



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

infotecs®

||| CENTER

КАК МОЖНО СЭКОНОМИТЬ бюджеты и сделать правильно?

Дмитрий КИБЕНКО
Центр

Алексей АЛЕКСЕЕВ
ИнфоТеКС


VIPNet
Virtual Private Network

Вопрос: КАК можно сэкономить бюджеты и сделать правильно?

Ответ 1: ВЫБРАТЬ правильного поставщик.

Критерий выбора поставщика	Удельный вес критерия	Оценка поставщика по выбранным критериям	Произведение удельного веса критерия на оценку
1. Надежность поставки	0,30		
2. Качество товара	0,25		
3. Цена товара	0,2		
4. Удаленность поставщика от потребителя	0,15		
5. Финансовое состояние поставщика	0,10		
Итого:	1,00		

QR код для интерактивного опроса



1. Надежность поставки

Коммерческий партнер, г. Казань
ГК Центр

The logo for 'CENTER' is positioned at the bottom of the dark blue text box. It consists of a square icon made of a 3x3 grid of small squares to the left of the word 'CENTER' in a bold, white, uppercase sans-serif font.



21 ГОД УСПЕШНОЙ РАБОТЫ



450+
проектов
по всей
России



Автоматизация бизнес-процессов

Разрабатываем и внедряем информационные системы для организаций



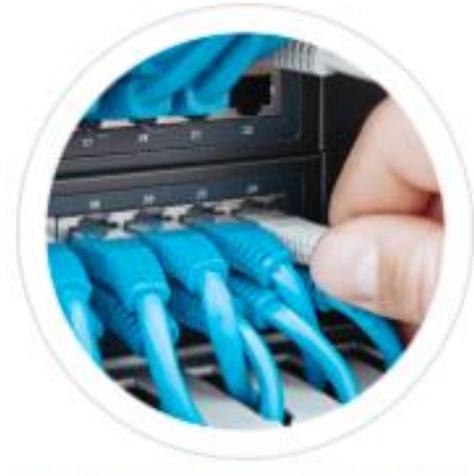
Системы информационной безопасности

Аудит, разработка, внедрение



Облака

Готовое корпоративное облако со всеми компонентами



Мультисервисные и вычислительные сети

Создаём локально-вычислительные и территориально распределённые сети

9+

ОФИСОВ ПО СТРАНЕ

1000+

СОТРУДНИКОВ

28 лет

НА РЫНКЕ ИБ

50+

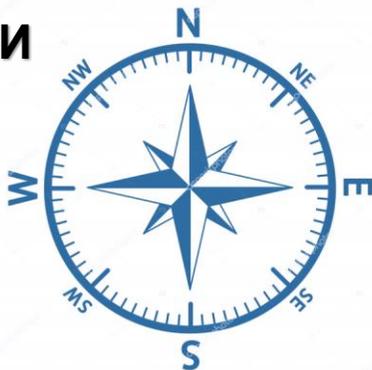
**ПРОДУКТОВ ДЛЯ
ЗАЩИТЫ
ИНФОРМАЦИИ**

>1млн

**РАБОЧИХ СТАНЦИЙ,
ЗАЩИЩЕННЫХ
ПРОДУКТАМИ
VIPNET**

Топ-5

**РОССИЙСКИХ
КОМПАНИЙ В
СФЕРЕ ЗАЩИТЫ
ИНФОРМАЦИИ**



infotecs



**ЧАПЧАЕВ
АНДРЕЙ
АНАТОЛЬЕВИЧ**

Уч.
Ц-тр

ОАО
ИнфоТеКС

ЗАО
ПМ

Исп.
Лаб.

ИнфоТеКС
Интернет
траст



**Миссия компании ИнфоТеКС –
создание защищенной
информационной среды для
бизнеса и повседневной жизни**





Подключение Республики
Тыва к системе ГосСОПКА

[ЧИТАТЬ ДАЛЕЕ](#)



ИнфоТеКС создал систему
защиты для объектов XXIX
Всемирной зимней
Универсиады 2019

[ЧИТАТЬ ДАЛЕЕ](#)



Компания ИнфоТеКС
разработала облачное
решение для
идентификации и
обслуживания пассажиров

[ЧИТАТЬ ДАЛЕЕ](#)



