета директоров.

DORA требует от органов управления финансового сектора утверждения и надзора за управлением рисками ИКТ.

NIS2 устанавливает ответственность органов управления и требования к их обучению.

Советам директоров всё чаще необходима экспертиза в области кибербезопасности. Многие организации вводят в состав директоров специалистов с опытом в сфере безопасности.

Руководители по безопасности должны эффективно взаимодействовать с советами директоров — на языке бизнеса, фокусируясь на рисках и стратегии, а не на технических деталях.

Подготовка к будущему

Организации должны готовиться к продолжающейся эволюции регулирования:

Мониторьте нормативные изменения в соответствующих юрисдикциях.

Создавайте адаптируемые программы соответствия, а не точечные решения для текущих требований.

Участвуйте в процессах общественных консультаций для влияния на требования.

Участвуйте в отраслевых ассоциациях для коллективного голоса и совместного обучения.

Инвестируйте в основы безопасности, которые актуальны для любого нормативного фреймворка.

Заключение

Подведём итоги того, что мы рассмотрели в данной лекции о политиках безопасности и соответствии.

Мы начали с иерархии политик безопасности: политики устанавливают требования, стандарты конкретизируют детали, процедуры предоставляют инструкции, а руководства содержат рекомендации. Ключевые политики включают информационную безопасность, допустимое использование, управление доступом, классификацию данных, реагирование на инциденты и непрерывность бизнеса.

ISO 27001 предоставляет международный стандарт для Системы менеджмента информационной безопасности. Версия 2022 года реструктурировала контроли в четыре темы и добавила новые контроли, учитывающие современные практики. Сертификация демонстрирует комплексное управление безопасностью.

Фреймворк кибербезопасности NIST 2.0 организует безопасность в шесть функций: Управление, Идентификация, Защита, Обнаружение, Реагирование и Восстановление. Уровни внедрения и профили помогают организациям надлежащим образом применять фреймворк.

Контроли CIS предоставляют приоритизированные технические контроли. Группы внедрения помогают организациям сосредоточиться на соответствующих контролях с учётом ресурсов и рисков.

Управление безопасностью обеспечивает поддержку организационных целей через вовлечение руководства, чёткие роли, систему политик и измерение эффективности. Аудиты обеспечивают уверенность посредством внутренних и внешних оценок.

Планирование реагирования на инциденты готовит организации к обнаружению, сдерживанию, устранению и восстановлению после инцидентов безопасности. Планы необходимо тестировать посредством кабинетных учений, функциональных учений и полномасштабных симуляций.

Нормативные акты ЕС трансформировали ландшафт соответствия. NIS2 расширяет требования безопасности по отраслям. DORA регулирует цифровую устойчивость финансового сектора. Закон об ИИ регулирует системы искусственного интеллекта. Закон о киберустойчивости устанавливает требования к продуктам с цифровыми элементами.

GDPR, PCI DSS и HIPAA остаются основными драйверами соответствия, требуя мер безопасности, уведомления о нарушениях и подотчётности.

Эффективные программы соответствия интегрируют множественные требования через сопоставление контролей и единые фреймворки. Соответствие необходимо, но недостаточно для безопасности — программы безопасности, основанные на оценке рисков, должны определять соответствие, а не наоборот.

На этом завершается наш цикл лекций по информационной безопасности. Надеюсь, эти лекции предоставили вам прочную основу в принципах, практиках и нормативных аспектах безопасности. Безопасность — это непрерывный путь: продолжайте учиться, следите за эволюцией угроз и нормативных актов и применяйте эти принципы в своей профессиональной деятельности.

Вопросы для обсуждения

1. Как организации могут избежать формального подхода к соответствию, превращая его в настоящее повышение безопасности?
2. С какими трудностями сталкиваются организации при навигации между множественными пересекающимися нормативными фреймворками в разных юрисдикциях?

