ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

Институт кибербезопасности
и защиты информации

Интенционно-ориентированные сети: угрозы безопасности и возможные подходы к защите

Исследование выполнено в рамках стипендии Президента РФ молодым ученым и аспирантам СП-1932.2019.5.

Попова Е.А., Лаврова Д.С.

2021

Интенционно-ориентированные сети (Intent-Based Networking, IBN)

Намерение – высокоуровневая цель, сформулированная без технических подробностей ее достижения

Намерение	Реализация намерения
Изменить права так, чтобы сотрудники отдела X имели доступ к ресурсам отдела Y	Переопределить ACL-списки в двух или более отделах, обновить конфигурацию сети, проверить отсутствие конфликтов
В 10 утра создать видеоконференцию с заказчиками	Создать канал для передачи HD-видео, менеджмент учетных записей, постоянное обеспечение QoS и безопасности соединения, завершение подключения
Развернуть многоуровневое приложение для обеспечения безопасности	Выделение нескольких сетей и подсетей, настройка ACL-списков и правил МЭ, передача данных маршрутизации

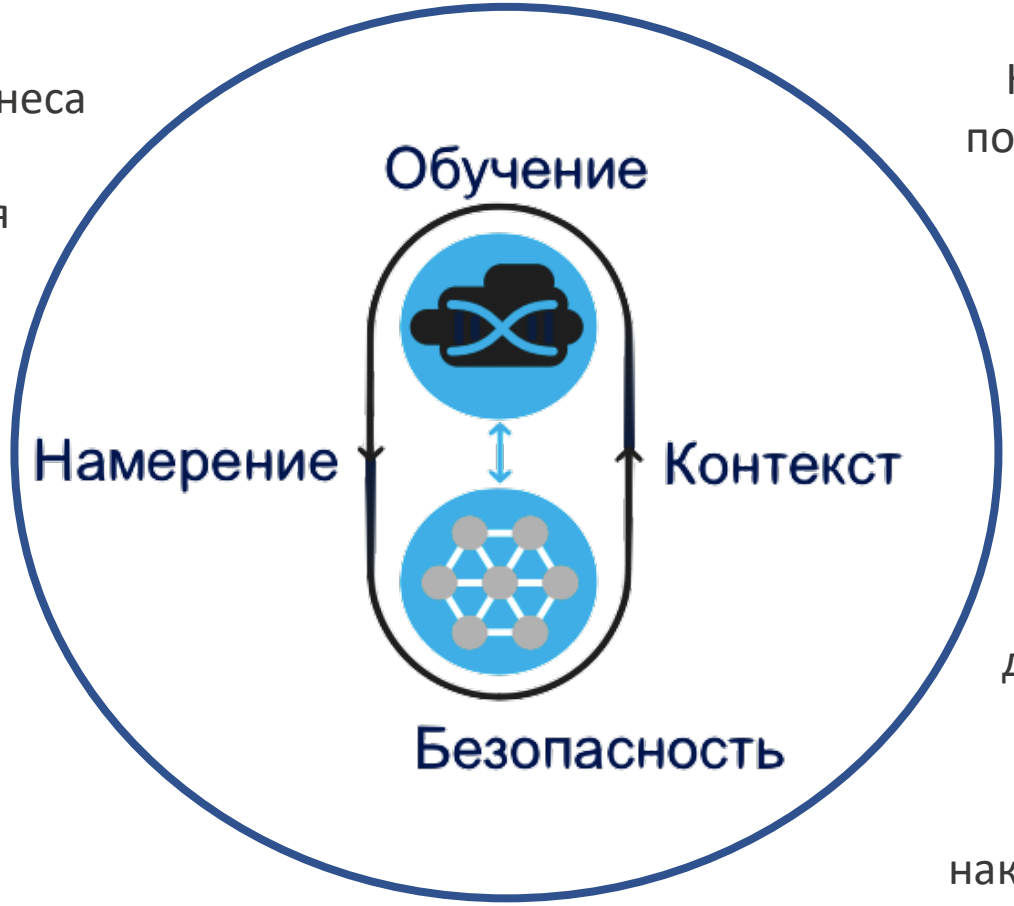
Сравнение концепции IBN с традиционными сетями

	Традиционная сеть	IBN
Архитектура	• управление на уровне устройств; • однонаправленная конфигурация; • непрограммируемые устройства.	• централизованное управление всей сетью; • автоматическая конфигурация замкнутого цикла и контроль; • программируемые физические и виртуальные инфраструктуры.
Трансляция	• интерпретация и перевод, требующие специальных знаний от администратора.	• использование системных функций трансляции намерения.
Поддержка политик	• политики реализуются через команды устройств.	• политики на основе намерений с использованием моделей.
Активация	• через сценарии, на уровне устройств.	• автоматизированная, в масштабе всей сети.
Контроль	• ручной.	• автоматизированный, с помощью AI/ML.