ViPNet для защиты канала
связи Тульского оружейного
завода

[ЧИТАТЬ ДАЛЕЕ](#)



«Кубаньэнерго» под
защитой СЗИ ИнфоТеКС



РАДИОЛОГИЯ МОСКВЫ
ДИАГНОСТИКА БУДУЩЕГО

ИнфоТеКС обеспечил
защиту каналов связи
Единого Радиологического
Информационного Сервиса



Компания Мед-Рей
использовала технологию
ViPNet для создания VPN-
сети



ViPNet защитил сеть
передачи данных
здравоохранения
Саратовской области

Первое в России подключение субъекта РФ – Республики Тыва – к системе ГосСОПКА



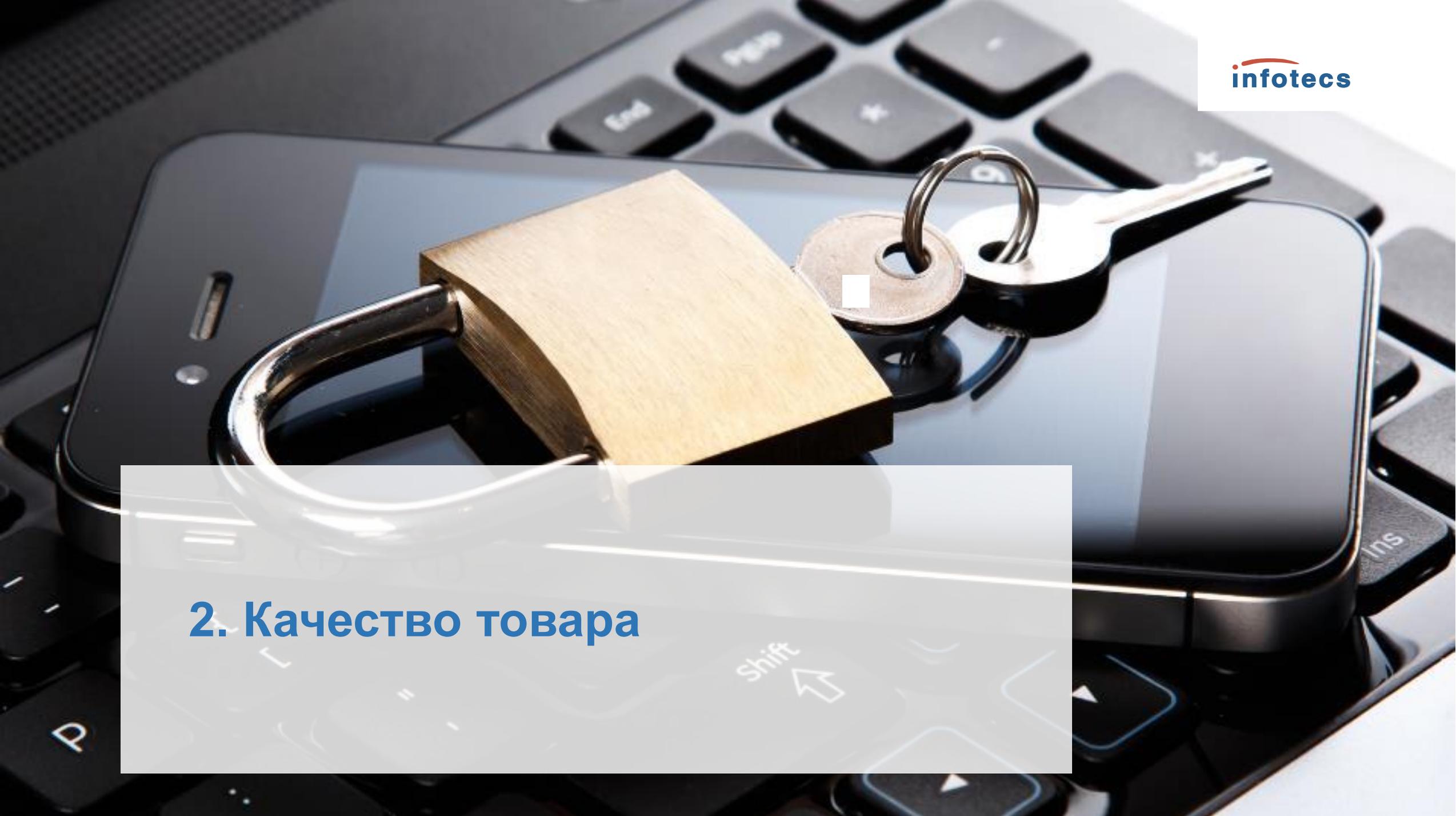
Для реализации задачи заказчиком было произведено объединение сетей министерств и ведомств Тывы в единую сеть передачи данных с одной точкой подключения к сетям международного обмена. Трафик с границы сети зеркалируется и анализируется сенсором средства обнаружения вторжений (СОВ) *ViPNet IDS NS. Для сбора и анализа информации используется *ПАК ViPNet TIAS.

