КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Объединяем всех участников отрасли и помогаем решать профессиональные задачи

24 апреля 2025г

Ежегодная конференция Кода безопасности. Пространство Freedom. Казанская ул., д.7

Интеграционные решения обеспечения функциональной безопасности цифровых экосистем предприятий и классификация внеклассических рисков

Мялковский Игорь Константинович

Управляющий федеральной компании ЭТМ по взаимодействию с ВУЗами и отраслевыми учебными центрами www.etm.ru
Почетный член правления клуба ИТ директоров Санкт-Петербурга http://www.spbcioclub.ru/
Член федеральной экспертной комиссии Президента России при СПбГУ https://spbu.ru/,
Член Государственной экзаменационной комиссии СПбГЭТУ «ЛЭТИ» https://etu.ru/
Руководитель всероссийских соревнований студентов университетов ЭП, ЭУП и ЭПАПК

Клуб Мероприятия Новости Spbcioclub.ru ВСТУПИТЬ В КЛУБ ВОЙТИ

Мы за партнерство профессионалов

https://congress.spbcioclub.ru/

SPB CIO CLUB

профессиональное сообщество ИТ-директоров ведущих компаний Северо-Западного региона

XX юбилейный конгресс ИТ-директоров СЗФО 23 мая 2025г

Миссия «SPb CIO Club» — поддержка и развитие профессионального сообщества ИТ-руководителей

Структура АСЗИ промышленного предприятия. Системный подход - образ мышления специалиста

Цель АСЗИ: гарантировать руководству, что его задачи в части функциональной безопасности и защиты конфиденциальной информации будут выполняться с заданной производительностью и результативностью (к установленному сроку). Конкретная реализация цели в виде SLA (OLA) и клиентоцентричных процессов системы

АСЗИ (АИС): > ГОСТ 34.003-90

Ищите в хаосе систему
А. Эйнштейн

Миссия системы - зачем создана

$$C=\Sigma Э_i$$

Внешние воздействия на АСЗИ:
- Законы
- Место
- Др условия работы
- Метасистема
- Суперсистема

Внешние партнеры ИБ: облачные, аутсорсинг

Люди или ИИ - ЛПР

Память и история системы

информация

ТС, ПО ОПО+СПО), ОРД

АСЗИ

Автоматическая или гибридная

бюджет

Архитектура: Σ протоколов технологий:
- Бизнес-процессы
- Вспомогательные или обеспечивающие процессы

Вспомогательные подсистемы

Хаос ОБИ:
1. Противоречия законодательства
2. Нет единства терминов ИБ
3. Нет единой стратегии развития
4. Нет системного подхода и единой стратегии развития