Преимущества и недостатки IBN

Преимущества:

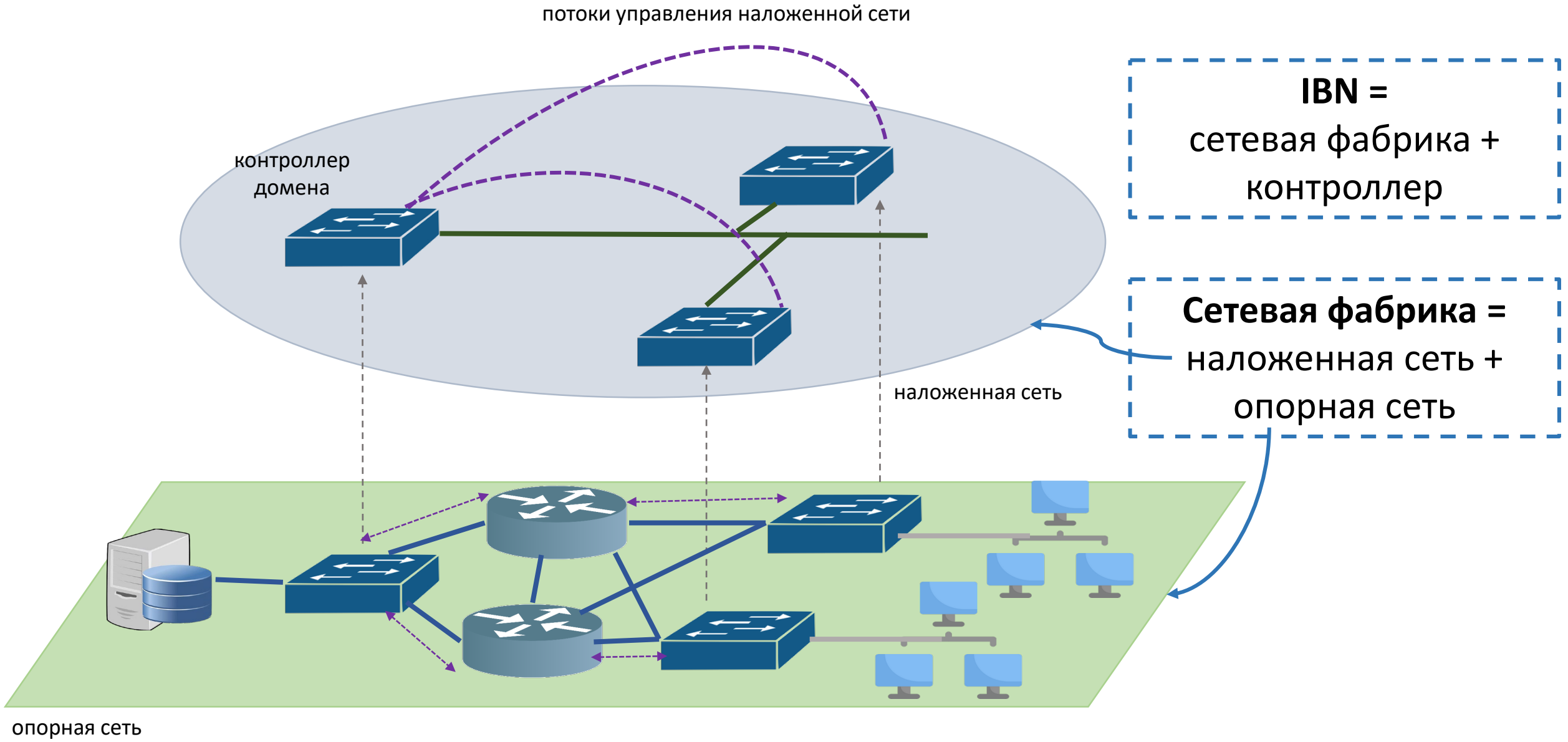
- Увеличение возможностей бизнеса
- Повышенная эксплуатационная активность
- Согласованность работы сети с бизнес-целями
- Снижение операционных расходов
- Снижение рисков
- Улучшенное обеспечение безопасности



