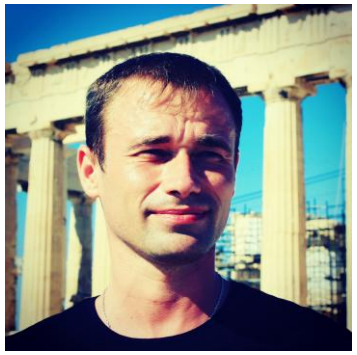
Риск-ориентированный подход vs ISO 27001



Кузьма Пашков

Instructor @ edu-zerde.kz

Содержание (1):

- Роли и модель бизнеса
- Бизнес-процессы и ИТ
- Интересы и базис ИБ
- Риски информатизации
- Доказательный и нормативный подходы
- Программа управления ИБ

Содержание (2):

- Учебные материалы
- Авторизованное обучение PECB
- Тестовый экзамен с обратной связью инструктора

Роли и модель бизнеса (1)

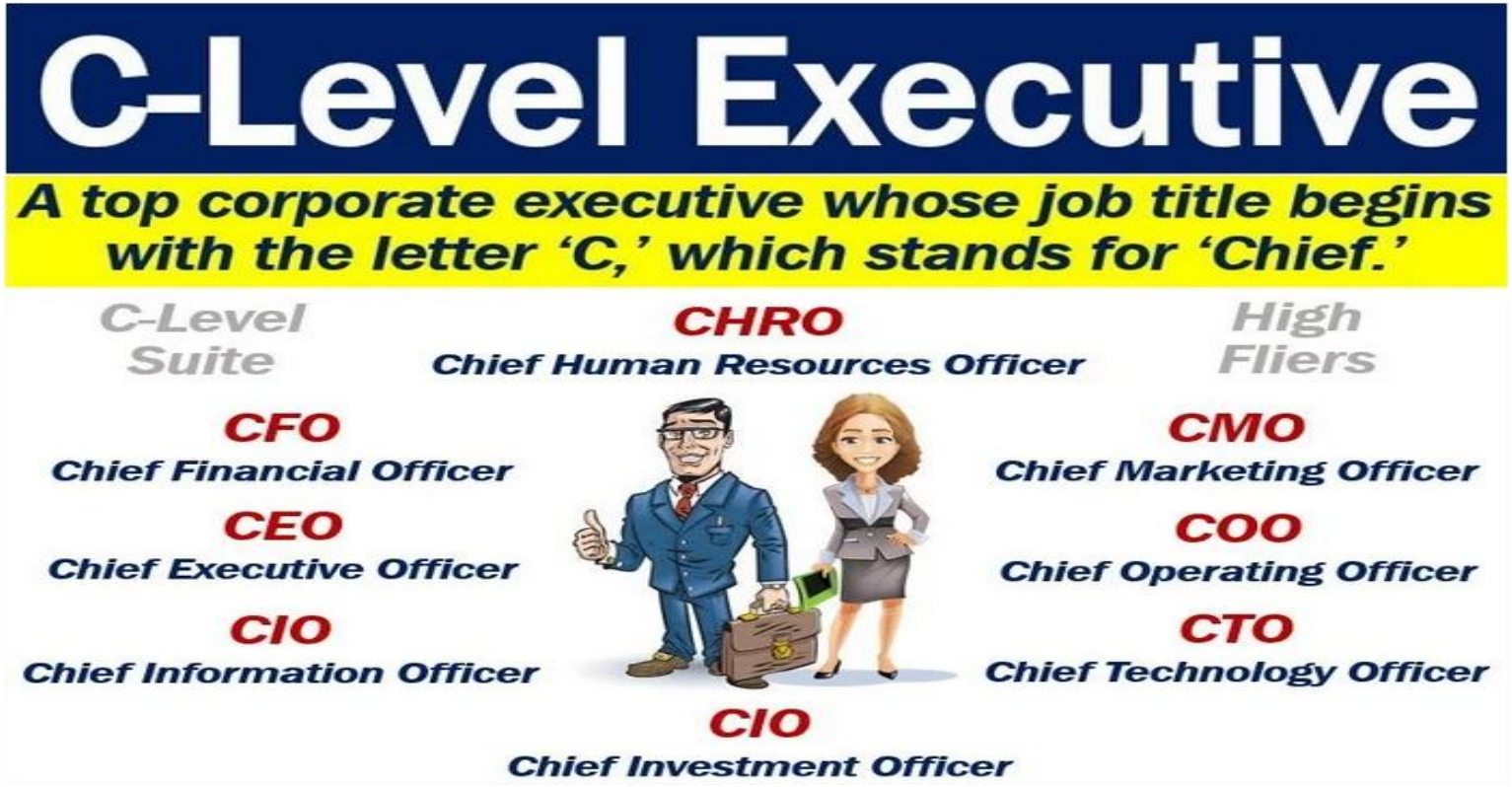
Основные категории Организаций:

- **Коммерческие** (commercial) – увеличить капитализацию, извлечь норму прибыли (profit)
- **Некоммерческие** (non-commercial) – накормить всех голодных детей Германии (non-profit)
- **Государственные** (state-owned) – комбинация целей

ISO 27001 предполагает любые сценарии, например, - коммерческая организация виде **публичного акционерного общества, привлекающего деньги инвесторов на бирже** (listed company)

Characteristic	Commercial Organizations	NPOs
Primary Mission:	Earn profits	Provide services that are of public benefit.
Secondary mission:	Provide services or sell goods in order to make profits	Maintain services by ensuring revenues are greater than expenses
Ownership:	Partners; Shareholders; Sole proprietary.	No ownership (run and managed by members).
Management Control:	Partners; Board of Directors.	Trustees; Coordinators.

Роли и модель бизнеса (2)



Некоторые категории и взаимоотношения ролей:

- Владелец задает **цели Организации**
- **назначает руководителя** высшего звена
- и **наделяет полномочиями** по управлению Организацией **для достижения целей**

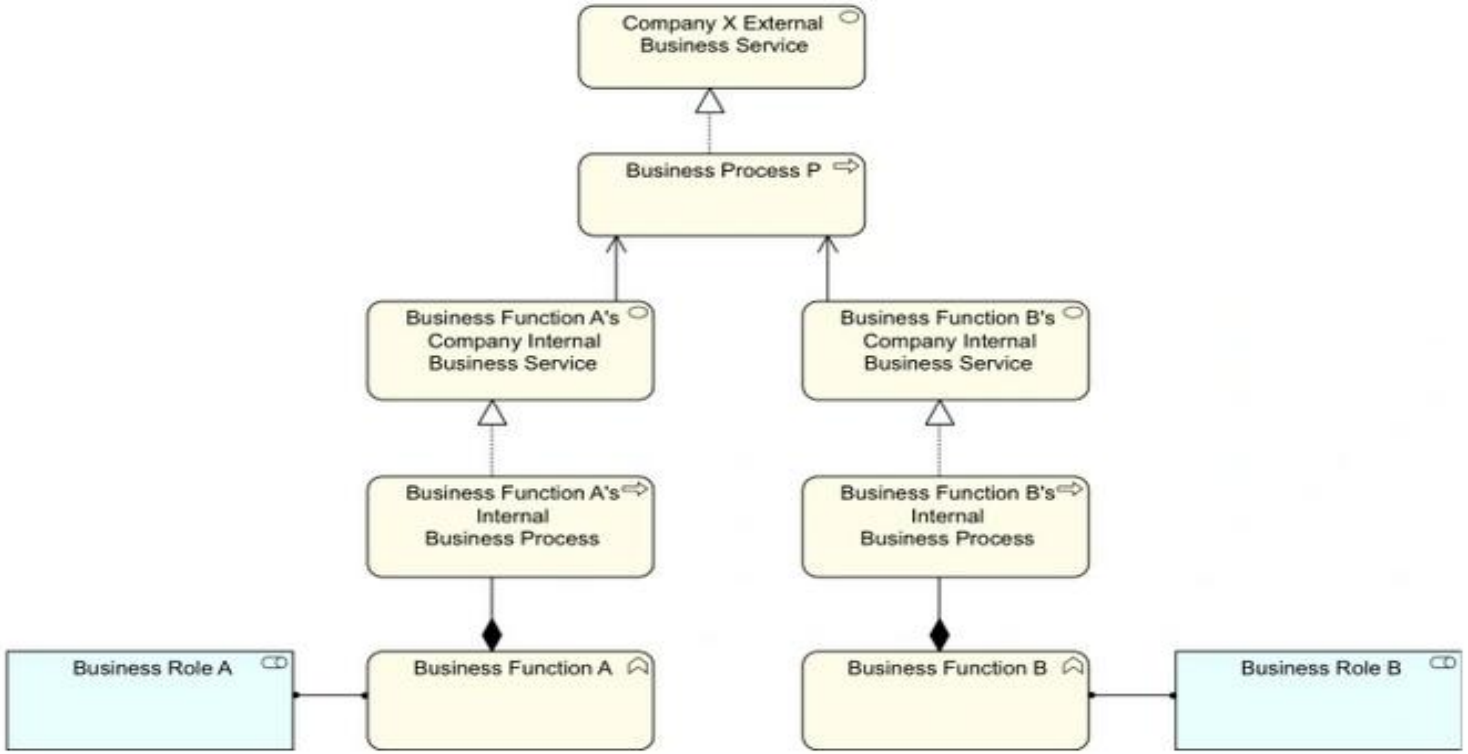
Полномочия руководителей высшего звена **уравновешены их персональной, вплоть до уголовной, ответственностью** за деятельность Организации

