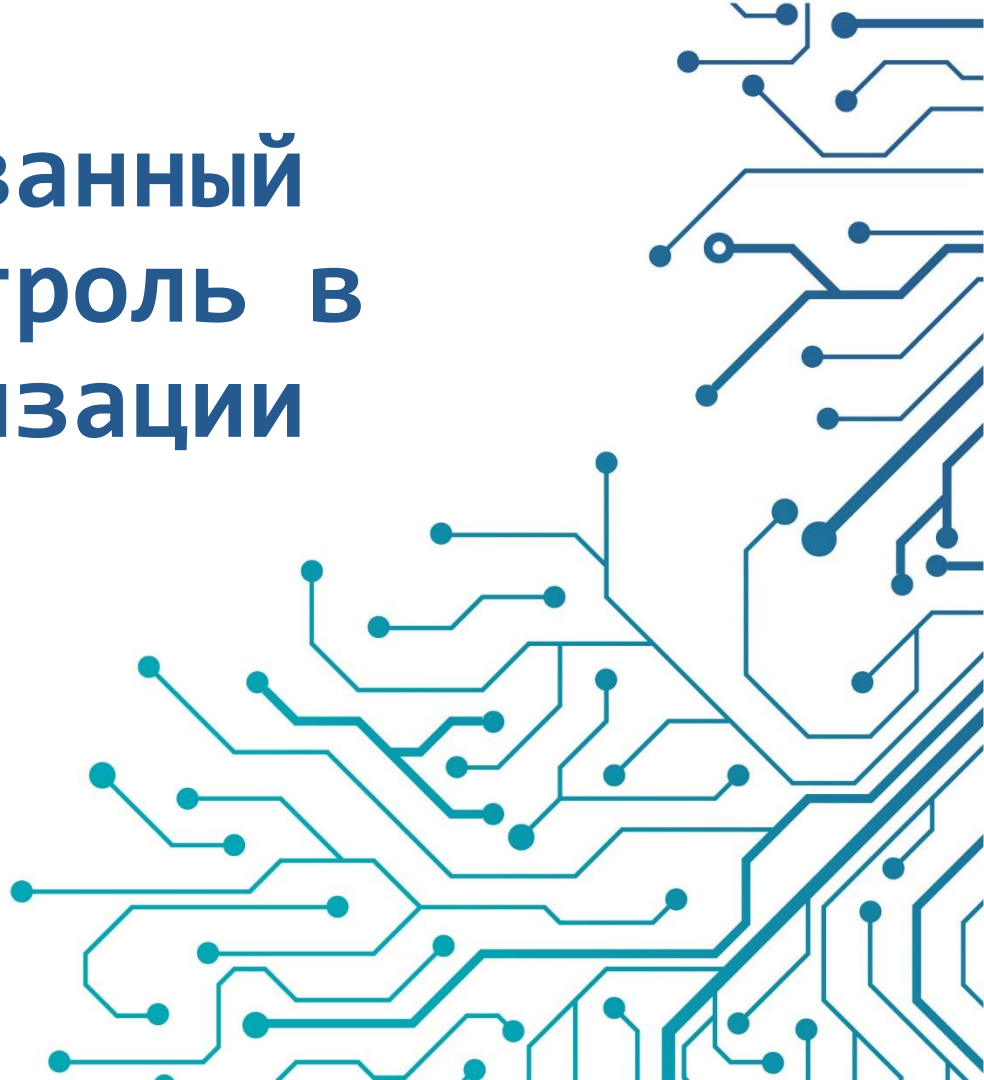
Риск-ориентированный внутренний контроль в сфере информатизации

Владимир Голованов
АО «ИнфоТеКС»