Недостатки:

- Недостаточная изученность подобных сетей не позволяет говорить об отсутствии прежних или новых угроз сетевой инфраструктуре
- Дороговизна и сложность проектирования и развертывания сети
- Наличие строгих правил для проверки корректности настройки и работы сети
- Использование AI/ML накладывает дополнительные ресурсные затраты и угрозы

Реализация IBN в реальных сетевых инфраструктурах

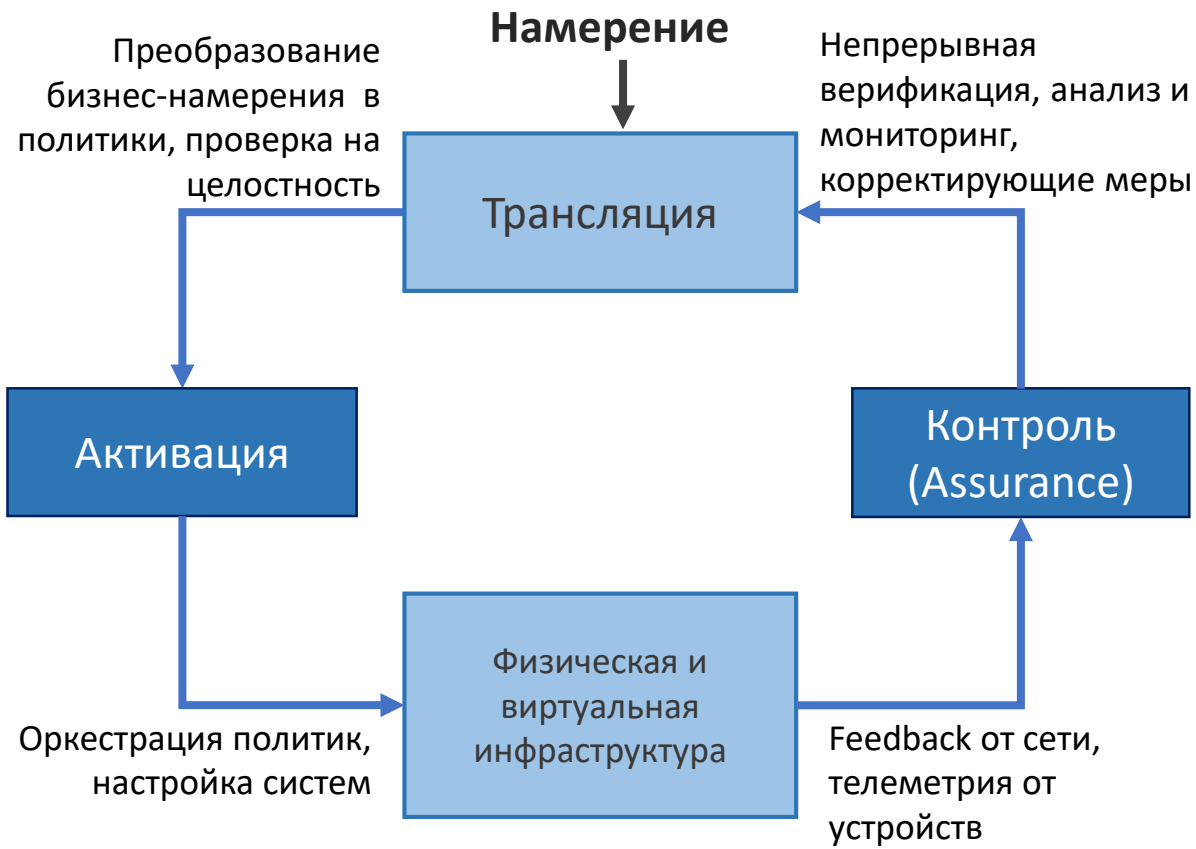


IBN =
сетевая фабрика +
контроллер

Сетевая фабрика =
наложенная сеть +
опорная сеть

Функционал IBN

Полнофункциональная интенционно-ориентированная сеть должна выполнять следующие основные функции:

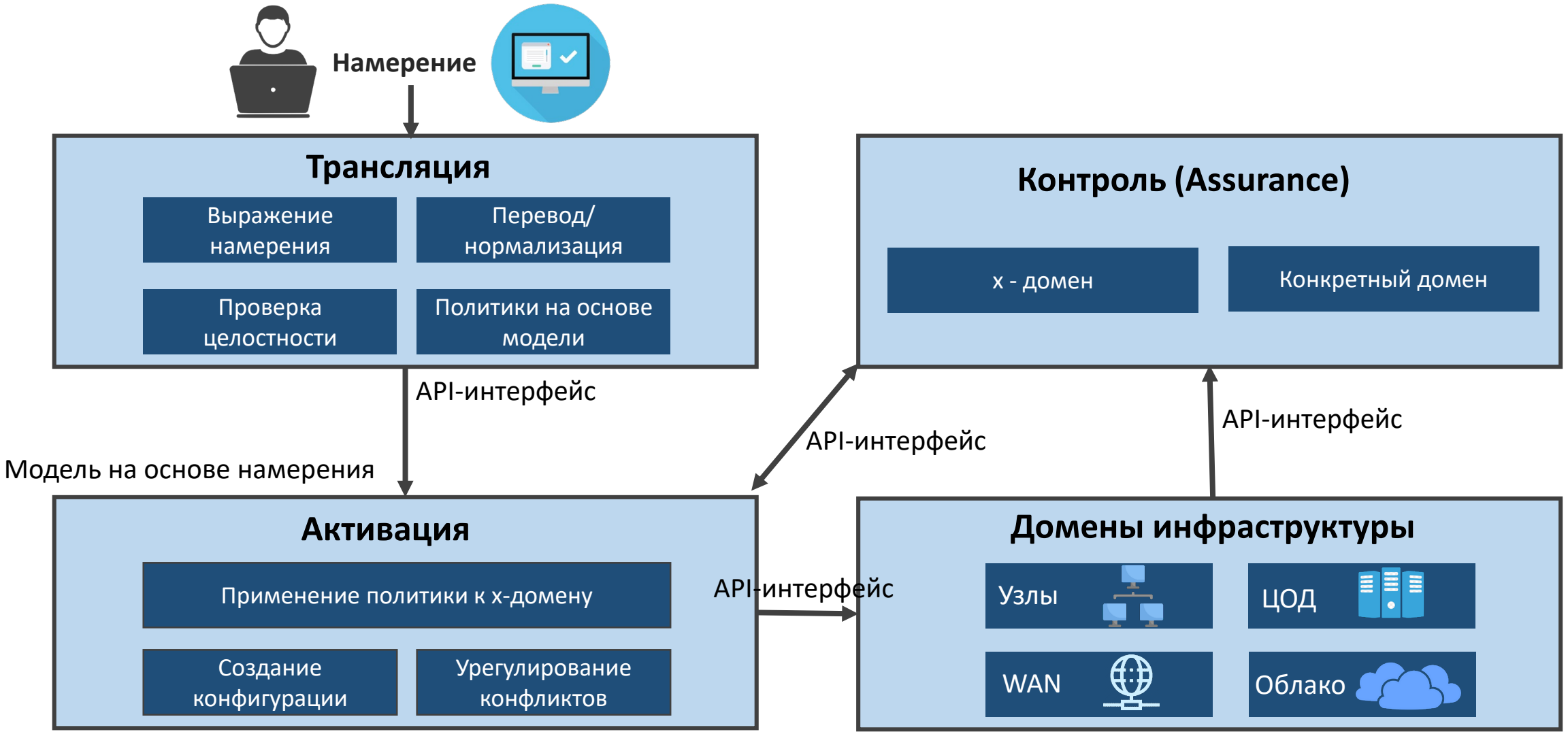


Трансляция включает две основные функции:
- интерфейс для задания бизнес-намерения администратором;
- преобразование полученных намерений в политики (MBP).

Активация. Задача активации — внедрить политики MBP, заданные на этапе трансляции, во все области сети, которых они касаются.

Контроль и непрерывная верификация. Предполагается, что IBN должна самостоятельно отслеживать корректность внедренных политик, а также уметь перенастраивать сетевую конфигурацию при обнаружении некорректных настроек.