Информация об инцидентах анализируется в Центре ГосСОПКА компании «Перспективный мониторинг» (входит в ГК ИнфоТеКС) и передается в систему ГосСОПКА через техническую инфраструктуру НКЦКИ.

<https://infotecs.ru/about/success-story/gossopka-tyva.html>

МАРШРУТНАЯ КАРТА



The background image shows a black smartphone lying on a laptop keyboard. A brass padlock is attached to the phone's screen, and a set of keys is resting on the phone's surface. The scene is lit from the side, creating strong highlights and shadows.

2. Качество товара

Лицензии

[ИСТОРИЯ](#) [ПРЕСС-ЦЕНТР](#) [ИСТОРИИ УСПЕХА](#) [ЛИЦЕНЗИИ](#) [ПАТЕНТЫ](#) [НАГРАДЫ](#) [МАТЕРИАЛЫ](#) [РАБОТА](#) [ВАКАНСИИ](#) [АКЦИОНЕРАМ](#) [АКАДЕМИИ](#)

Деятельность компании ИнфоТеКС на российском рынке информационной безопасности и информационных технологий осуществляется на основании лицензий ФСБ России, ФСТЭК России, Министерства обороны РФ и соответствует требованиям ГОСТ ИСО 9001-2015 (ISO 9001:2015)

ВСЕ

ФСБ РОССИИ

МИНОБОРОНЫ РОССИИ

ФСТЭК РОССИИ

МПЦ ЭКСПЕРТИЗА

МПЦ ЭКСПЕРТИЗА



Сертификат соответствия требованиям ГОСТ Р ИСО 9001-2015 (ISO 9001:2015)

Настоящий сертификат выдан компании ИнфоТеКС и удостоверяет, что система менеджмента качества применительно к выполнению работ по проектированию, разработке, производству и технической поддержке программных, программно-аппаратных и аппаратных средств защиты информации, а также оказанию услуг по проектированию и внедрению систем информационной безопасности соответствует требованиям ГОСТ Р ИСО 9001-2015 (ISO 9001:2015). Выдан на основании решения экспертной комиссии.



infotecs

Мы защищаем информацию,
которую вы цените



Правила гарантийного обслуживания ПАК ViPNet:

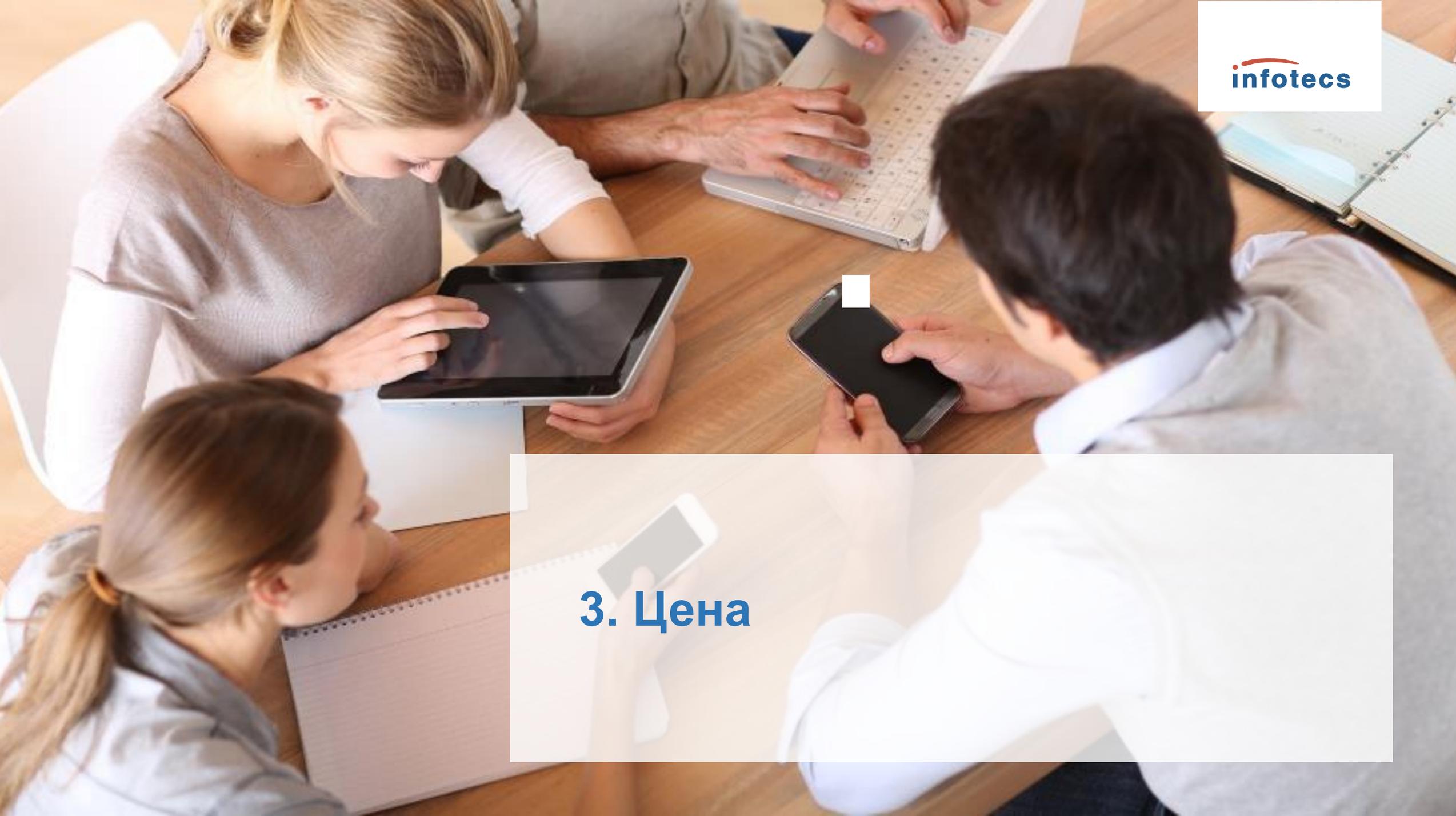
На всё оборудование, поставляемое в составе ПАК ViPNet, устанавливается гарантийный срок 1 (один) год с момента продажи.

- Гарантийное обслуживание может осуществляться:
- в течение гарантийного срока;
- в течение контракта на расширенную техническую поддержку на второй, третий, четвертый и пятый год с момента продажи ПАК при условии, что расширенная техническая поддержка не прекращалась.

СХЕМЫ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ — набор услуг, направленных на оказание помощи ПОЛЬЗОВАТЕЛЯМ ПРОДУКТОВ, оказываемых ИСПОЛНИТЕЛЕМ

Схемы технической поддержки	Описание
Базовая (Гарантия)	Предполагает оказание помощи Производителем в рамках гарантийного срока по гарантийным случаям.
Совместная Стандартная ТП	На первой линии технической поддержки выступает авторизованный партнёр. Объём оказываемых услуг приведен в соглашении об уровне сервиса.
Совместная Расширенная ТП	На первой линии технической поддержки выступает авторизованный партнёр. Объём оказываемых услуг приведен в соглашении об уровне сервиса.
Прямая (Авторская) Расширенная ТП	На первой линии технической поддержки выступает служба технической поддержки Производителя. Объём оказываемых услуг приведен в соглашении об уровне сервиса.
Прямая (Авторская) Премиальная ТП	На первой линии технической поддержки выступает служба технической поддержки Производителя. Объём оказываемых услуг приведен в соглашении об уровне сервиса.

Соглашение об уровне сервиса: <https://infotecs.ru/support/sla>

A high-angle photograph of four business professionals sitting around a wooden table. A woman on the left is using a tablet. A man on the right is using a smartphone. Another woman in the foreground is looking at a notebook. A laptop is open in the background. A semi-transparent white box is overlaid on the bottom half of the image, containing the text '3. Цена'.