ИнфоТеКС в цифрах

infotecs

В **Топ-5**
компаний в сфере защиты информации в России

>10 млн
рабочих станций, защищенных продуктами ViPNet

В **Топ-5**
компаний по количеству патентов в области цифровых технологий

>30
лет работы на рынке ИБ

>60
Продуктов для защиты информации

12
офисов по всей стране

>1700
сотрудников

ИнфоТеКС на официальных площадках

infotecs

Профессиональные объединения и ассоциации

Минцифры России

Ассоциация документальной электросвязи

АЗИ

Торгово-промышленная палата Российской Федерации

Евро-азиатская ассоциация ЕВРАЗС

Производители товаров и услуг в области безопасности

Доверенная ПЛАТФОРМА

Ассоциация Разработчиков Программных Продуктов Отечественный софт

Национальная технологическая инициатива

Пространство возможного

ОПКИТ

Национальная и международная стандартизация

ТК 26

ТК 122

ТК 362

ISO

ISO/TC 307

Понятия «использование ИТ [в организации]» и «внутренний контроль»

Внутренний контроль и риски

(2013г.)

Внутренний контроль - процесс, направленный на получение достаточной уверенности в том, что экономический субъект обеспечивает:

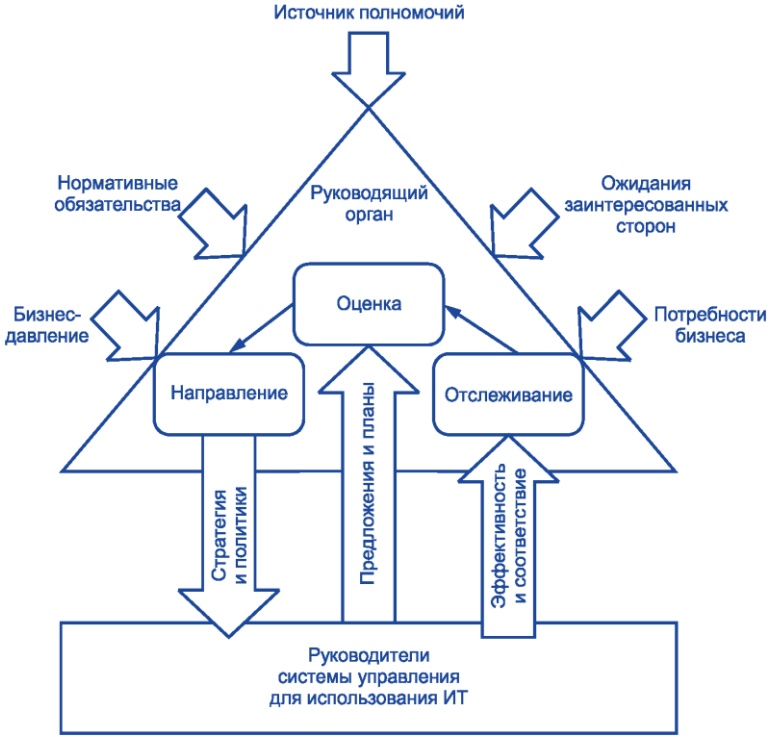
а) эффективность и результативность своей деятельности, в том числе достижение финансовых и операционных показателей, сохранность активов;

б) достоверность и своевременность бухгалтерской (финансовой) и иной отчетности;

в) соблюдение применимого законодательства, в том числе при совершении фактов хозяйственной жизни и ведении бухгалтерского учета.

Министерство финансов Российской Федерации, документ ПЗ-11/2013 "Организация и осуществление экономическим субъектом внутреннего контроля совершаемых фактов хозяйственной жизни, ведения бухгалтерского учета и составления бухгалтерской (финансовой) отчетности".

Корпоративное управление ИТ (ГОСТ Р ИСО/МЭК 38500-2017, ОЭСР)



Руководящие органы должны управлять ИТ посредством трех основных задач:

a) оценки текущего и будущего использования ИТ;

b) направления подготовки и внедрения стратегий и политик, чтобы гарантировать соответствие ИТ целям бизнеса;

c) отслеживания соответствия политикам и эффективности стратегии.