Модель IBN


Намерение
Трансляция
Выражение намерения
Перевод/ нормализация
Проверка целостности
Политики на основе модели
API-интерфейс
Модель на основе намерения
Активация
Применение политики к х-домену
Создание конфигурации
Урегулирование конфликтов
API-интерфейс
Контроль (Assurance)
х - домен
Конкретный домен
API-интерфейс
API-интерфейс
Домены инфраструктуры
Узлы
ЦОД
WAN
Облако

Проблемы безопасности IBN (1)

Проблема согласования политик

Намерение 1: Разрешить всем изменение конфигурации маршрутизатора R1

Намерение 2: запретить Иванову Ивану изменять конфигурацию маршрутизатора R1

В маршрутизаторах Cisco проверка сетевого пакета на соответствие ACL осуществляется по порядку, начиная с первого правила.
Если пакет попадает под условия первого ACL, то дальше правила не просматриваются.

Таким образом, пакет попадет под правило «Разрешить всем», а значит, что даже Иванов Иван сможет изменять конфигурацию R1.

Проблема некорректной трансляции намерений в политики

Намерение: предоставить Иванову Ивану доступ ко всем бухгалтерским отчетам

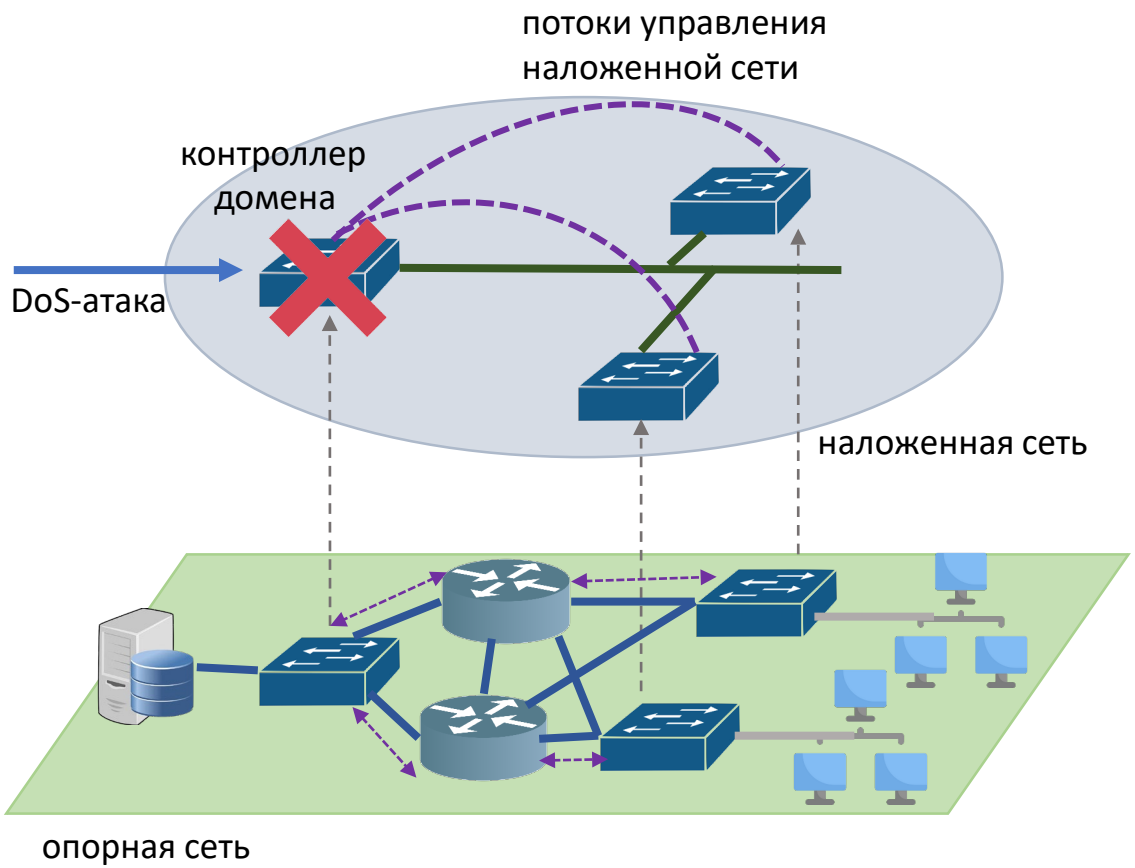
Политика:

Grant to Иванов Иван Петрович,
Иванов Иван Семенович
access READ to Бухгалтерия_отчеты