Внешние и внутренние клиенты АСЗИ

KPI, CSAT, CES

Системный подход. Архитектура АСЗИ

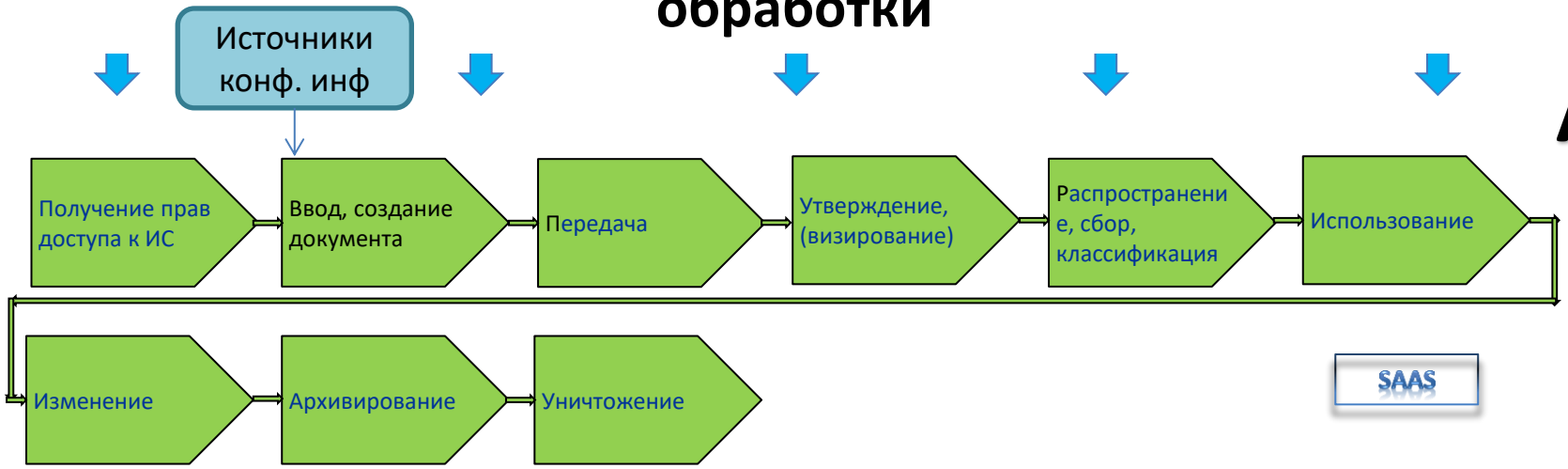
ИСО 27001, 17799, COBIT, СТР-К

Конфиденциальность | **Целостность** | **Доступность**

Аутентичность – подтверждение подлинности и достоверности эл документов

Неотказуемость – невозможность отрицания совершенных действий

Системный аудит архитектуры АСЗИ - процесс проверки уровня защиты конфиденциальной информации (каждого вида тайны из 58) на всех этапах ее обработки