Использование ИТ [в организации] (ГОСТ Р ИСО/МЭК 38500-2017)

Использование ИТ (use of IT): Планирование, проектирование, разработка, развертывание, эксплуатация, управление и применение ИТ для выполнения задач бизнеса и создания ценности для организации.

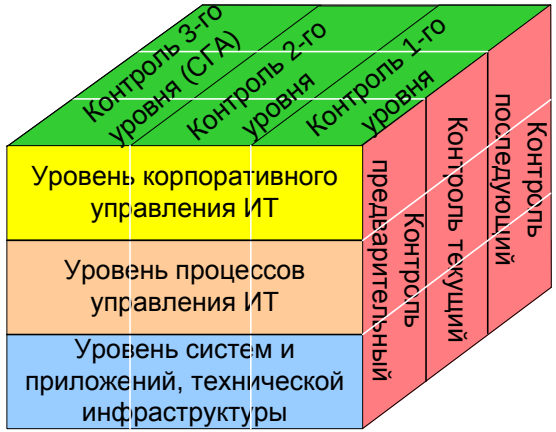
Примечания:

1. Использование ИТ подразумевает как спрос в области ИТ, так и предложение в этой области.

2. Использование ИТ относится как к текущему, так и будущему использованию.

Внутренний контроль и управление ИТ

Вариант реализации. Управление ИТ в организации и уровни и виды внутреннего контроля



Адаптация модели COSO к специфике конкретной организации

Основание для **регламентации и стандартизации** внутренних процедур

Основание для **совершенствование организационной инфраструктуры** для обеспечения в решении требуемых задач (с учетом содержания задач по управлению ИТ)

Основа для будущих решений по **инструментальной поддержке**

Корпоративное управление ИТ, процессы жизненного цикла ИТ в организации

- ✓ **Политики**: роли и ответственность, права и обязанности в организации;
- ✓ **Проекты** в области информатизации;
- ✓ Обеспечение **эксплуатации** и развития ИС, ИТС, ИТКС, АС …

Проекты в области информатизации. Соответствующие стандарты и практики для реализации и контроля ИТ-проектов

Здесь оптимальными являются практики по управлению проектами с учетом «**предпочтений**» персонала

PMBoK

(Project Management Body Of Knowledge) в версии либо от Института по управлению проектами (PMI), либо ИСО, есть ГОСТированные фрагменты

PRINCE2

(Projects In Controlled Environments, версия 2) опубликовано Правительственным коммерческим управлением Великобритании

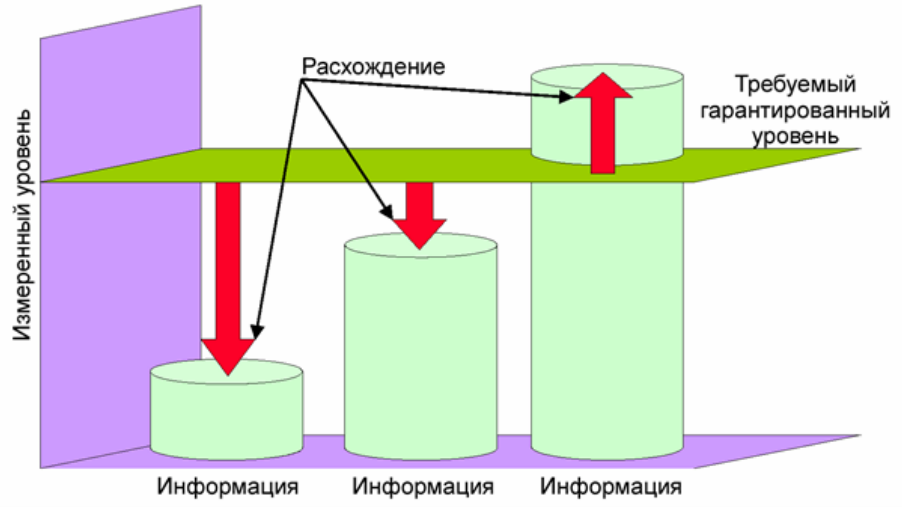
ISACA Serving IT Governance Professionals

COBIT

ITIL

Не только проекты, но и эксплуатация

ИТ-проекты и управление рисками. Пороги и принятие решений



- ✓ Риски процессов управления проектами
- ✓ Риски при применении «продукта» ИТ-проекта

ИТ-проекты и управление рисками. Риски «продукта» проекта. Моделирование угроз

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден
ФСТЭК России
5 февраля 2021 г.

