



ЦЕНТР
ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ
Красноярского
края

Оказание сервисной модели
информационной безопасности

Предпосылки

- Развитая защищенная сеть передачи данных между органами власти Красноярского края
- Хаотичное выстраивание модели системы защиты информации каждым органом власти Красноярского края
- Отсутствие в органах власти средств защиты информации и обслуживающего их персонала

Цель:

Выстраивание единой модели системы защиты информации на территории Красноярского края

Повышение уровня защищенности

Задачи:

Формирование списка оказываемых услуг ИБ

Подключение к инфраструктуре КГКУ «ЦИТ»

Техническое сопровождение оказываемых услуг, с предъявлением отчетности

Список услуг



Защита
каналов
связи



Аттестация
информацио
нных систем



Поиск и
анализ
уязвимостей



Защита WEB-
приложений



Антивирусная
защита



Мониторинг
и управление
доступом
поставщиков
ИТ-услуг

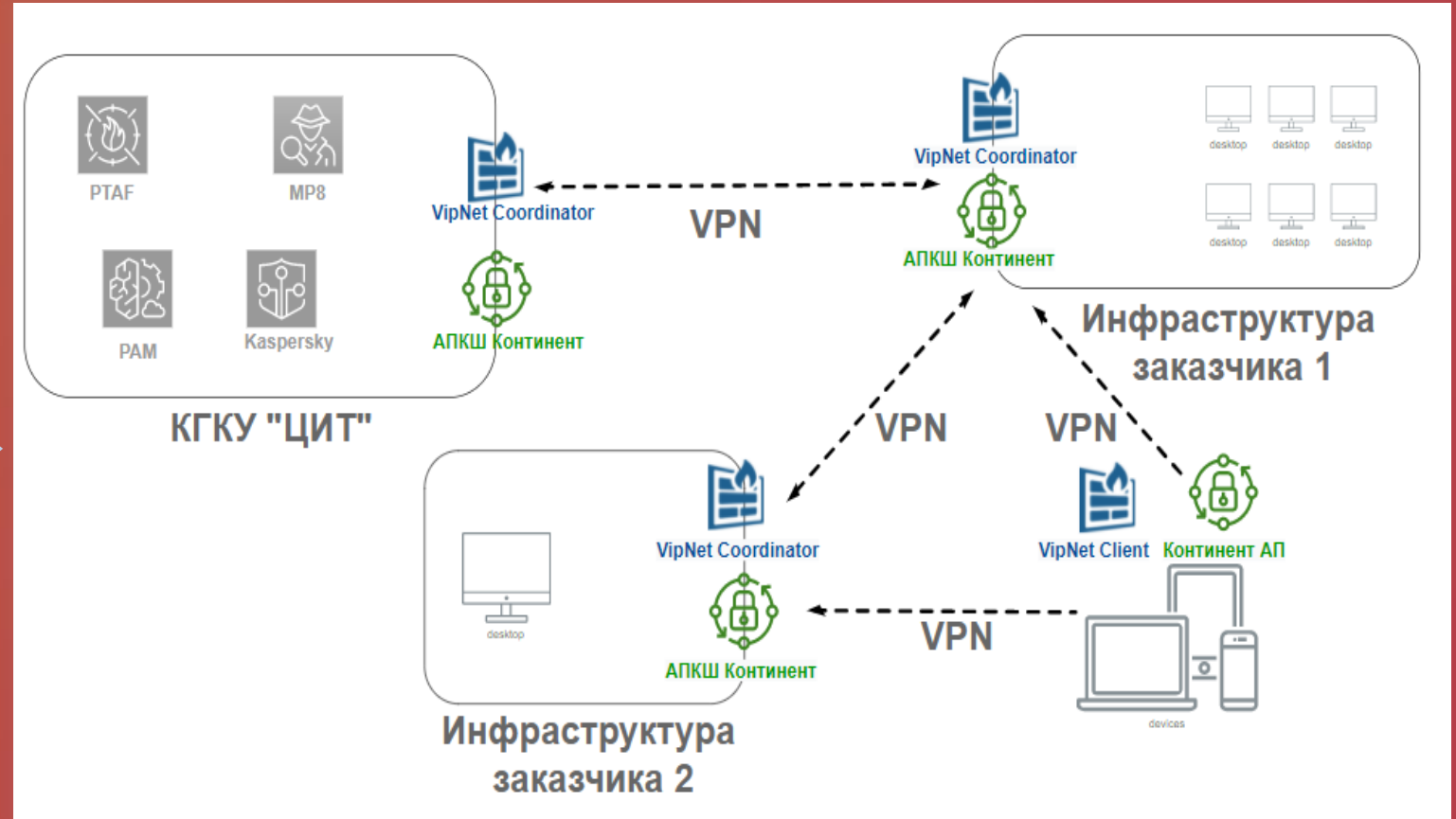
Защищенная сеть

Около 2000 узлов ЗСПД

Удаленный доступ с любого устройства

Транспорт для предоставления остальных услуг ИБ

Защищенная связь между филиалами



Аттестация информационных систем

4050	18.02.2022	бессрочно	Крайнее государственное казенное учреждение "Центр информационных технологий Красноярского края" (КГКУ ЦИТ)	1102468001316	2466226448	660021, г. Красноярск, ул. Рубежсера, д. 32, пом. 176	660060, г. Красноярск, ул. Брянская, д. 23	а, б, в, г, д, е	24-л от 18.02.2022	Действующая
------	------------	-----------	---	---------------	------------	---	--	------------------	--------------------	-------------

Первая Предыдущая 1 **2** Следующая Последняя
 Записи с 11 по 20 из 20 (отфильтровано из 2,885 записей)

* в случае если лицензиат является физическим лицом.
 ** виды работ, услуг, составляющих лицензируемый вид деятельности (в соответствии с пунктом 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79):
 а - услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам*** (а1...а4):
 а1 - в средствах и системах информатизации;
 а2 - в технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается;
 а3 - в помещениях со средствами (системами), подлежащими защите;
 а4 - в помещениях, предназначенных для ведения конфиденциальных переговоров (далее - защищаемые помещения);
 б - услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
 в - услуги по мониторингу информационной безопасности средств и систем информатизации;
 г - работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации (г1...г3);

Соответствие требованиям, утвержденным приказом ФСТЭК России от 18.02.2013 г. № 21

Соответствие требованиям, утвержденным приказом ФСТЭК России от 11.02.2013 г. № 17

Поиск и анализ уязвимостей

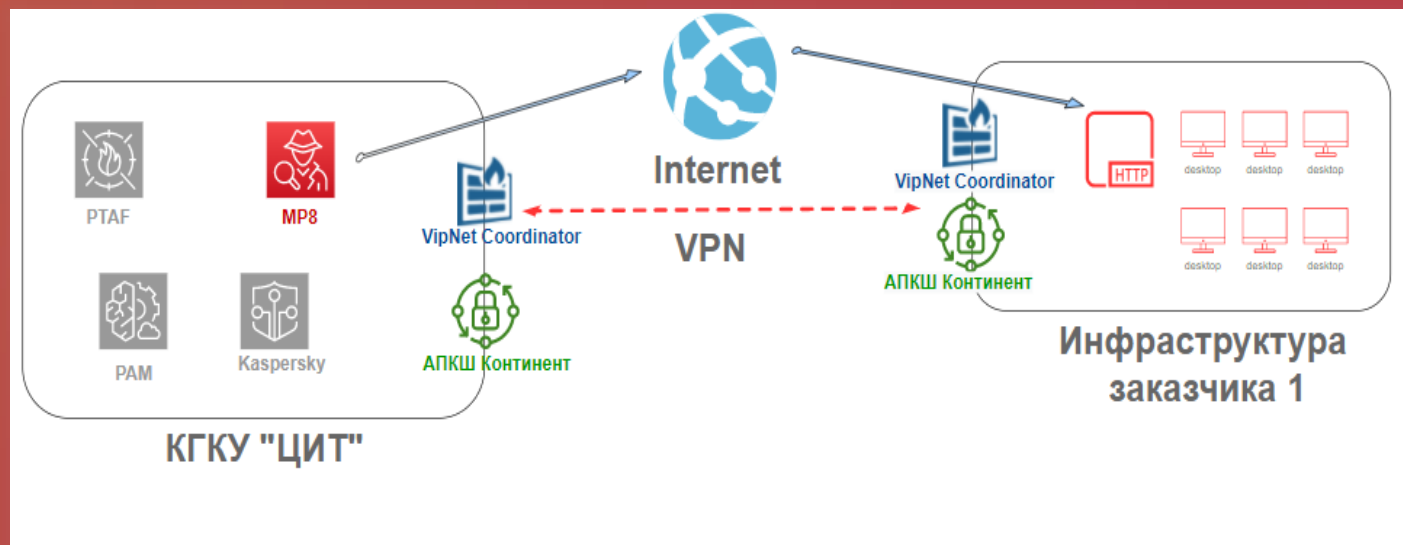
Audit ИТ-инфраструктуры

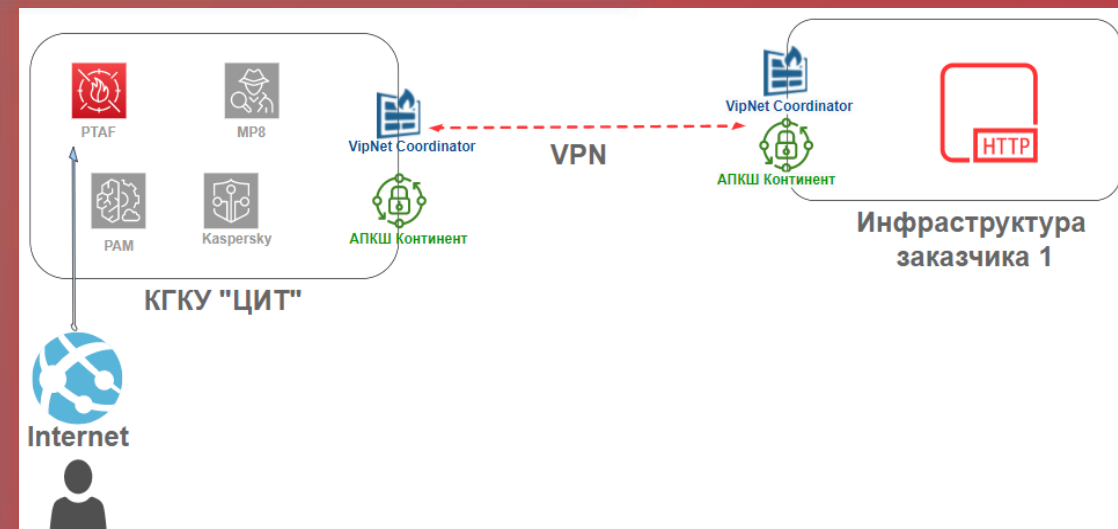
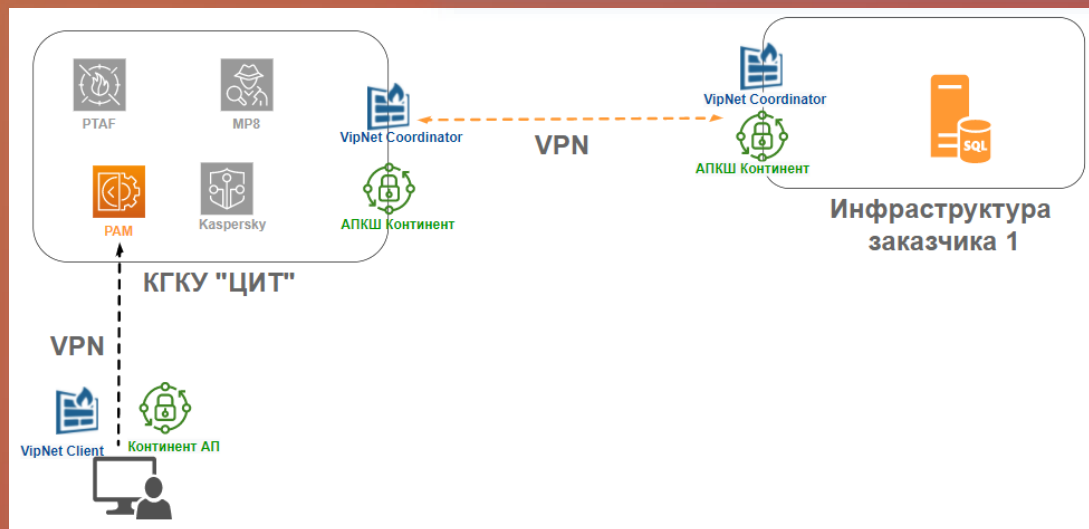
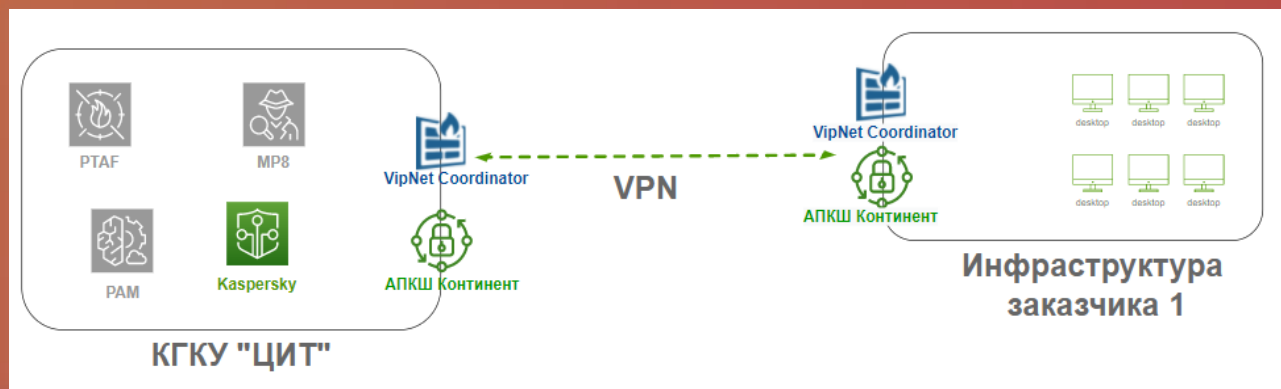
Инвентаризация ИТ-активов

Поиск уязвимостей ПО

PenTest приложений

Отчетность с рекомендациями по устранению уязвимостей





Защита Web-приложений

- Защита от атак Zero Day
- Защита на уровне приложения
- Защита DDoS
- Защита от ботов
- DashBoard для мониторинга

Антивирусная защита

- Доступ для мониторинга и управления защитой

Мониторинг и управление доступом поставщиков ИТ-услуг

- Предоставление доступа по согласованию
- Запись действий
- Ограничение действий

Развитие услуг



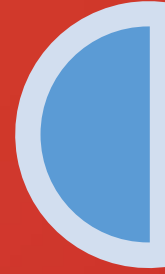
Масштабируемость

Оказываемые услуги должны обеспечивать широкий запас к масштабированию



Развитие технической вооруженности

Постоянное расширение парка средств защиты с учетом необходимости приобретаемого функционала



Стандартизация

Накопленный опыт документируется и на его базе формируется единый стандарт к выстраиванию единой модели системы защиты информации

Спасибо за внимание!