Роли и модель бизнеса (3)

Некоторые категории и взаимоотношения ролей:

- Руководители высшего звена могут даже **получать процент от прибыли** Организации, но все же **остаются наемными работниками**
- Владелец **принимает решение о продлении или прекращении полномочий** наемного руководителя

Роли и модель бизнеса (4)



Деятельность любой Организации можно описать:

- В виде экономической модели
- На языке составляющих ее бизнес-процессов
- И бизнес-функций

Формализованное описание экономической модели и его поддержка в актуальном состоянии – **нетривиальный, трудоемкий и связанный с разнообразием проблем процесс**

Бизнес-процессы и ИТ (1)

Составляющие бизнес-процесса:

- Персонал (и организационно-распорядительная документация)
- Рабочее пространство
- ИТ-услуга

Бизнес-процессы и ИТ (2)

Уровни автоматизации бизнес-процесса:

- Ручной (без ИТ-услуги)
- Частично автоматизированный (требуются все три составляющие)
- Полностью автоматизированный (без персонала)

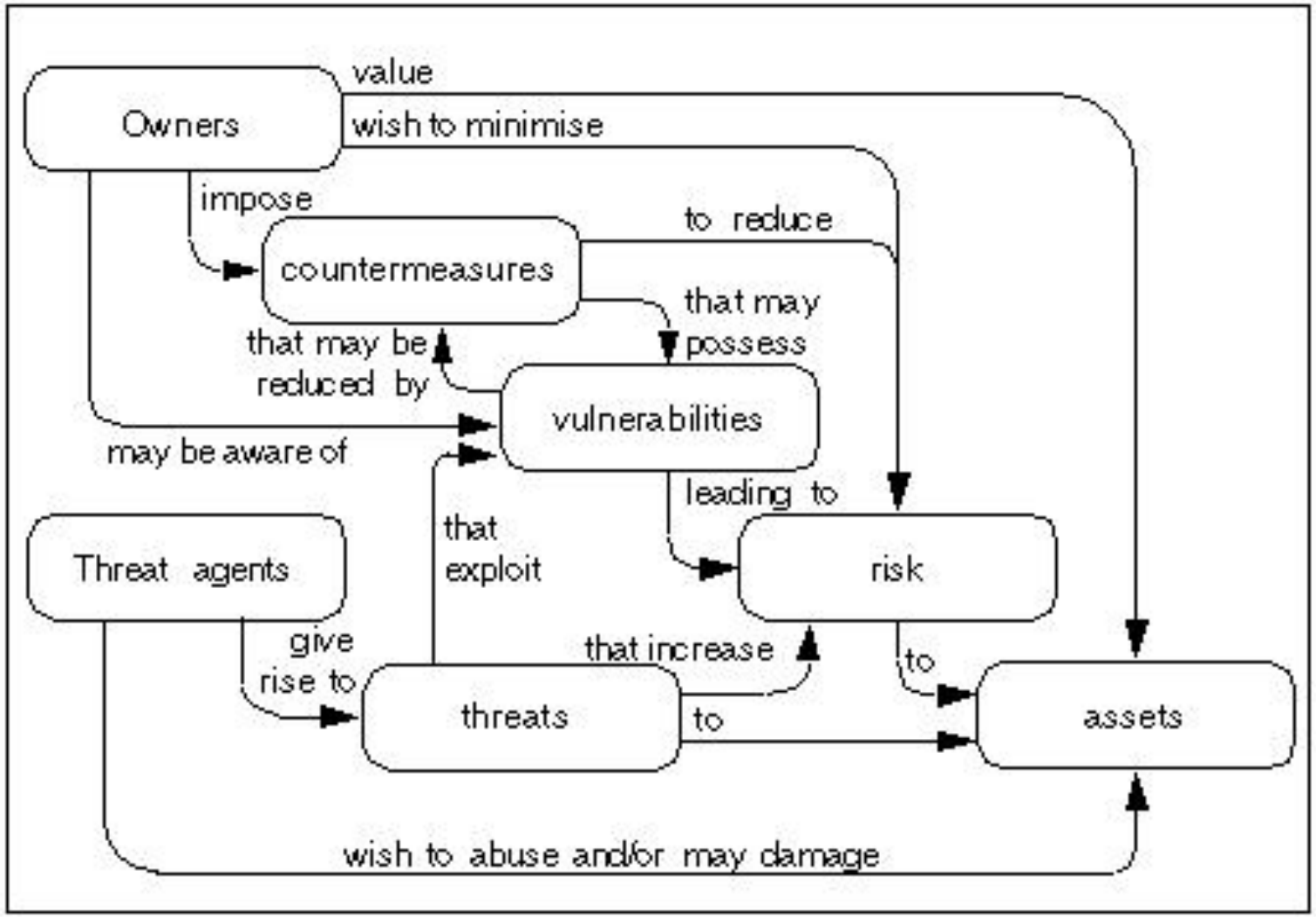
Большая часть бизнес-процессов в Организациях автоматизирована частично.