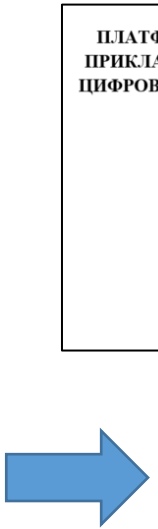
МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

1. Общие положения

1.1. Настоящая Методика оценки угроз безопасности информации (далее - Методика) разработана в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085.

1.2. Методика определяет порядок и содержание работ по определению угроз безопасности информации, реализация (возникновение) которых возможна в информационных системах, автоматизированных системах управления, информационно-телекоммуникационных сетях, информационно-телекоммуникационных инфраструктурах центров обработки данных и облачных инфраструктурах (далее - системы и сети), а также по разработке моделей угроз безопасности информации систем и сетей.



ПЛАТФОРМА ДЛЯ СОЗДАНИЯ, РАЗВИТИЯ И ЭКСПЛУАТАЦИИ ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ЕДИНОЙ ЦИФРОВОЙ ПЛАТФОРМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ «ГОСТЕХ»

ТИПОВЫЕ МОДЕЛИ УГРОЗ ГИС, СОЗДАВАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КОМПОНЕНТ ПЛАТФОРМЫ

ТОМ 3

Страниц с 935 по 1366
на 434 листах

ОЗДАНИЯ, РАЗВИТИЯ И ЭКСПЛУАТАЦИИ
РАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ЕДИНОЙ
МЫ РОССИЙСКОЙ ФЕДЕРАЦИИ «ГОСТЕХ»