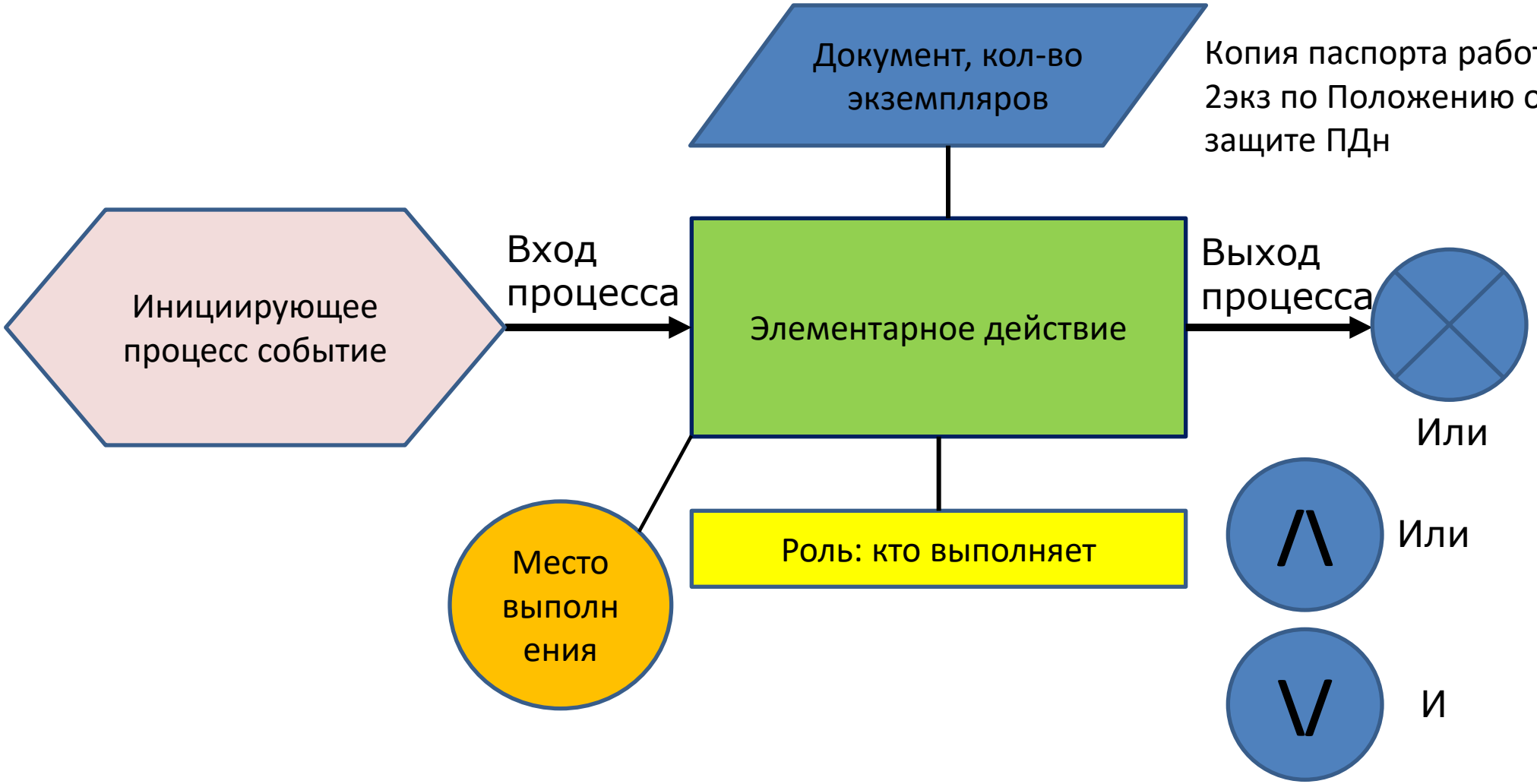
$$A=\Sigma Пр_i$$

У нас дыры в безопасности! - Хорошо еще, что у нас хоть что-то в безопасности

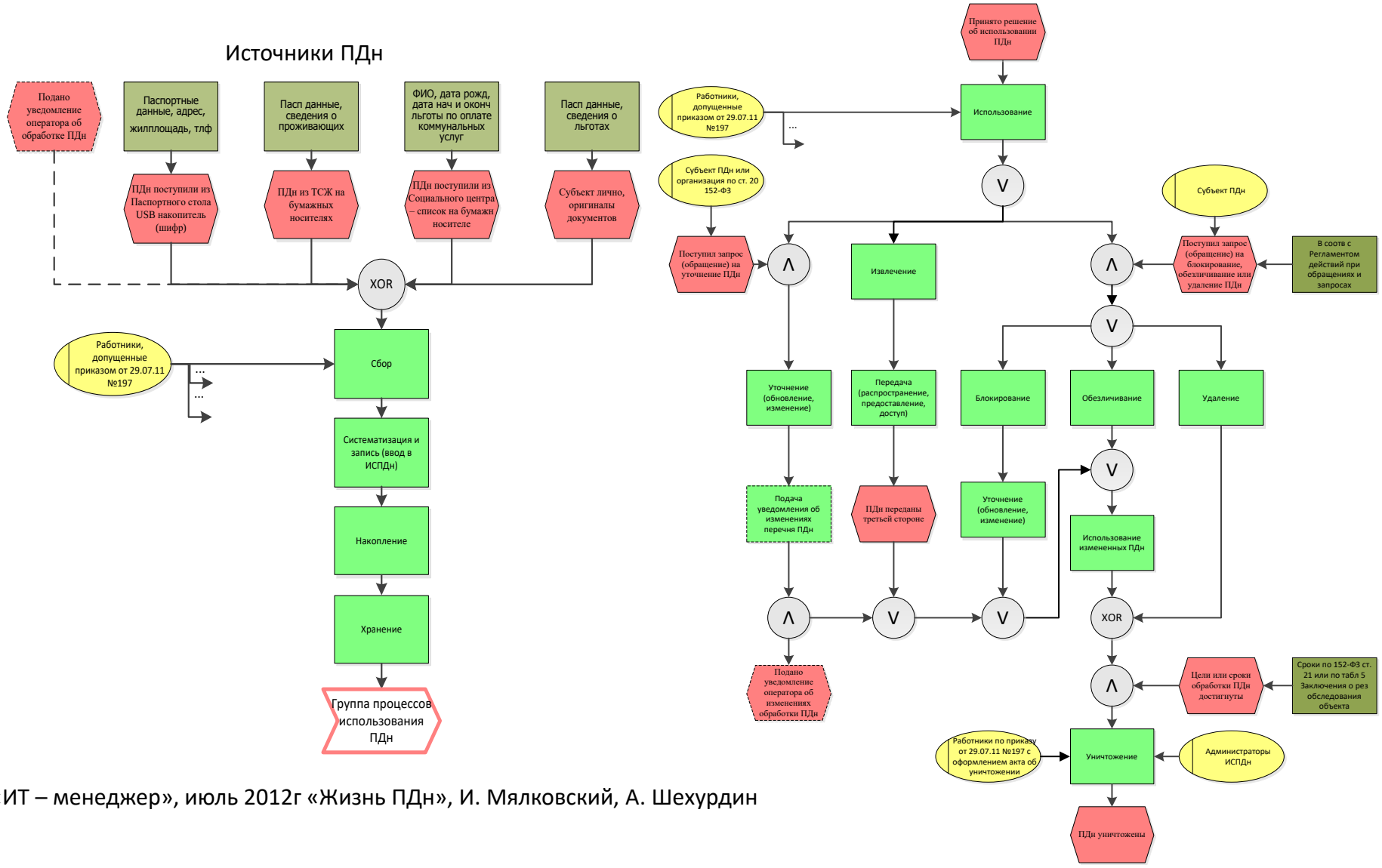
Моделирование архитектуры АСЗИ в нотации Aris 8.0

Варианты: ELMA, BPMN,….