Прямая корреляция между уровнем автоматизации и измеримой пользой для Организации

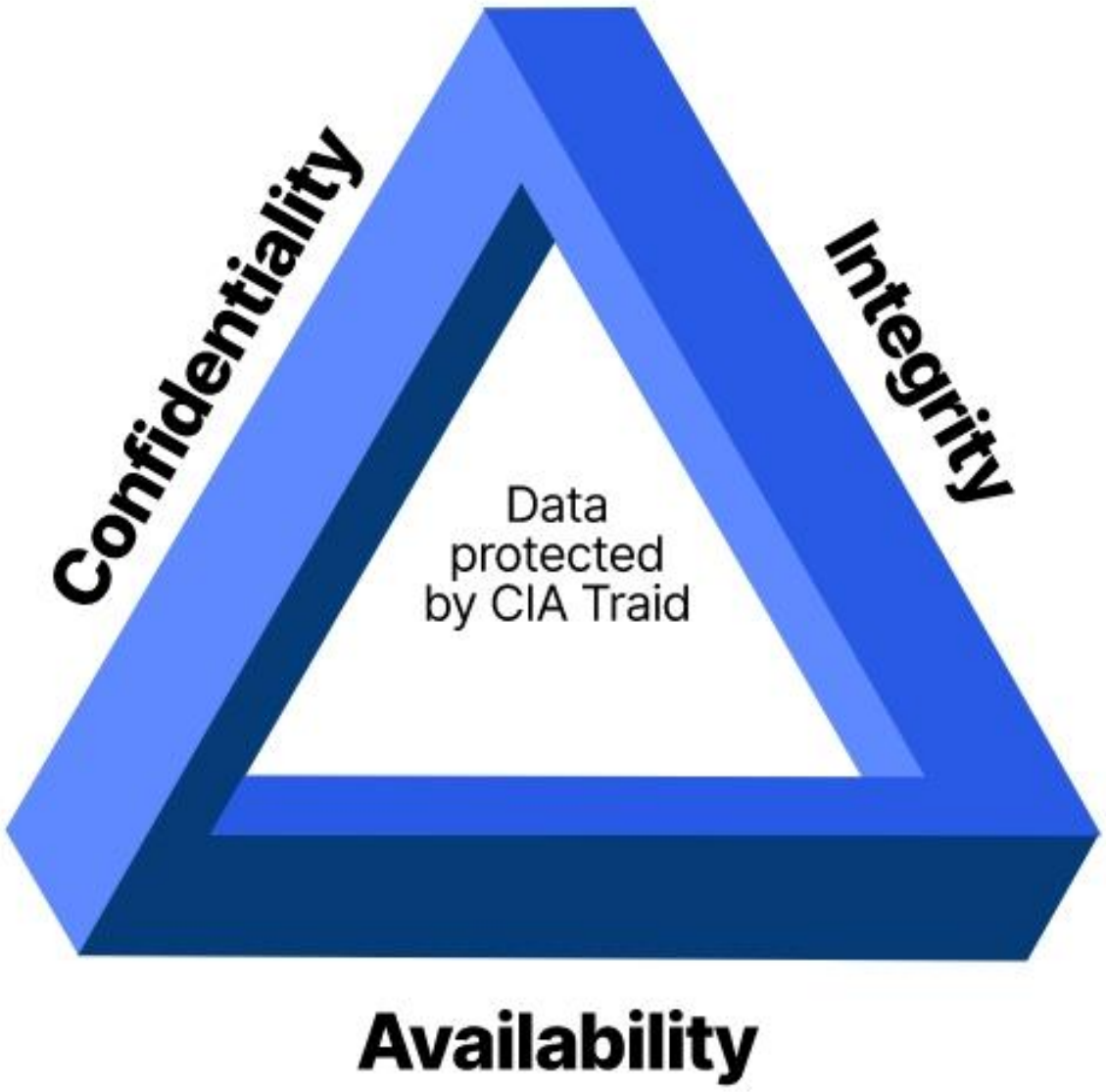
Интересы и базис ИБ (1)