МОДЕЛИ УГРОЗ ПЛАТФОРМЫ,
ЮЙ НА БАЗЕ ВЫЧИСЛИТЕЛЬНОЙ
НФРАСТРУКТУРЫ ЦОД

ТОМ 4

Страниц с 935 по 1307
на 375 листах

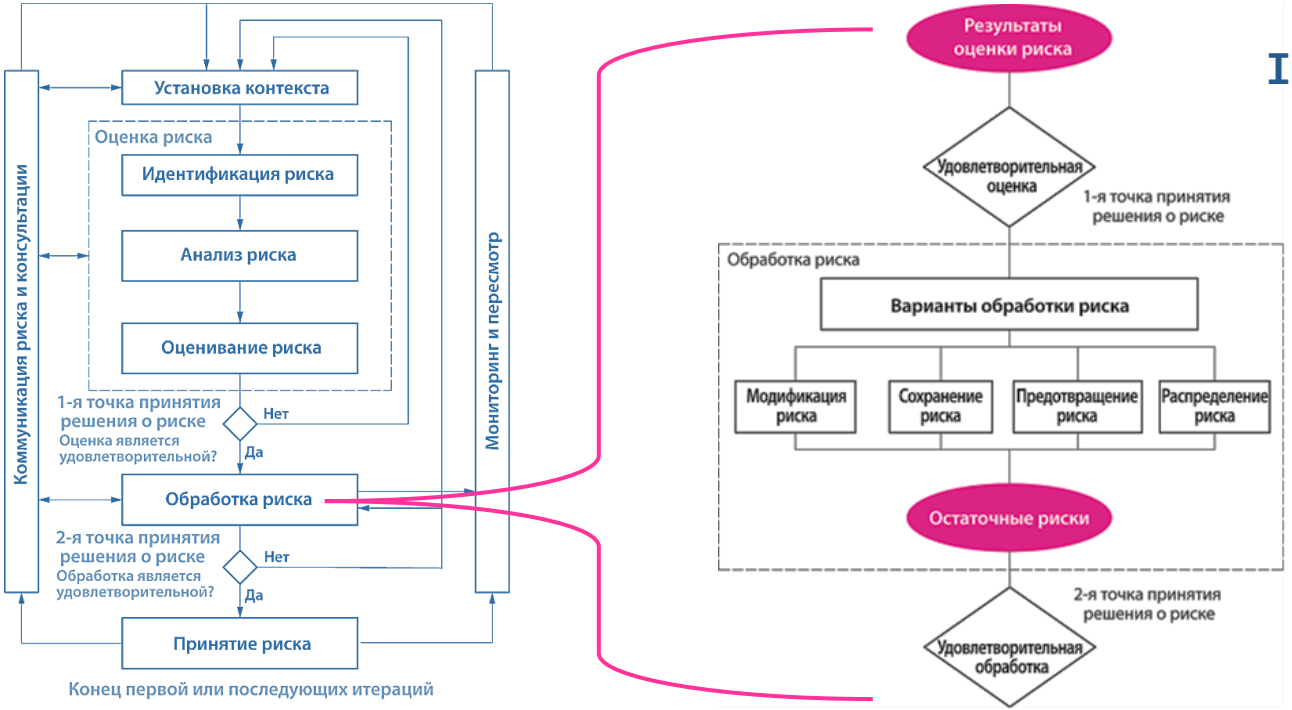
ПЛАТФОРМА ДЛЯ СОЗДАНИЯ, РАЗВИТИЯ И ЭКСПЛУАТАЦИИ ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ЕДИНОЙ ЦИФРОВОЙ ПЛАТФОРМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ «ГОСТЕХ»

ТИПОВЫЕ МОДЕЛИ УГРОЗ ПЛАТФОРМЫ, РАЗМЕЩАЕМОЙ НА БАЗЕ ВЫЧИСЛИТЕЛЬНОЙ ИНФРАСТРУКТУРЫ ЦОД

ТОМ 5

Страниц с 1308 по 1709
на 404 листах

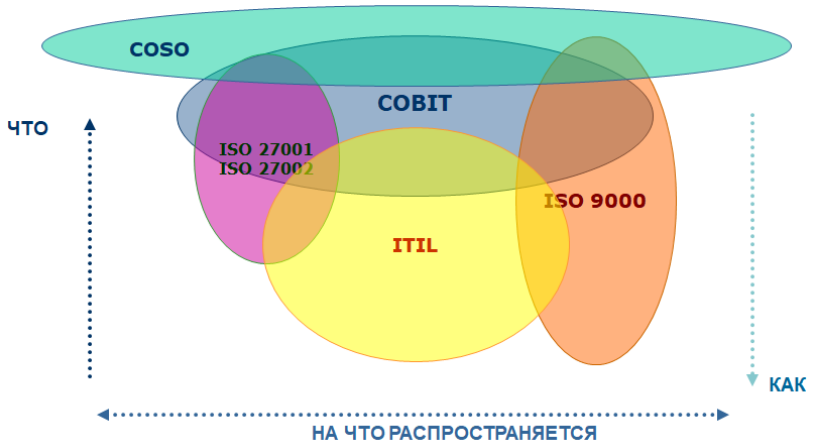
ИТ-проекты и управление рисками. Риски продукта проекта. Моделирование угроз



ISO 27005

ИТ-проекты и управление рисками. Риски продукта проекта. Меры для контроля рисков. Источники

