Краснодарское высшее военное училище имени генерала армии С.М. Штеменко

Доклад на тему:

АЛГОРИТМ РЕЗЕРВИРОВАНИЯ СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК В СЕТИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

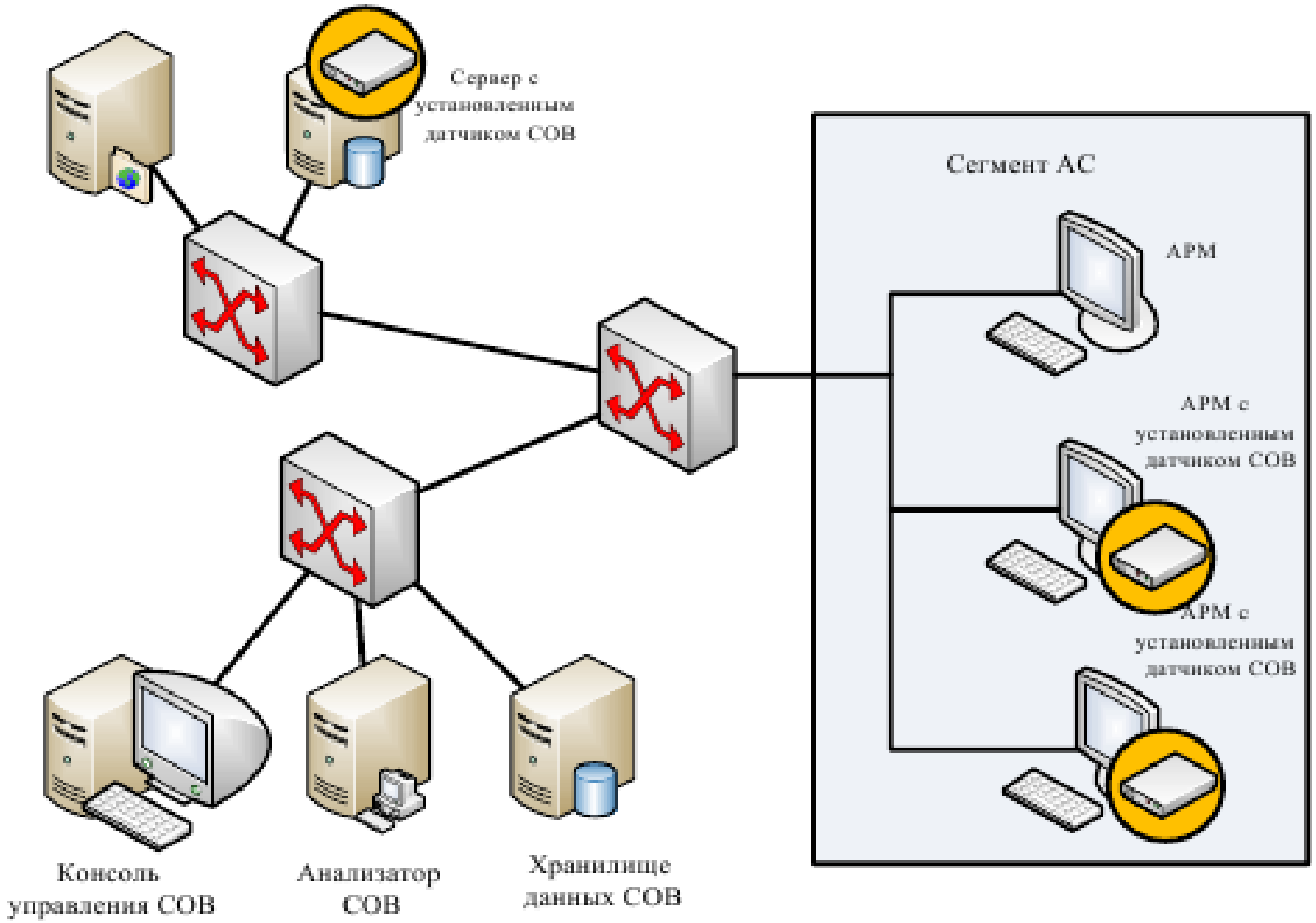
Докладчики: Лебедкина Т.В., Львов В.А.

Актуальность исследования

Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»	обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры (КИИ) РФ, в мирное время, в период непосредственной угрозы агрессии и в военное время»
Федеральный закон РФ № 187-ФЗ от 26 июля 2017 года «О безопасности критической информационной инфраструктуры Российской Федерации»	недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта КИИ
Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы	обеспечить комплексную защиту информационной инфраструктуры РФ, в том числе с использованием системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (СОПКА) на информационные ресурсы и системы критической информационной инфраструктуры; проводить непрерывный мониторинг и анализ угроз, возникающих в связи с внедрением новых информационных технологий, для своевременного реагирования на них
ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения	Критически важная система информационной инфраструктуры – информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление или информационное обеспечение критическим объектом или процессом, или используется для официального информирования общества и граждан, нарушение или прерывание функционирования которой (в результате деструктивных информационных воздействий, а также сбоев или отказов) может привести к чрезвычайной ситуации со значительными негативными последствиями

Классификация систем обнаружения атак

Типовая схема применения системы обнаружения атак в сети специального назначения



Алгоритм резервирования системы обнаружения атак в сети специального назначения

Алгоритм относится к области информационной безопасности вычислительных сетей и может быть использован в автоматизированных системах специального назначения с целью оперативного повышение живучести системы обнаружения атак.

Основная задача - обеспечение беспрерывной работы системы обнаружения атак, а также дополнительной защиты компонентов автоматизированной системы и вычислительной сети.

ВЫВОДЫ

С целью повышения живучести системы обнаружения атак в сетях специального назначения

проведен анализ

требований нормативно-правовых и методических документов Федеральной службы технического и экспортного контроля, рассматривающих СОА

исследованы

реализации процесса резервирования и аварийного восстановления СОА

разработан

алгоритм реализации процесса резервирования СОА в сетях специального назначения

Спасибо за внимание