Важная цель моделирования – сократить затраты путем объединения путей обработки инф разных видов тайн там, где возможно



Пример модели процесса обработки ПДн на этапах жизненного цикла ПДн согласно ст. 3 п.3 152-ФЗ (без номеров помещений и ролей)



Журнал «ИТ – менеджер», июль 2012г «Жизнь ПДн», И. Мялковский, А. Шехурдин

Пример: выписка из 187-ФЗ 26.07.2017г ст. 2 Основные понятия

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О БЕЗОПАСНОСТИ
КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Принят
Государственной Думой
12 июля 2017 года

РД-50-680-88 АС. Основные положения

1.1. АС представляет собой **организационно-техническую систему**, обеспечивающую выработку решений на основе автоматизации информационных процессов в различных сферах деятельности (управление, проектирование, производство и т.д.) или их сочетаниях.

П.1. Автоматизированная система управления – комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами;

АСУ – комплекс, а не система, и она для контроля (не управления) и потом все же для управления тоже !!!

Пример противоречий терминов

Термин	Где встречается?	Что это?
Уровень значимости информации	Приказ ФСТЭК 17 -14	Абстрактная величина. «Уровень значимости информации - степень возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности, целостности или доступности информации.»
Уровень защищенности информации	149-ФЗ, Приказ 17 ФСТЭК	Абстрактная величина, определения нет. Некое состояние системы, при котором выполняются определенные требования к ИБ в ней.
Уровень защищенности ПДн	152-ФЗ, ПП1119, Пр 17, Пр 21-14	Конкретный показатель (1-4). «Комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности ПДн при их обработке в ИСПДн»
Уровень защищенности ИС	152-ФЗ	Абстрактная величина, определения нет. По сути, некое состояние системы, при котором выполняются определенные требования к ИБ в ней.
Класс защищенности ИС	Приказ 17 СТР-К	Конкретный показатель (1-4). «Классификация информационной системы проводится в зависимости от значимости обрабатываемой в ней информации и масштаба информационной системы (федеральный, региональный, объектовый)»
Уровень полноты безопасности УПБ	ГОСТ Р МЭК 61511-1-2018	УПБ (safety integrity level; SIL): Дискретный уровень (принимающий одно из четырех возможных значений) определяющий требования к полноте безопасности, которая должна быть достигнута реализуемой ПСБ – приборной системой безопасности

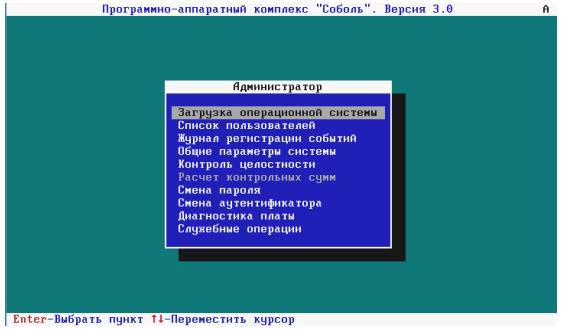
Комплексный подход к ФБ и ИБ

1. Комплекс - набор из двух и более типов элементов, без цели, учета связей и динамики развития
2. Взят из практики, обыденного (бытового) сознания, обычное перечисление, список, перечень
3. Комплекс не имеет цели, предназначен для выполнения определенной функции
4. Не учитывает воздействия суперсистемы (старшей системы), метасистемы (внешней системы).
5. Не учитывает историю и память системы
6. Позволяет объединить несколько систем без рассмотрения достижений цели полисистемы (объединенной, интегрированной или общей системы предприятий – нескольких участников условной жизни объекта)
7. Субъективный подход
8. Комплекс – почти всегда может быть рассмотрен, как система, но не каждая система - комплекс

АПКШ Континент 3.9. ЦУС - Сервер Доступа. Платформа IPC100. КриптоПро 4.0. КС2 HSEC-3.9-IPC100-CM-ACS-CSP4.0-KC2-SP1Y

ПАК «Соболь»

Аппаратно-программный модуль доверенной загрузки



Результат комплексного подхода к ФБ и ИБ - что-то новенькое полезное (не очень совместимое) возьму у каждого вендора

ГОСТ Р МЭК 61508 – 1- 2012

Нет гарантий:

1. Учета всех рисков
2. Исполнения Политики ИБ
3. Достижения цели АСЗИ
4. учета динамики несоответствий между точечными решениями разных средств защиты

Комплексный подход интегратора к ОБИ роботизированной интеграции АИС в ЖЦО капитального строительства

Виртуализация VDI + HyperV (VMVare)

ERP+CRM+MES+WMS. Система управления от 475 000 рублей.