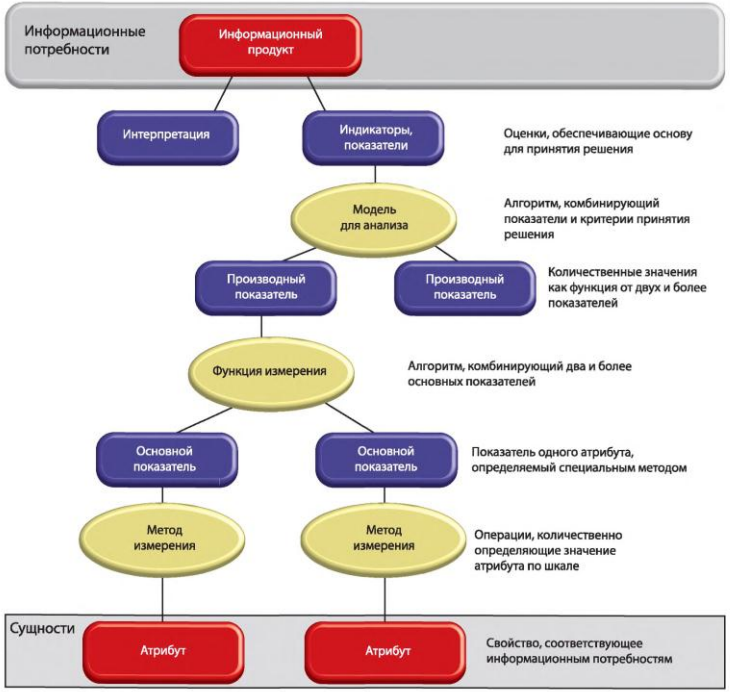
Традиционная иллюстрация



- ✓ Законодательство
- ✓ Нормативные акты регуляторов
- ✓ Требования национальных стандартов
- ✓ Требования международных стандартов
- ✓ Требования отраслевых и профессиональных стандартов

Проектирование показателей оценки

Оценка процесса. Показатели оценки эффективности



Информационная модель измерения в [ИТ] - это структура, связывающая информационные потребности с соответствующими сущностями и атрибутами. К сущностям относятся процессы, продукты, проекты и ресурсы.

Информационная модель измерения в [ИТ] описывает, как соответствующие атрибуты определяются количественно и преобразуются в показатели, которые обеспечивают основу для принятия решений.

ISO/IEC/IEEE 15939 Systems and software engineering. Measurement process (ГОСТ Р 58606-2019)

Контроль процессов. С участием персонала. Проектные и системные риски. Шаблон

Возможные проблемы/риски на этапе осуществления проекта

Возможные проблемы/риски после введения системы в эксплуатацию

Риск	Уровень риска	Предполагаемые системы контроля	Подход при аудите
Проектные риски и системы контроля			
.....	.	•	• .....
.....	.	•	• .....
.....	.	•	• .....
Системные риски и системы контроля			
.....	.	•.....	•.....
.....	.	•	• .....