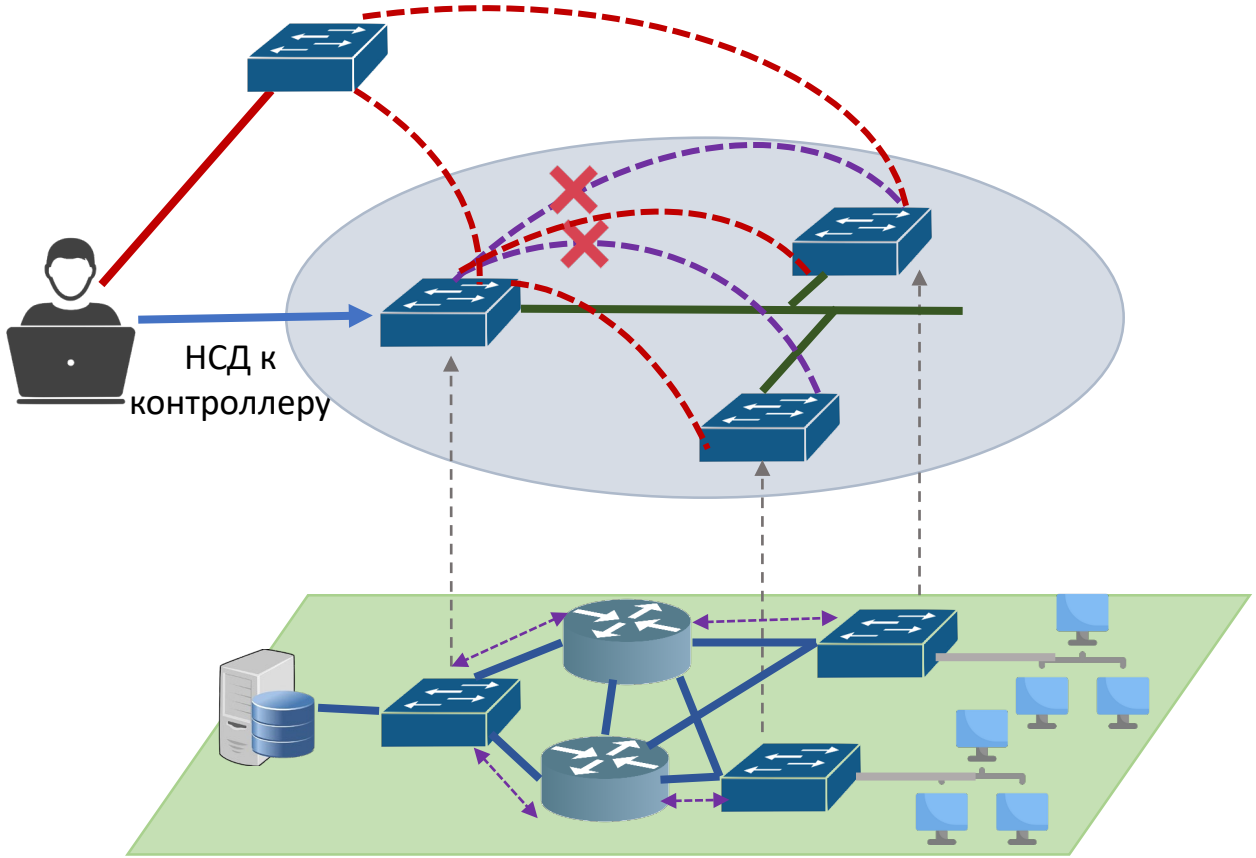
Активация

Проблемы безопасности IBN (2)

Проблема уязвимости к DoS-атакам единой точки отказа



Проблема несанкционированного воздействия на контроллер



Проблемы безопасности IBN (3)