АРМ: СУБД поставщика

RPA: Счет на оплату в Интернет-магазине

vGate + Соболь + Мониторинг RPA (FireMon) + антивирус ЛК

NanoCAD BIM «Электро»

СметаВИЗАРД

Контур-Диадок

Шифрование серверное

АРМ Контрагента

RPA: интеграция iPRO + NanoCAD BIM «Электро»

Где гарантия того, что сделали все для реализации Политики ИБ?

«Точечный» подход интегратора

Центральный офис

Виртуализация VDI + HyperV (VMVare)

RPA + ИИ

Счет на оплату клиенту в интернет-магазине

vGate + Соболь + Мониторинг RPA (FireMon)

1С:ERP: ПДн

АПКШ Континент 3,9 IPC50

ГОСТ 28147

1С:СЭД ЦО

АРМ Контрагента 1С:СЭД и 1С:УТ

Контур-Диадок

1С:СЭД филиал

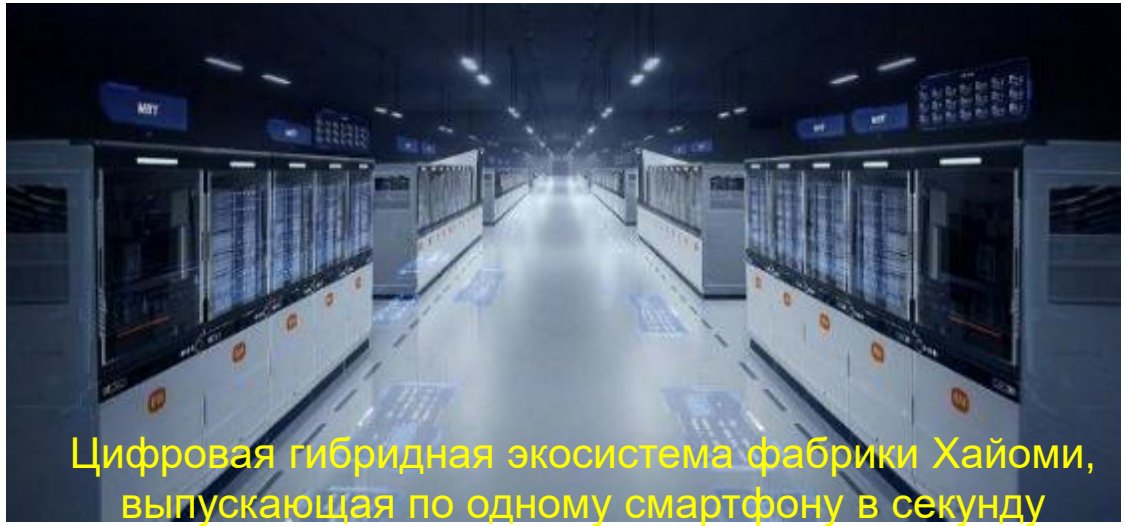
RPA + ИИ: интеграция данных из одной системы, например, из фед реестра сметных нормативов для отображения сведений в другой в сметаВИЗАРД-гипотетически

RPA + ИИ: Первичный рекрутинг «рутинных специалистов» - обзвон

Новые для ФБ признаки цифровой экосистемы

1. Синергия отлаженного взаимодействия элементов
2. Самовоспроизводство и тиражирования, например используя модули отлаженного Service Desk
3. Условная самодостаточность ресурсов для развития - повышения производительности взаимодействия открытых систем

Налицо стратегическое несоответствие имеющихся политик ИБ, стратегий ИТ и развития цивилизации



Цифровая гибридная экосистема фабрики Хайоми, выпускающая по одному смартфону в секунду

Источник: https://www.ixbt.com/news/2024/07/09/xiaomi-24-1.html

Внеклассическое управление рисками цифровой экосистемы с ИИ и RPA

Три классических способа управления рисками:

1. Принять как есть
2. Применить меры противодействия
3. Перевести риск на другого: более квалифицированного или имеющего больше полномочий. Страхование

Методические ошибки моделирования угроз при разработке Политики ИБ (ФБ) с использованием ИИ и RPA по Даниеэлю Канеману (нобелевский лауреат):