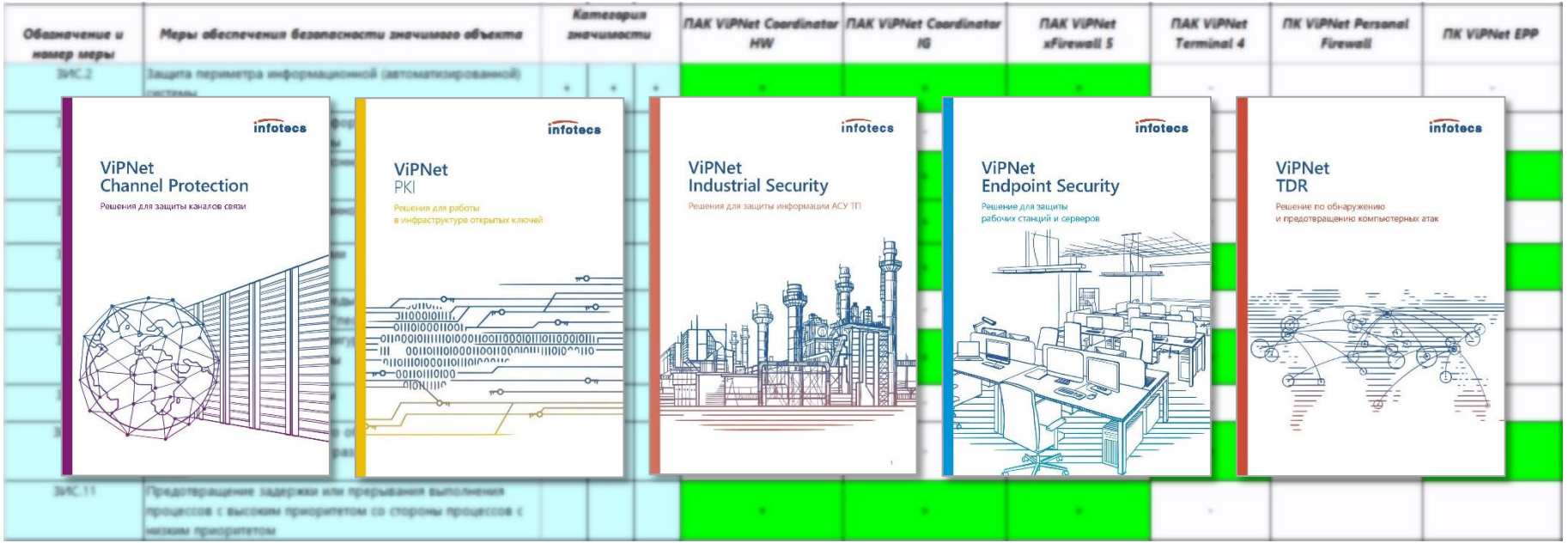
Контроль процессов. С участием персонала. Контроль доступа / права доступа. Пример

Риск	Уро-вень риска	Предполагаемые меры контроля	Методики проверки
Контроль доступа к сети			
.....	.	•	• .....
В результате несанкционированного доступа к **сетевым услугам** могут быть нарушены конфиденциальность, достоверность и сохранность данных обрабатываемых системой	Н	Из ГОСТ Р ИСО/МЭК 27002: • Политика использования сетевых услуг (11.4.1) • Подтверждение личности пользователя ри внешнем подключении (11.4.2) • Идентификация аппаратуры в сетях (11.4.3) • Удаленная диагностика и защита порта конфигурации (11.4.4) • Сегментация сети (11.4.5) • Контроль подключения к сети (11.4.6) • Контроль маршрутизации в сети (11.4.7)	• Интервью • Анализ документации • Соблюдение регламентов • Испытания в рабочем режиме
.....	.	•	• .....
.....	.	•	• .....

infotecs

Средства контроля ИТ-рисков

Универсальные и специализированные средства и технологии защиты информации (средства контроля ИТ-рисков)



infotecs

Технологии защиты нового поколения

Интеллектуальная система выявления компьютерных атак: ViPNet TIAS

В реестре российского ПО появился первый продукт с признаком искусственного интеллекта

Система интеллектуального анализа событий **ViPNet TIAS стала первым продуктом в Едином реестре российских программ** для электронных вычислительных машин и баз данных, который получил специальный признак, указывающий на **отнесение программного обеспечения к сфере Искусственного Интеллекта**

Защита информации на новом уровне. Внедрение квантовых технологий

А.А. Чапчаев, Генеральный директор АО «ИнфоТеКС»

«...ИнфоТеКС занимается квантовыми коммуникациями **с 2017 года**, именно тогда стартовал совместный проект с Центром квантовых технологий физического факультета МГУ имени М.В. Ломоносова.

...

Что касается практического применения ККС ВРК **ViPNet QTS Lite**, сейчас мы сфокусированы на двух больших проектах. **Первый** – это производство оборудования для одной из веток **магистральной квантовой сети РЖД**. Второй – реализация проекта территориальной квантовой сети для Газпрома....»