Использование ИТ для автоматизации бизнес-процессов кроме пользы:

- **порождает все больше нематериальных активов составляющих ценность** для Организации
- В виде **информационных ресурсов**
- **Нарушение свойств** которых **угрозами**
- Наносит **ущерб интересам владельцев**



Интересы и базис ИБ (2)



- **Базисом информационной безопасности** как научной дисциплины **является информационный ресурс, составляющий ценность для субъекта**

- ИБ в том числе исследует влияние **изменений свойств информационных ресурсов на интересы субъектов в связи с реализацией угроз**

Риски информатизации (1)

Основные категории рисков:

- **Финансовые** связаны с финансовыми записями, транзакциями и остатками на счетах
- **Операционные** связаны с эффективностью и результативностью операционной практики

Эти категории рисков значимы исторически для руководителей Организации

Риски информатизации (2)

Такой же значимой стала категория рисков информатизации в составе:

- **Риски ИТ** связанные с использованием информационных технологий
- **Риски ИБ** связанные с нарушением свойств информационных ресурсов составляющих ценность
- **Риски Непрерывности Бизнеса** связанные с нарушением непрерывности бизнес-процессов и функций

ISO 27001 фокусируется рисках ИБ для достижения целей Организации посредством гибридного подхода

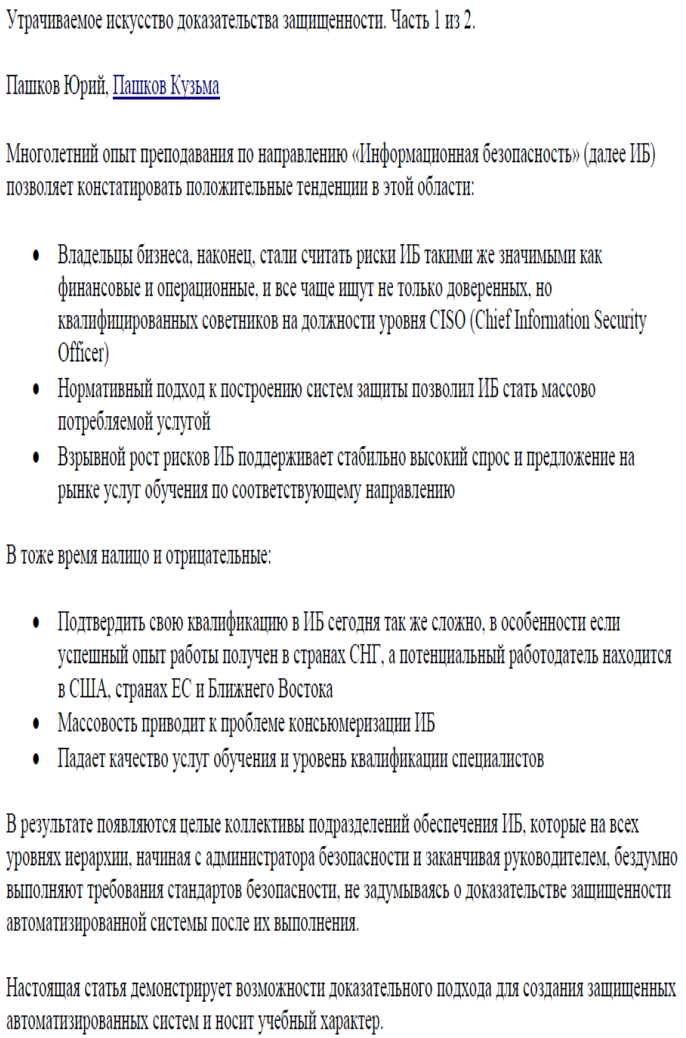
Доказательный и нормативный подходы к ИБ (1)