1. Легкость, с какой возможные катастрофы (риски) приходят в голову, не обязательно отражает их реальную вероятность (угрозу)
2. Риск можно сильно недооценить, если некоторые возможные опасности (угрозы) трудно представить, или они не успели прийти в голову (неполная модель – не системный, а комплексный был подход при аудите информзащиты организации – пропустили важные факторы в модели угроз)
3. Эффект привязки к конечной цели. Во многих случаях оценок при разработке модели угроз и аудитах люди начинают с исходной величины, а потом корректируют свое направление рассуждений в сторону ожидаемого окончательного ответа. При проектировании RPA и АСЗИ с ИИ нужна более точная стратегия управления рисками (ИИ учится быстрее человека, но дешевле покупать самый простой ИИ).
4. Политике ИБ нужен системный подход!!! Комплексный – для частных случаев аудитов развития АСЗИ

Классификация рисков цифровых экосистем среднего бизнеса при использовании RPA и ИИ

Риски взаимодействия цифровых систем

Честность партнеров – необходимое условие синергии и интеграции в жизненном цикле объекта производства или кап строительства

Нарушения (сбои) регламентов

Несоответствие сроков получения прибыли и ее ожидаемых размеров

Риски применения ИИ и программных роботов

Комплементарные риски

Сокращения сотрудников и их последствия с уводом части клиентской базы

Перерасход бюджета в связи с неверным выбором решения RPA

Безответственное приуменьшение риска взлома и НСД, потому что есть ИИ в среднем бизнесе

Риски стратегии цифровой трансформации

Управляющие технологии и ОБИ развиваются медленнее остальных

Коллективное сознание аналогично клеткам организма. Оно способно увлечь в неправильном направлении

Ограничение настроек защиты инф только ограничениями прав доступа

Риски договоров с иностранными хостинг компаниями

Операционный риски эксплуатации сложных цифровых систем

Не все процессы предприятия нужно оптимизировать и делать максимально эффективными. Некоторые могут оставаться привычными, как клавиатура QWERTY

Риски в следствие несоблюдения противоречивого законодательства (недостаточной квалификации)

Риски квантового шифрования

Куби́т (q-бит, кьюбит, кубит; от *quantum bit*) — наименьшая единица информации в квантовом компьютере (аналог бита в обычном компьютере), использующаяся в квантовых вычислениях.

Так, как будто у будущих хакеров не появится методов взлома на основе квантовых компьютеров

Мы предлагаем заказчикам
использовать то,
чего никто в мире не понимает
в хаосе квантов,
гарантируя им
абсолютную безупречность
результата – невозможности
расшифровать

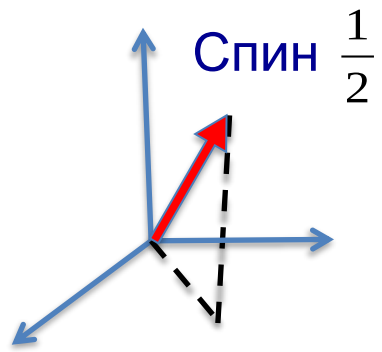
Перспективы использования квантовых технологий для создания новых информационных сервисов

https://www.youtube.com/watch?v=8cTNMuw8R98

Проще Википедии

См. в материалах презентацию дтн Астафьева, Сколково \ МФТИ

Квантовый бит или кубит может одновременно находится в двух состояниях, оцениваемых вероятностями и суперпозицией в отличие от обычного бита в двух определенных состояниях 0 или 1

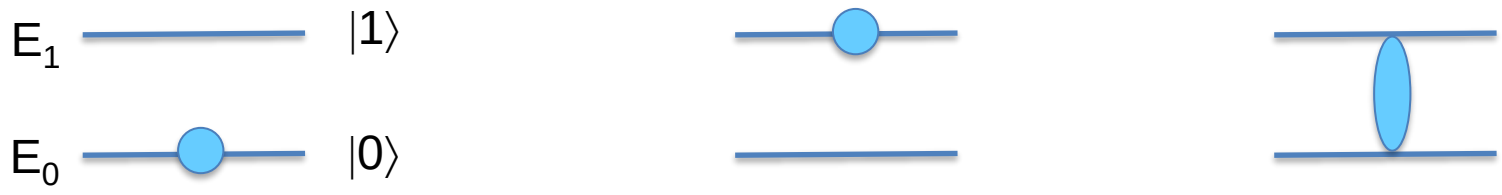


Информация кодируется в двух-уровневых квантовых системах

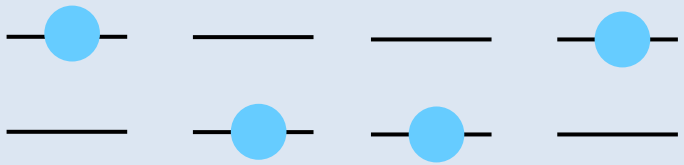
Нижнее состояние: $0 \rightarrow |0\rangle$

Возбуждённое состояние: $1 \rightarrow |1\rangle$

Суперпозиция: $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$

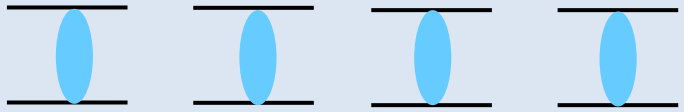


Кодирование чисел



$|1001\rangle$

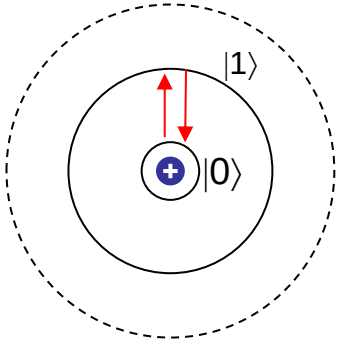
Суперпозиция



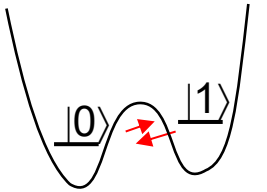
$$\frac{|0000\rangle + |0001\rangle + |0010\rangle + \cdots + |1110\rangle + |1111\rangle}{\sqrt{16}}$$

Элементарная логика (одно- и двух-кубитные операции): NOT, SWAP, CNOT

Атомы, ионы



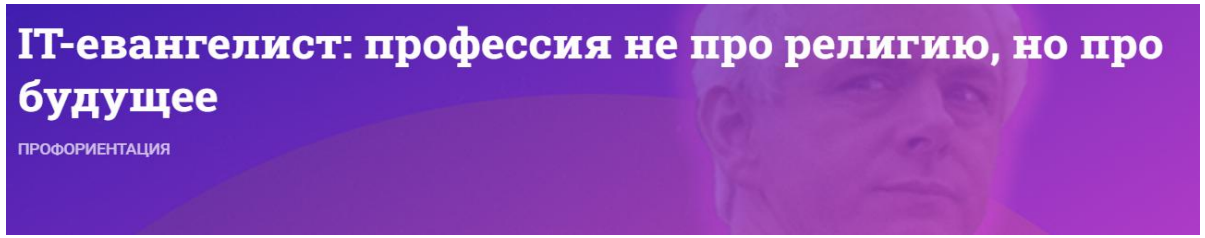
Квантовые точки



Сверхпроводниковые наноструктуры

Организационные риски цифровых экосистем

Признаки ИТ-экосистемы, создающие неклассические угрозы:



1. Отлаженное взаимодействие – синергия
2. Саморазвитие
3. Активное противодействие внешним негативным воздействиям – силовое синергетическое поле
4. Единая информационная среда
5. Творческая тусовка или почти творческая секта – технологические евангелисты

Технологический евангелист – специалист, профессионально занимающийся пропагандой в сфере информационных технологий.

Два необычных риска новых функций управления:

- потери управления толпой (потери влияния), «стадный эффект»
- неуправляемого лидера (евангелиста)

Две тенденции безопасного взаимодействия автоматизированных цифровых систем в электроэнергетике

Итоги наблюдений: внедрение программных роботов по отраслям в 2024г

Рынок PRA (программных роботов с ИИ) в 2024г:

1. Комплексный или системный подходы к цифровой трансформации рутинных операций
2. Роботы с ИИ (RPA) начинает эволюционировать в экосистемы предприятий для создания «цифровых сотрудников» нового уровня качества (с новыми свойствами отсутствия усталости, отсутствия з\п и т.п.) на основе различных технологий RPA + IDP, RPA+ML, RPA+ LLM
3. Гиперавтоматизация (или сверх автоматизация всего)
4. Встроенные системы обучения персонала с RPA ИИ на местах

Различия классической автоматизации и программной роботизации

И что с этим делать безопасникам?

Традиционные системы автоматизации документов	Системы программных роботов RPA
разработчик программного обеспечения **создает список действий** для автоматизации задач и взаимодействия с сервером с помощью серверных интерфейсов прикладного программирования (API) или специального языка сценариев	системы RPA разрабатывают **список действий, наблюдая за тем, как пользователь выполняет эту задачу в графическом пользовательском интерфейсе приложения** (GUI), а затем **автоматизирует процесс**, повторяя эти задачи непосредственно в **графическом интерфейсе пользователя**.

Тренды роботизации с ИИ и что с этим делать безопасникам?