3. Цена

Цена на ТП:

- Совместная Базовая ТП – 15%*
- Совместная Расширенная ТП – 25%*
- Прямая Расширенная ТП – 35%*
- Прямая Премиальная ТП – 50%*

*от стоимости Прав на ПО / ПАК / Лицензии расширения по ценам действующего прайс-листа

Цены публичные: <https://infotecs.ru/product/prices.php>

The background of the slide is a photograph of a wind farm at sunset. Several wind turbines are silhouetted against a bright orange and yellow sky with scattered clouds. In the foreground, a series of high-voltage power lines and pylons stretch across the landscape.

4. Удаленность поставщика от потребителя

С благодарностью остаюсь, в г. Казань

АЛЕКСЕЙ АЛЕКСЕЕВ

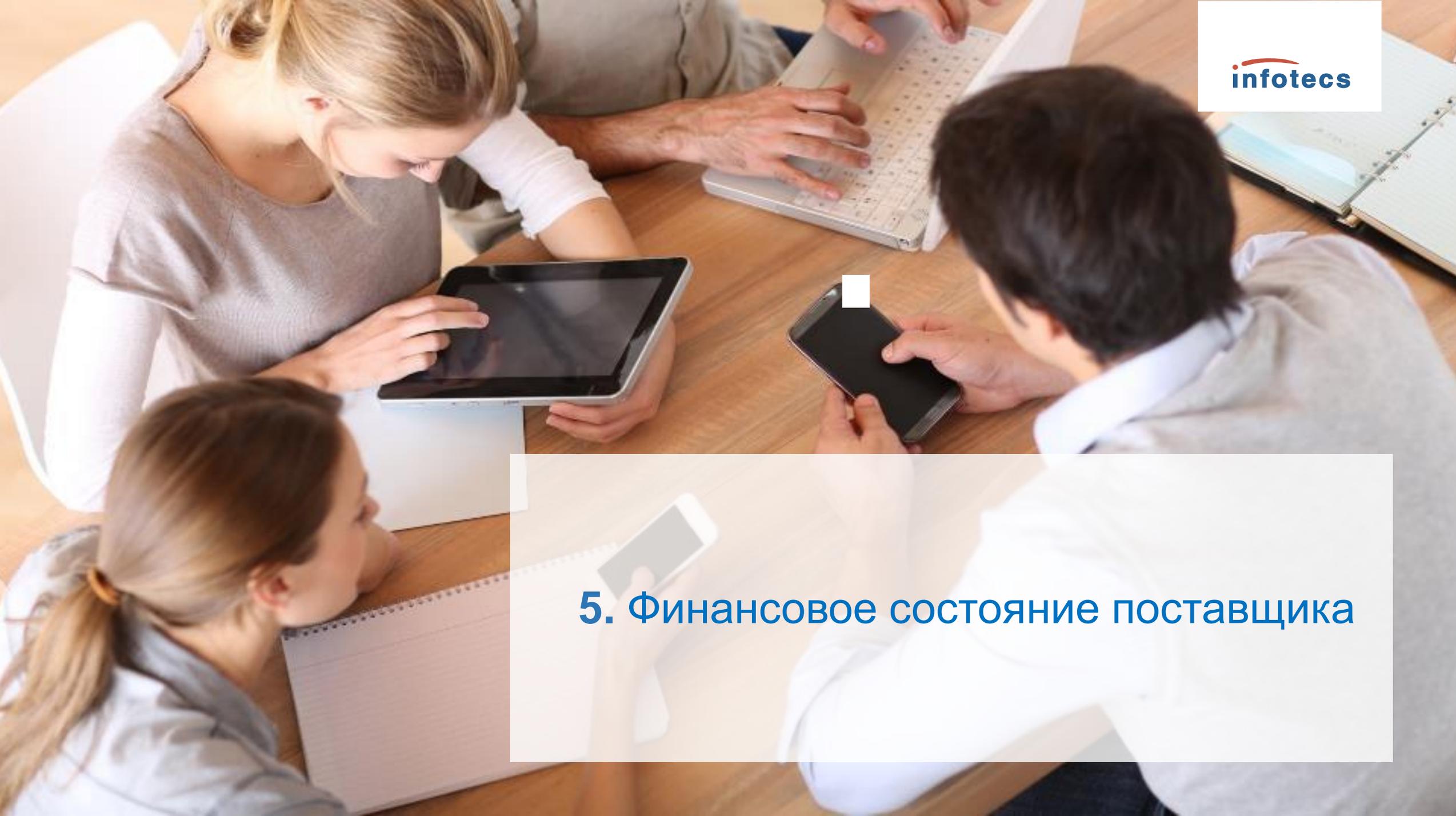
Региональный представитель

Aleksey.Alekseev@infotecs.ru

+7 917 899 8180




РЕГІОН ВОЛГИ

A high-angle photograph of a business meeting. Three people are seated around a wooden table. A woman on the left is using a tablet. A man on the right is using a smartphone. A woman in the foreground is looking at a notebook. A laptop is open in the background. A semi-transparent white box with blue text is overlaid on the bottom right of the image.

5. Финансовое состояние поставщика

ИнфоТеКС усилил свои позиции в рейтинге «СNews Security: Крупнейшие компании России в сфере защиты информации 2018»



Крупнейшее издание в сфере информационных технологий СNews опубликовало рейтинг «СNews Security: Крупнейшие компании России в сфере защиты информации 2018». Рейтинг подготовлен в рамках обзора Средства защиты информации и бизнеса 2018. По результатам рейтинга компания ИнфоТеКС поднялась с 5-й на 4-ю позицию по сравнению с предыдущим отчетным периодом. Выручка ИнфоТеКС выросла на 14% и составила в 2017 году 4 231 307 тыс. руб.

Продуктовые линейки ViPNet



ViPNet Network Security

Линейка ViPNet Network Security объединяет в своем составе компоненты сетевой безопасности, а также средства мониторинга и обнаружения вторжений



ViPNet PKI

Линейка ViPNet PKI представляет собой как самостоятельный комплекс компонентов, реализующий полную инфраструктуру продуктов открытого ключа, так и выступает в виде дополнения к средствам сетевой безопасности ViPNet Network Security



ViPNet Mobile Security