3. Как растущее число нормативных актов по кибербезопасности во всём мире повлияет на инновации и гибкость бизнеса?
4. Сотрудник использует личный телефон для доступа к корпоративной электронной почте. Какие вопросы политики безопасности это поднимает?
5. Компания проходит аудит соответствия, но в следующем месяце подвергается взлому. Означает ли это, что аудит был бесполезен? Что это говорит нам о взаимосвязи между соответствием требованиям и безопасностью?

Благодарю вас за внимание на протяжении всего курса. Есть ли заключительные вопросы?

Контрольные вопросы

1. Опишите иерархию политик безопасности (политики, стандарты, процедуры, руководства) и объясните назначение каждого уровня.
2. Что такое СМИБ согласно ISO 27001 и каковы основные этапы внедрения?
3. Опишите четыре фазы реагирования на инциденты и объясните, почему планирование и тестирование необходимы.
4. Каковы основные требования безопасности Статьи 32 GDPR (General Data Protection Regulation, Общий регламент защиты данных ЕС) и каковы сроки уведомления о нарушениях?
5. Объясните разницу между безопасностью, движимой соответствием, и соответствием, движимым безопасностью. Какой подход более эффективен?
6. Каково назначение аудита безопасности и как часто его следует проводить?

Ключевые термины

- **ACME**: протокол автоматического управления сертификатами (Automatic Certificate Management Environment)
- **Закон об ИИ (AI Act)**: Закон ЕС об искусственном интеллекте, комплексный регламент, регулирующий системы ИИ, включая те, что используются в сфере безопасности
- **Контроли CIS**: приоритизированный набор лучших практик безопасности от Центра интернет-безопасности
- **CISO**: Директор по информационной безопасности (Chief Information Security Officer), руководитель, ответственный за программу информационной безопасности организации

- **COBIT**: Контрольные цели для информационных и смежных технологий (Control Objectives for Information and Related Technologies), фреймворк управления ИТ
- **Закон о киберустойчивости (Cyber Resilience Act)**: регламент ЕС, устанавливающий требования кибербезопасности для продуктов с цифровыми элементами
- **DORA**: Закон о цифровой операционной устойчивости (Digital Operational Resilience Act), регламент ЕС для кибербезопасности финансового сектора
- **DPO**: Ответственный за защиту данных (Data Protection Officer), роль, требуемая GDPR для надзора за соблюдением требований защиты данных
- **GDPR**: Общий регламент по защите данных (General Data Protection Regulation), регламент ЕС, регулирующий защиту персональных данных
- **GRC**: Управление, риск и соответствие (Governance, Risk, and Compliance), интегрированный подход к управлению этими функциями
- **HIPAA**: Закон о переносимости и подотчётности медицинского страхования (Health Insurance Portability and Accountability Act), закон США о защите медицинских данных
- **Реагирование на инциденты (Incident Response)**: структурированный процесс подготовки, обнаружения, сдерживания и восстановления после инцидентов безопасности
- **СМИБ (ISMS)**: Система менеджмента информационной безопасности, определённая в ISO 27001
- **ISO 27001**: международный стандарт для систем менеджмента информационной безопасности
- **NIS2**: Директива о сетевой и информационной безопасности 2 (Network and Information Security Directive 2), директива ЕС, расширяющая требования кибербезопасности
- **NIST CSF**: Фреймворк кибербезопасности NIST (NIST Cybersecurity Framework), добровольный фреймворк для управления рисками кибербезопасности
- **PCI DSS**: Стандарт безопасности данных индустрии платёжных карт (Payment Card Industry Data Security Standard), для организаций, работающих с данными платёжных карт
- **Центр операций безопасности (SOC)**: централизованный объект для мониторинга, обнаружения и реагирования на события безопасности
- **Отчёт SOC (SOC Report)**: отчёт о контролях сервисной организации (Service Organization Control), обеспечивающий уверенность в контролях поставщика услуг

- **SOX**: Закон Сарбейнса-Оксли (Sarbanes-Oxley Act), законодательство США, требующее контролей финансовой отчётности и аудита ИТ-систем
- **Модель трёх линий (Three Lines Model)**: модель управления, разделяющая функции менеджмента, надзора и гарантий