

ВУЗ

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
на тему:**

**«Организация безопасного обмена данными
центрального офиса с сотрудниками,
работающими удаленно в компании»**

Выполнил:

Научный руководитель:

Методологической основой исследования являются анализ нормативно-правовых стандартов обеспечения информационной безопасности при организации удаленного доступа, научные труды отечественных и зарубежных ученых в области организации локально-вычислительных сетей и мероприятий по обеспечению их защищенности.

Актуальность темы исследования определяется комплексом системных мероприятий по обеспечению режима информационной безопасности при организации безопасного обмена данными центрального офиса с сотрудниками, работающими удаленно.

Новизна темы обуславливается комплексным подходом к разработке системы обеспечения режима информационной безопасности при удаленном доступе сотрудников к ресурсам локальной сети организации.

Цель и задачи

Цель - организация безопасного обмена данными центрального офиса с сотрудниками, работающими удаленно в компании.

Задачи:

1. провести анализ литературы по теме исследования;
2. проанализировать необходимость защиты информации при удаленном доступе к локальным ресурсам;
3. оценить перспективные решения в сфере информационной безопасности;
4. разработать рекомендации и предложения по проектированию системы удаленного доступа.

Основные элементы локальной компьютерной сети

рабочие станции и
серверное оборудование;

коммуникационное
оборудование;

системное и прикладное
программное обеспечение.

Требования к локальной сети организации

надежности и
отказоустойчивости;

производительности;

масштабируемости;

обеспечения
информационной
безопасности;

экономической
эффективности

Требования для организации безопасного обмена данными центрального офиса с сотрудниками

центральный сервер,
обрабатывающий запросы
сотрудников на
предоставление удаленного
доступа;

программный доверенный
модуль, устанавливаемый на
рабочие станции удаленных
сотрудников,
предназначенный для
аутентификации
пользователя.

Архитектурно комплекс состоит из нескольких решений

Криптошлюз — основной элемент комплекса, обеспечивающий практически весь необходимый функционал



Детектор Атак – система обнаружения вторжений, подключаемая к SPAN-порту и обнаруживающая атаки сигнатурными и эвристическими методами. Детектор атак способен в режиме реального времени информировать администратора или аудитора о выявленных инцидентах либо с помощью специального ПО, либо через электронную почту.

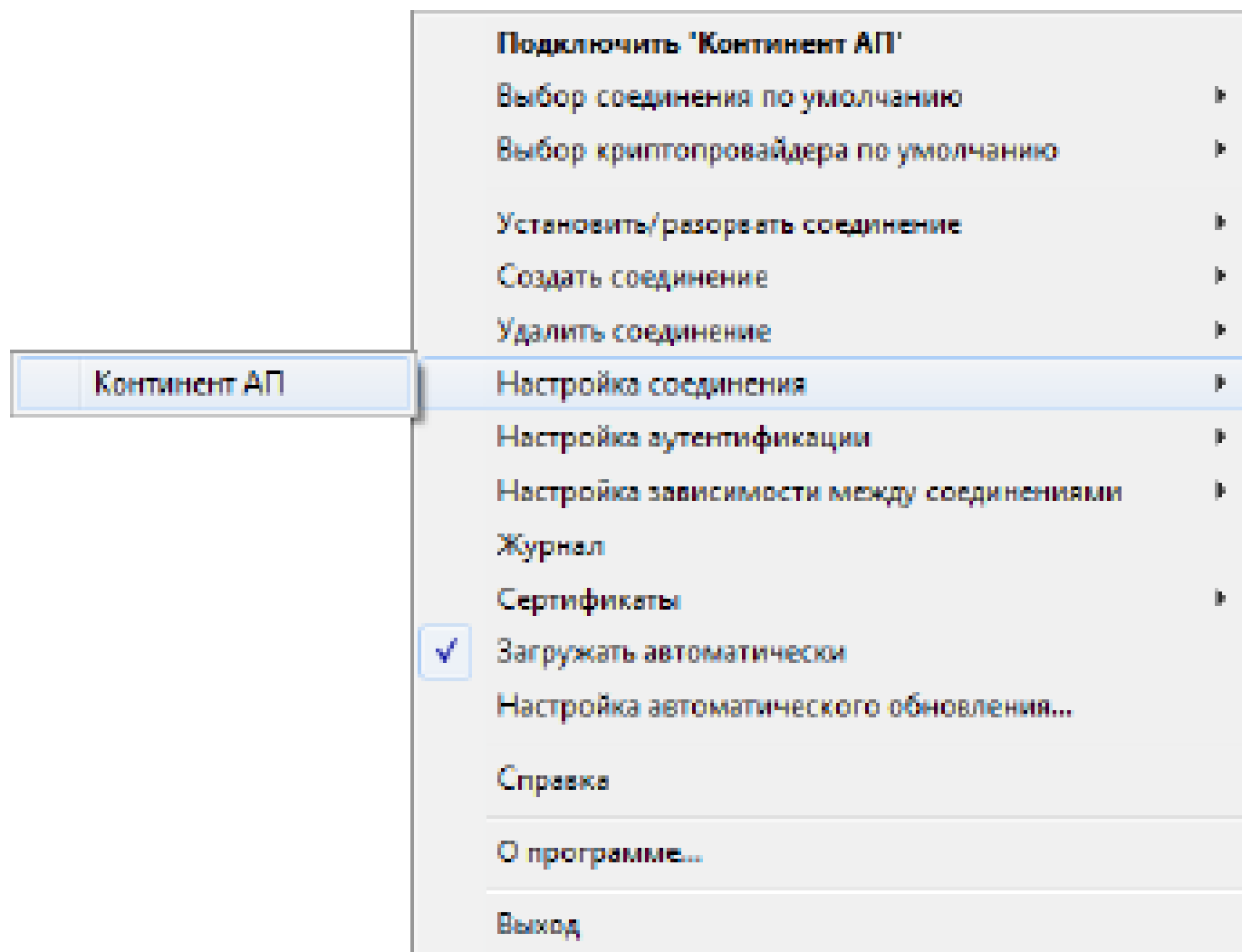


Центр Управления Сетью, он же ЦУС – средство централизованного управления и мониторинга перечисленных выше устройств «Континент». Сам по себе может выполнять роль криптошлюза, обеспечивая маршрутизацию, функции NAT и построение L3 VPN.



СПО «Сервер Доступа» и СКЗИ «Континент-АП», используемые для обеспечения защищенного удаленного доступа отдельных рабочих станций. Сервер доступа – серверный компонент, отвечающий за настройку маршрутизации, добавление или удаление клиентов, а также выпуск сертификатов. Сервер доступа может быть развернут либо на Центре Управления Сетью, либо на криптошлюзе.

Настройка соединения СКЗИ «Континент-АП»



АПКШ «Континент», платформа IPC-100



Проектирование системы безопасного обмена данными центрального офиса с сотрудниками, работающими удаленно, позволило:

обеспечить существенную экономию затрат при относительно высоких начальных вложениях за счёт низких эксплуатационных расходов при длительном сроке эксплуатации;

повысить эффективность работы предприятия за счет совместного использования данных и сетевых устройств, применения современных систем контроля управления трафиком.

БЛАГОДАРЮ ЗА ВНИМАНИЕ!