Линейка mobile security предлагает эффективные и надежные решения для защиты мобильных устройств от внешних и внутренних сетевых атак



ViPNet Industrial Security

Линейка ViPNet Industrial Security позволяет построить системы защиты информации для АСУ и систем межмашинного взаимодействия в соответствии с лучшими мировыми практиками и требованиями Российского законодательства



ViPNet EDI

ViPNet EDI – линейка сертифицированных продуктов для защищенного информационного обмена данными с Системой межведомственного электронного взаимодействия (СМЭВ) и Единым порталом государственных услуг и функций (ЕПГУ).



Бесплатные продукты

Линейка бесплатных продуктов представлена средствами электронной подписи ViPNet CSP, утилитой ViPNet HashCalc и другими продуктами.

Центр мониторинга компьютерных инцидентов с 2014 года, первый коммерческий контракт ГосСОПКА с 2017 года.

353 млн.
событий за 2018 г.

894
инцидента за 2018 г.



И ещё более 40 организаций подклю

Экз. № 1



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(ФСБ России)

ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ И
СПЕЦИАЛЬНОЙ СВЯЗИ
(8 Центр)

Генеральному директору Закрытого
акционерного общества
«Перспективный мониторинг»

В.В. Клименко

31 октября 2017 г. № 149/2/7-912

Москва

О направлении подписанного
Соглашения

Уважаемый Владимир Васильевич!

Направляем подписанное Соглашение о взаимодействии Федеральной службы безопасности Российской Федерации и Закрытого акционерного общества «Перспективный мониторинг» в области обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Приложение: от вх. № 928 от 29 сентября 2017 г. (№ 149/2/7-647), на 7 л.

С уважением,

Заместитель руководителя службы ФСБ России –
начальник Центра

А.М. Ивашко
А.М. Ивашко

БАЗА РЕШАЮЩИХ ПРАВИЛ (БРП)

- БРП в IDS NS/HS это набор сигнатур, написанных аналитиками (ЗАО «Перспективный мониторинг») на основе анализа разного рода вредоносных активностей (Атак, вредоносного ПО и так далее). Сигнатура может, как детектировать однозначно какую-либо атаку, так и какие-либо косвенные признаки этой атаки.
- БРП TIAS (экспертные данные) это набор который содержит в себе правила для корреляции всех сигнатур IDS NS и/или IDS HS между собой.