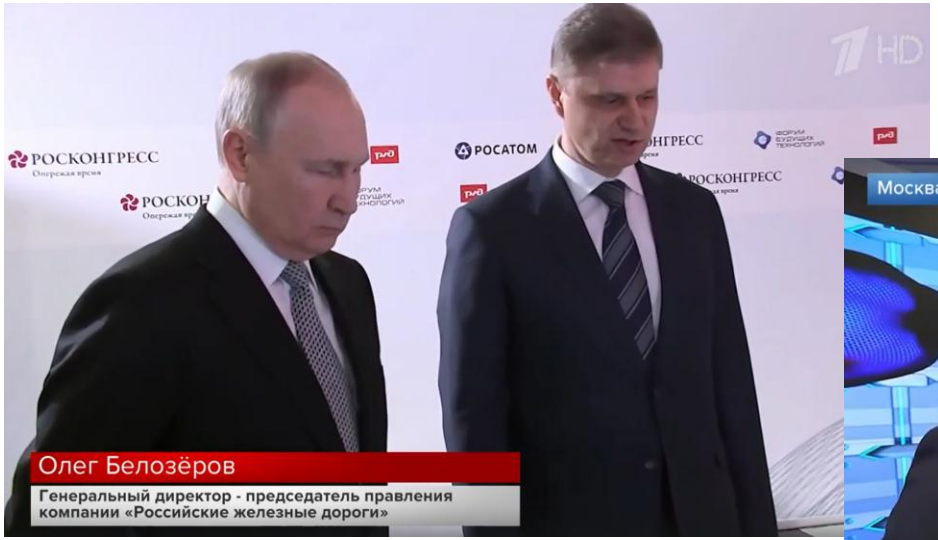
Журнал «Риск - менеджмент. Практика», новость от 20.07.2023, «ИнфоТеКС» представила проекты в области квантовых коммуникаций на Форуме будущих технологий

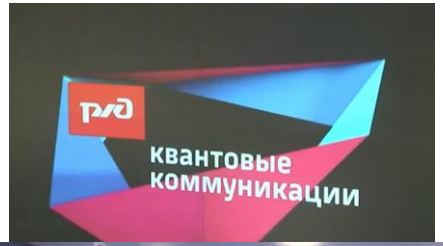
09-14 июля 2023. Москва
Форум будущих технологий

Компания ИнфоТеКС приняла участие в Форуме будущих технологий – одном из самых престижных научно-практических мероприятий в сфере квантовых технологий.

Пленарное заседание Форума будущих технологий с участием Президента РФ В.В. Путина. Надежда Борщевская, ЦКТ МГУ имени М.В.Ломоносова, отметила АО ИнфоТеКС как индустриального партнера.

09-14 июля 2023. Москва
Форум будущих технологий





Совместные проекты АО РЖД и АО «ИнфоТеКС». Стандартизация новых технологий для обеспечения широкого повсеместного применения

ТЕХНИЧЕСКИЙ КОМИТЕТ ПО СТАНДАРТИЗАЦИИ

«КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

МР 26.4.003–2023

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

Ин

Крипто

Кл

многоарен

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Защищенный протокол взаимодействия квантово-криптографической аппаратуры выработки и распределения ключей и средства криптографической защиты информации

Рекомендации по стандартизации «Информационная технология. Криптографическая защита информации. Защищенный протокол взаимодействия квантово-криптографической аппаратуры выработки и распределения ключей и средства криптографической защиты информации»

Методические рекомендации по стандартизации ТК26 «Информационная технология. Криптографическая защита информации. Ключевая система сети шифрованной связи с использованием ККС ВРК с сетевой топологией «звезда»

Методические рекомендации по стандартизации ТК26 «Информационная технология. Криптографическая защита информации Термины и определения в области квантовых криптографических систем выработки и распределения ключей»

МР 26.4.003-2023 «Информационная технология. Криптографическая защита информации. Ключевая система полносвязной многоарендаторной сети шифрованной связи на базе ККС ВРК с ДПУ»

Спасибо за внимание!

Vladimir.Golovanov@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

t.me/infotecs_news

rutube.ru/channel/24686363