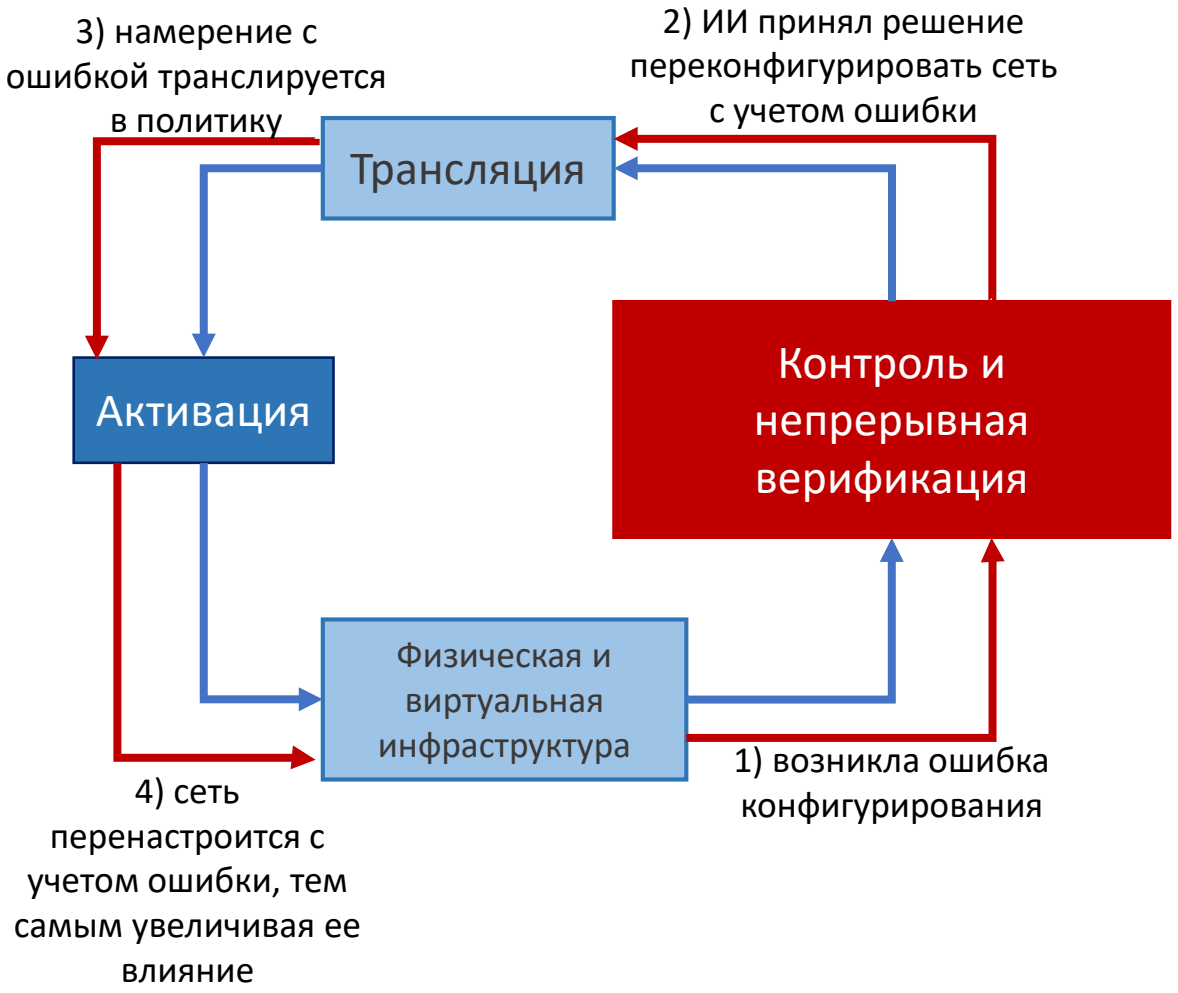
Проблемы, связанные с управлением доступом

Приложение для видеосвязи:
необходимо провести видеоконференцию в четверг в 10 утра.