Доказательный подход к построению информационных систем в защищенном исполнении предполагает:

- Формулирование политики безопасности
- Выбор модели безопасности
- Формальное доказательство
- Интерпретация

Применяется для защиты уникальных интересов.
В ISO 27001 **не рассматривается**

Научная статья «Утрачиваемое искусство доказательства защищенности»



Утрачиваемое искусство доказательства защищенности. Часть 1 из 2.

Пашков Юрий, Пашков Кузьма

Многолетний опыт преподавания по направлению «Информационная безопасность» (далее ИБ) позволяет констатировать положительные тенденции в этой области:

- Владельцы бизнеса, наконец, стали считать риски ИБ такими же значимыми как финансовые и операционные, и все чаще ищут не только доверенных, но квалифицированных советников на должности уровня CISO (Chief Information Security Officer)
- Нормативный подход к построению систем защиты позволил ИБ стать массово потребляемой услугой
- Взрывной рост рисков ИБ поддерживает стабильно высокий спрос и предложение на рынке услуг обучения по соответствующему направлению

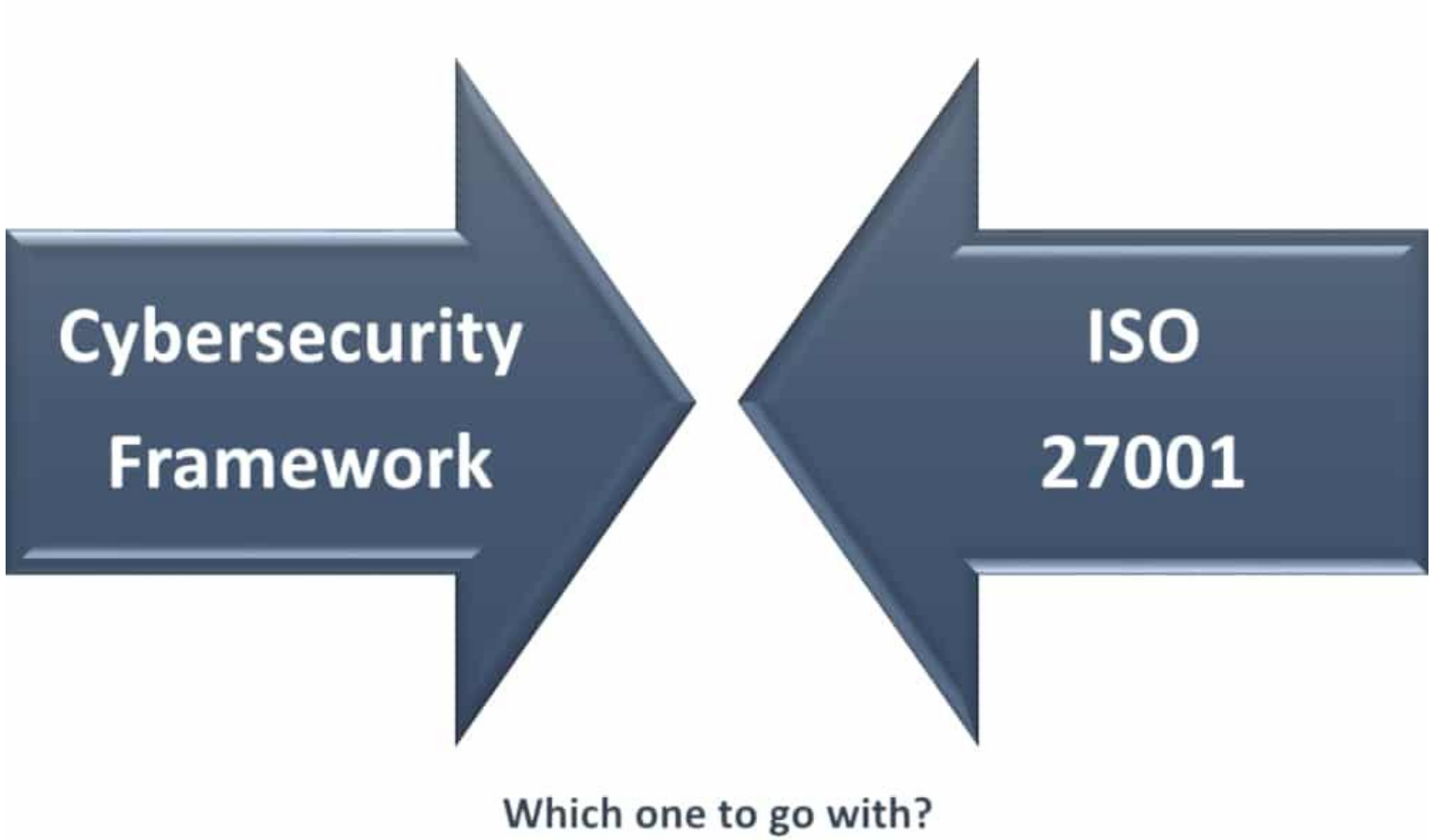
В тоже время налицо и отрицательные:

- Подтвердить свою квалификацию в ИБ сегодня так же сложно, в особенности если успешный опыт работы получен в странах СНГ, а потенциальный работодатель находится в США, странах ЕС и Ближнего Востока
- Массовость приводит к проблеме консьюмеризации ИБ
- Падает качество услуг обучения и уровень квалификации специалистов

В результате появляются целые коллективы подразделений обеспечения ИБ, которые на всех уровнях иерархии, начиная с администратора безопасности и заканчивая руководителем, бездумно выполняют требования стандартов безопасности, не задумываясь о доказательстве защищенности автоматизированной системы после их выполнения.

Настоящая статья демонстрирует возможности доказательного подхода для создания защищенных автоматизированных систем и носит учебный характер.

Доказательный и нормативный подходы к ИБ (2)



Нормативный подход к построению информационных систем в защищенном исполнении предполагает:

- Определение отрасли и юрисдикции
- Следование релевантным стандартам
- и/или их национальным производным

Применяется для защиты универсальных интересов. **Изучается в** ISO27001.

Программа управления ИБ (1)

Программа управления ИБ предполагает:

- Получение **обоснованной уверенности в достижении целей** Организации
- за счет **выделенного подразделения, курируемого руководителем высшего звена**
- **Уполномоченного и ответственного** за
- **Разработку, реализацию и совершенствование**
- **Программы управления ИБ как опционального свойства системы делопроизводства** Организации (далее СУИБ)
- в составе групп процессов **формализованных, облеченных в бумажную форму и реализованных в соответствии с описанием**

Учебные материалы

Учебные материалы включают:

- **Детальные разъяснения** требований стандарта
- **Описание каждой группы процессов** СУИБ
- **Рекомендации по прохождению добровольной сертификации** СУИБ Организации

PECB

IAS ACCREDITED Personnel Certification Body PCB-111

UKAS PERSONNEL CERTIFICATION 21923

Professional Evaluation and Certification Board

hereby attests that

Kuzma Pashkov

is awarded the title

PECB Certified ISO/IEC 27001 Lead Implementer

having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

Certificate Number: ISLI1165747-2024-10
Issue Date: 2024-10-17
This certificate is valid for three years for the purpose of PECB certification

Carolina Cabezas
Chief Compliance Officer

Авторизованное обучение PECB (1)

- **Продолжительность:** 5 дней (сдача экзамена на 5 день)
- **Формат:** семинар (80% лекции / 20% практика)
- **Ближайшие даты:** 28.04-2.05.2025
- **Стоимость:** 665 000 KZT