Интеграция RPA с системами «интеллектуальной автоматизации», с ИИ и нейросетями, например GPT

Смещение основной точки создания бизнес-ценности обратно с Unattended на Attended – автоматизацию, благодаря прогрессу ИИ и рекордно низкой безработице

Обеспечение совместимости с BRM, CRM и ERP системами

Интегрированные интеллектуальные помощники в создании процессов – модули Copilot

Усиление роли гражданской разработки за счет обогащения No-Code подхода AutoGen инструментами программирования

Работа с неструктурированными данными и с нечеткой логикой

Смещение фокуса внимания RPA с бухгалтеров, логистов на юристов и HR – т.е. на профессии, которые прежде считались слабо автоматизируемыми

Наличие мобильного клиента для платформ стало одним и важных условий выбора ИТ-решений

Использование больших языковых моделей LLM

«Грабли» функциональной безопасности

Учитывать время года	Корректировка процессов
4-й квартал обычно сильно загружен, для CIO запускать новый проект внедрения сложных орг-техн изменений рискованно и крайне сложно	Счет ошибок: робот делает много разных запросов и если пересекается с живыми сотрудниками выдает ошибку. Если сотрудник склада перевел товар уже в резерв в тот же момент обращения робота, то робот может выдать ошибку. В момент принятия решения ИИ закончилась лицензия на ПО
Не типовой продукт и особенности его обслуживания, циклы жизни, развития, пересечение с другими проектами	**Равномерная загрузка робота**
Сам проект пересекался с достаточно сложным периодом компании – выходили новые формы документов, законодатели переписывали законы, 1С:УТ –условно типовая + несколько расширений, в которых множественные внешние доработки нужны были для учета изменений законов. Для работы робота пришлось поднимать несколько релизов 1С:УТ одновременно	Время работы робота больше времени работы живого сотрудника, в т.ч. Клиентов и поставщиков. Требуется оптимизировать загрузку поставщиков, установить приоритеты, каких поставщиков важнее обрабатывать.
Быстродействие и администрирование	**Анализ результативности**
Робота запустили на выделенном RDP АРМ, на котором работали еще несколько пользователей, настроено завершение сеанса робота по таймауту и отсутствию активности. Робот в таких условиях мог работать только если поддерживал сессию	Робот подтолкнул к необходимости анализировать труд сотрудников

Как внедрять ИИ в условиях противоречий законодательства и терминов ИБ?

Критическое мышление и системный подход

Комплексный подход к ЦТ
не обеспечивает функциональной безопасности орг-структурных изменений организаций
на стратегическом и операционном (тактическом) уровнях.

Требуются системный подход и правильная стратегия, учет динамики взаимодействия АИС контрагентов особенно в жизни критически важных объектов

Какой должна быть внятная Политика ФБ и ИБ цифровой экосистемы

Ты занимаешься цифровой трансформацией?

Если Вы не используете системный подход для ОБИ внешних цифровых информационных сервисов, безопасно интегрированных с цифровой КИС своего предприятия и безопасно не перевели все процессы обработки информации в цифровую форму сигналов, то вы занимаетесь чем угодно:
автоматизацией, информатизацией или даже роботизацией или чем-то еще,

но не ЦТ!!!

Что тут делать безопасникам? То же самое, когда они делали при внедрении облачных технологий

Выводы: над чем подумать безопасникам, чтобы не отставать

1. Мы непрерывно учимся делать больше с меньшими затратами.
2. Чем более развита технология, тем меньше ресурсов тратится на единицу производства. Смартфон заменяет десятки устройств
3. Ресурсный капкан: возможен ли бесконечный рост в конечной системе?
4. Следующий этап развития экосистем: не противоречие природе, а симбиоз технических систем с ней
5. Развитию технологий организации должна соответствовать эволюция культур подразделений. Современная культура потребления, противоречия законодательных актов и инициатив, а тем более навязываемая религиозная культура в противоречие ст. 14 п. 1 и п.2 Конституции России не соответствует развитию и внедрению цифровых экосистем
6. Внедрение ИИ и RPA способно привести к появлению новых форм цифрового разума и к резкому скачку производительности обработки и потребностей защиты информации

Путин В.В.:
"Да, церковь отделена от государства. И патриарх [Кирилл] не раз мне говорил: несмотря на это, у нас сложились уникальные отношения между церковью и государством. Что хотел бы в этой связи заметить: ну нельзя отделить церковь от общества и от человека. С этим я полностью согласен", - подчеркнул глава государства.

Мялковский Игорь Константинович

Задайте вопросы.
Но это еще не все!

VK: https://vk.com/id64927354