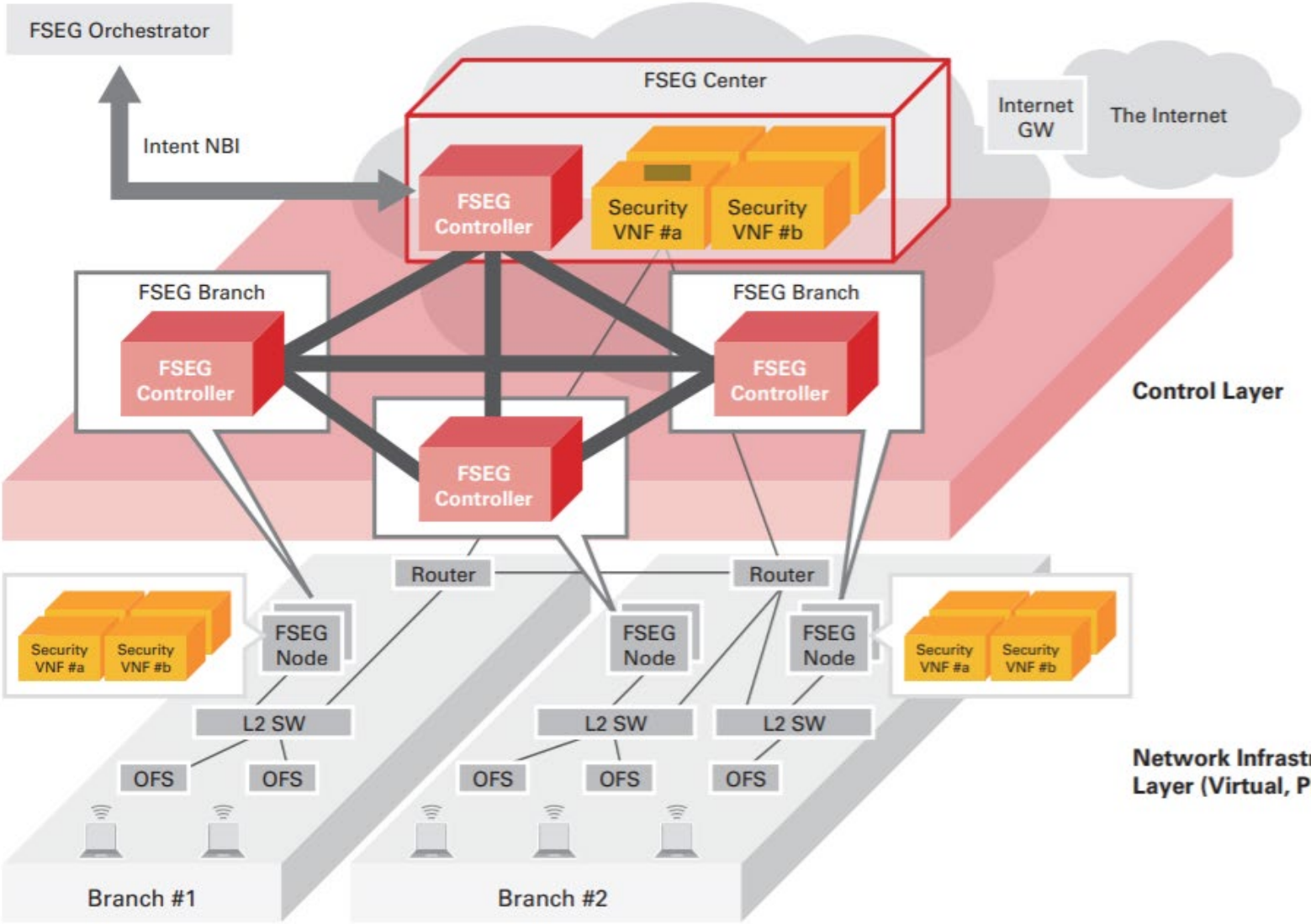
- Создать вебинарную комнату
- Пригласить пользователей
- Добавить запись в календарь событий компании

Если администратор не предоставил доступ приложению для видеосвязи к календарю, то напоминание о конференции не дойдет до участников, что приведет к возможному срыву бизнес-мероприятия

Проблемы безопасности, характерные для технологии искусственного интеллекта (ИИ).



Подходы к решению проблем безопасности IBN (1)



Решение, применяемое в IIJ Group, базируется на создании наложенной топологии FSEG.

FSEG-контроллеры выполняют 3 функции:

- аутентификацию пользователей и устройств;
- контроль над политиками;
- контроль над FSEG-узлами.

Подходы к решению проблем безопасности IBN (2): развитие наработок ИКиЗИ СПбПУ

Обеспечение киберустойчивости IBN-сетей на основе саморегуляции

Введение дополнительных функциональных элементов в структуру IBN-сетей, способных осуществлять:

- дублирование некоторых функций контроллера;
- принятие решения в случае возникновения конфликта трансляции намерений;
- урегулирование конфликтов при активации политик.

Раннее предупреждение угроз ИБ на основе технологий ИИ и предиктивной аналитики

- Обнаружение и предсказание ошибок при трансляции намерений с использованием теории графов и графовых нейронных сетей;
- Предсказание конфликтов при активации политик на основе обработки текстовых данных.

Заключение

- Сетевая концепция IBN может обеспечить более гибкое функционирование сетевых технологий.
- Построение сетевых инфраструктур в парадигме IBN ведет к появлению новых угроз безопасности.
- Компании-разработчики сетевых технологий в настоящий момент не предоставляют способов защиты от озвученных в докладе проблем.