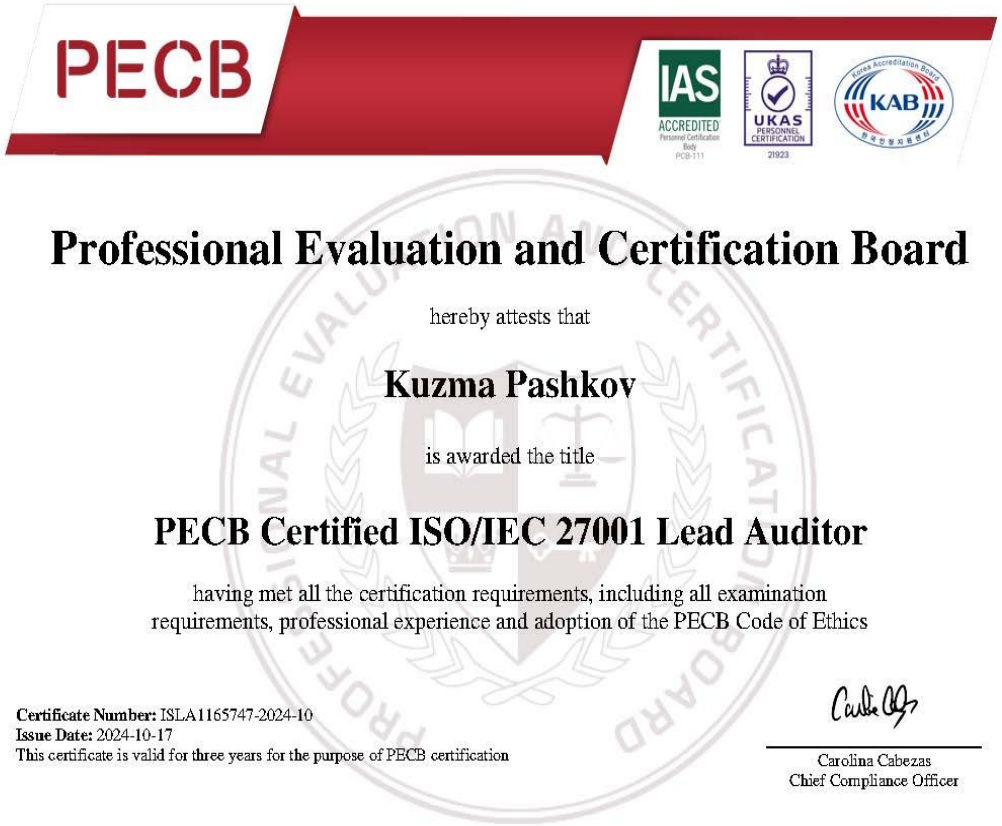
https://edu-zerde.kz/pecb-iso-27001/

Авторизованное обучение PECB (1)

- **Продолжительность:** 5 дней (сдача экзамена на 5 день)
- **Формат:** семинар (80% лекции / 20% практика)
- **Ближайшие даты:** 3-7.11.2025
- **Стоимость:** 665 000 KZT

https://edu-zerde.kz/pecb-iso-27001/

Авторизованное обучение PECB (3)



PECB

Professional Evaluation and Certification Board

hereby attests that

Kuzma Pashkov

is awarded the title

PECB Certified ISO/IEC 27001 Lead Auditor

having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

Certificate Number: ISLA1165747-2024-10
Issue Date: 2024-10-17
This certificate is valid for three years for the purpose of PECB certification

Carolina Cabezas
Chief Compliance Officer

- Курс дает вам все необходимое для сдачи **сертификационного экзамена** и последующего получения профессиональной сертификации

- https://edu-zerde.kz/pecb-iso-27001/

Тестовый экзамен с обратной связью инструктора

Оценочный тест с вопросами формата и уровня сложности как на экзамене CISM

ISO27001_AssessmentTest60QAEs

Обсуждение с коллегами в чате Telegram @AskKuzmaCyberResilience


PECB

BEYOND RECOGNITION

Professional Evaluation and Certification Board

RECOGNIZES THAT

Kuzma Pashkov

IS HEREBY APPROVED AS

Certified Trainer

Certificate Number: CT07836-10-2024
Valid up to: October 21, 2027

Tim Rama, CEO

trainer@pecb.com | www.pecb.com

Эффективная методика подготовки

Алтын a.suleymenova@zerde-edu.kz

Кузьма AskKuzma@gmail.com

Жайдарлы zh.zhaydarly@zerde-edu.kz

PECB

ЗЕРДЕ

https://pecb.com https://askkuzma.kz https://edu-zerde.kz