Т.е. грубо говоря, IDS (например NS) на основе БРП срабатывает на какой – либо паттерн какой-либо атаки на этапе прохождения трафика по сети, TIAS анализирует все эти срабатывания и сопоставляет их между собой и генерирует алерт (подозрение на инцидент) . Помимо этого БРП TIAS еще отвечает за распределения сигнатур IDS по категориям.

Состав экспертных данных ViPNet TIAS:

- БРП IDS NS
- Метаправила (правила выявления инцидентов)
- Список тегов (для классификации типов угроз)
- Шаблоны инцидентов (для создания карточек инцидентов и рекомендаций)
- Математическая модель принятия решений (модель переобучается раз в месяц на актуальных данных и переобученная модель в составе экспертных данных передается в TIAS)
- Справочник с геоданными
- Справочники с TI-feeds (индикаторы атак и компрометаций)

Первая линия

Взаимодействие с пользователями

Анализ событий и обнаружение компьютерных атак и инцидентов

Регистрация инцидентов ИБ и оповещение заинтересованных лиц

Вторая линия

Помощь в расследовании и установлении причин инцидентов

Координация действий при реагировании на инциденты ИБ

Анализ уязвимостей, анализ защищенности, тестирование на проникновение

Третья линия

Подготовка и улучшение нормативной базы, описание сценариев выявленных инцидентов

Разработка сигнатурных правил и правил корреляции

Углубленный анализ Инцидентов ИБ, сбор доказательной базы

Ссылки на документы, где есть определение обязательности (и желательности) пентестов:

- Для государственных информационных систем

Приказ ФСТЭК № 17

П. 10 — о возможности привлечения сторонней организации

П. 16.6 — на этапе проектирования ГИС проводится анализ уязвимостей

П. 18.3 — проведение анализа защищённости на этапе функционирования

п. 20.8 — описание мер по анализу защищённости

- Для банков:

Положение 382-П, 683-П, там в явном виде указана обязательность проведения тестирования на проникновение и анализа уязвимостей. Раз в год. Сторонней организацией — лицензиатом ФСТЭК.

- Для ИСПДн

Приказ ФСТЭК 21

П. 8.8 — про систематические мероприятия по контролю защищённости

П. 11. — применение пентестов при наличии определённых угроз

Услуги ЗАО ПМ: пентесты



infotecs®

Ссылки на документы, где есть определение обязательности (и желательности) пентестов:

- Для АСУТП

Приказ ФСТЭК 31

П 15.7 — про возможность проведения пентестов АСУТП

- Для субъектов КИИ:

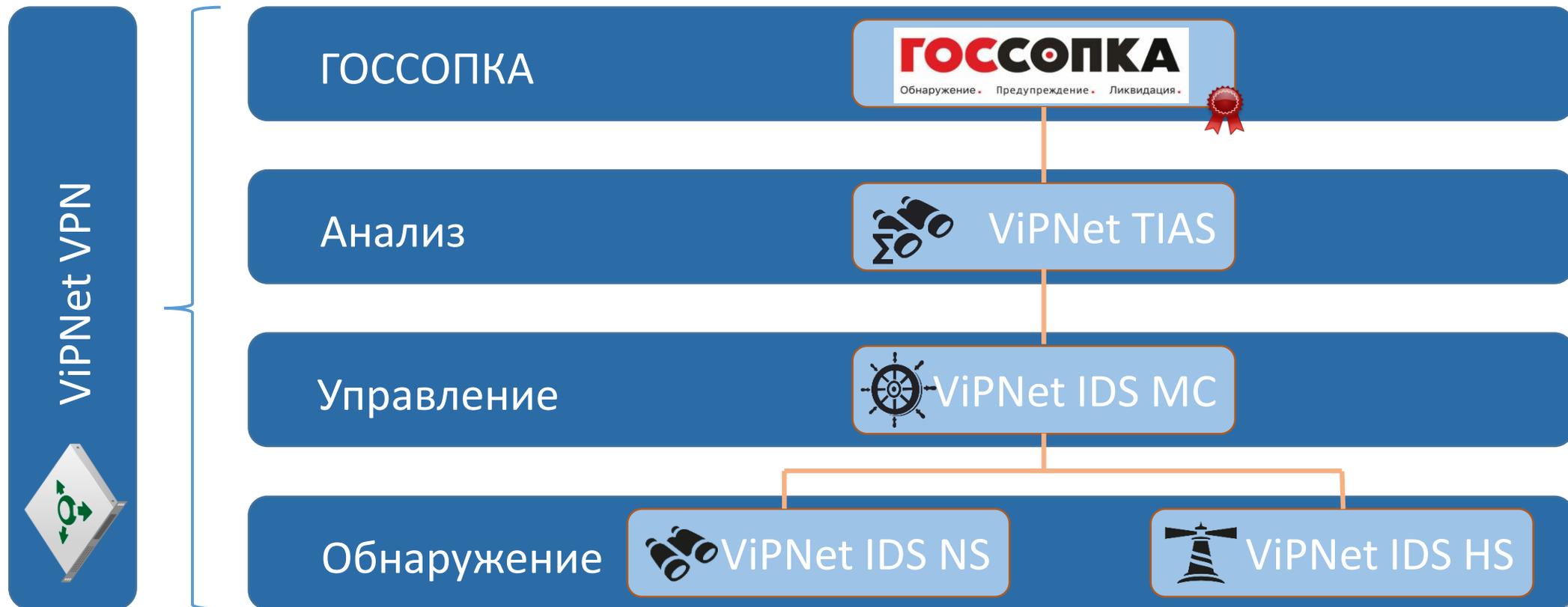
Документ НКЦКИ «МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ по проведению мероприятий по оценке степени защищенности от компьютерных атак». Мероприятия (к которым относятся и пентесты) рекомендуется проводить не реже раза в год.

Приказ ФСТЭК №235, п.п. 35, 36. Должен проводится ежегодный контроль состояния безопасности. Могут привлекаться сторонние организации, лицензиаты ФСТЭК.

Вопрос: КАК можно сэкономить бюджеты и сделать правильно?

Ответ 2: ДОГОВОРИТЬСЯ с поставщиком в рамках взаимовыгодного сотрудничества.

ViPNet TIAS и передача данных в ГосСОПКА



Варианты исполнения ViPNet TIAS

Desktop



ПАК ViPNet TIAS 100

Server 1U



ПАК ViPNet TIAS 1000
 ПАК ViPNet TIAS 2000
 ПАК ViPNet TIAS 5000

Virtual Appliance



ViPNet TIAS VA

техно infotecs
2019 Фест

ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

12
09 2019

Один день, три потока, стендовые доклады и мастер-классы, технические презентации и демонстрации решений продуктов и услуг ИнфоТеКС. Киберучения, интерактивы и How to от продуктовых менеджеров.

Как обеспечить защиту КИИ, как подключиться к системе ГосСОПКА, как сегментировать распределенные ИС, как внедрять белые списки и легко выявлять аномалии, как удостовериться в защищенности ИС, как создавать продукты совместно с ИнфоТеКС – Вы сможете узнать ответы на все эти вопросы, а также задать свои!

ПРЕЗЕНТАЦИИ:

<https://infotecstechfest.ru/presentations/>

**Выездное обучение в Казани
«АДМИНИСТРИРОВАНИЕ СИСТЕМ ЗАЩИТЫ
ИНФОРМАЦИИ WIN&LIN ВЕРСИИ 4»**

Даты проведения обучения:

21 октября по 25 октября 2019 года.

Форма проведения обучения: очная с отрывом от работы.

Продолжительность обучения: 5 рабочих дней очно.

Адрес оказания услуг: г. Казань, КНИТУ-КАИ

СПАСИБО

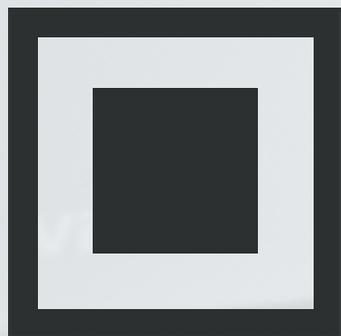
infotecs

Вопросы сюда:

CG CENTER

Дмитрий КИБЕНКО | dk@cg.ru

+7 917 297 8532



**КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ**