Особенности проектирования систем защиты информации с применением СКЗИ

Филиппов Владимир
Руководитель отдела клиентских проектов ОАО «ИнфоТеКС»

О чем

infotecs

Особенности проектирования

систем защиты информации с применением СКЗИ

на примере территориально распределенной ИС

с удаленным доступом сотрудников к ИР компании

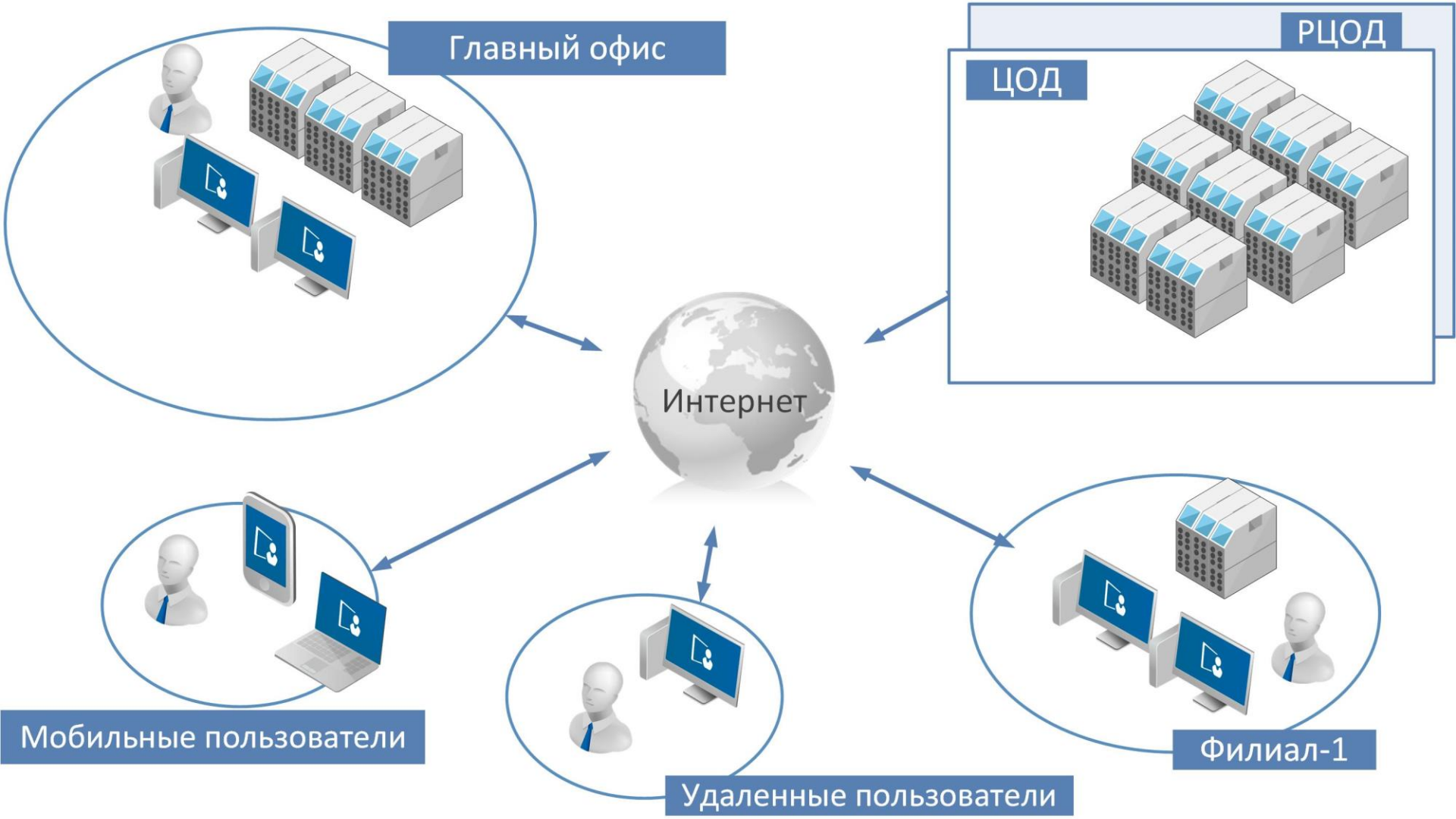
Объект защиты

- **типовая структура распределенной ИС:**
  - ✓ ЛВС нескольких офисов и территориальных филиалов
  - ✓ удаленные пользователи (вне офисов)
  - ✓ мобильные пользователи (вне офисов)

- **в ИС происходит обработка информации ограниченного доступа, не содержащей сведений, относящихся к государственной тайне**

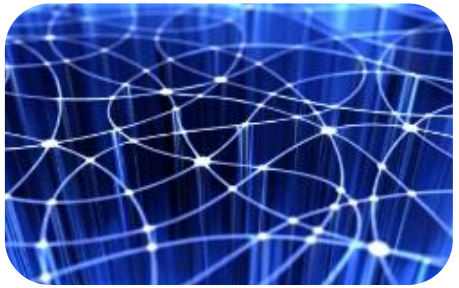
- **передача информации осуществляется по каналам сетей связи общего пользования (ССОП)**

Типовая схема распределенной ИС с удаленным доступом



Разработка Модели угроз и нарушителя

- анализ угроз ИБ и возможностей нарушителей безопасности информации определяют
  - ✓ структуру и содержание мер защиты
  - ✓ состав средств защиты информации (СрЗИ)



Трудности при построении СиЗИ

- отсутствие у заказчиков «необходимости» разрабатывать Модель угроз и нарушителя (МУиН) для своих ИС

- Нежелание брать на себя ответственность за сделанные в МУиН предположения

  - ✓ о неактуальности тех или иных угроз
  - ✓ об отсутствии тех или иных уязвимостей
  - ✓ от какого нарушителя строится защита

Что имеем

- решаются частные задачи защиты информации
- занижается класс криптосредств на границах сегментов ИС
  (снижается защита от внешнего нарушителя)
- исключается использование криптосредств внутри ИС
  (отсутствует защита от внутреннего нарушителя)
- не используются средства мониторинга, обнаружения вторжений
  (со временем Заказчик теряет контроль над защитой в его ИС)

Что делать

Грамотный обоснованный подход к разработке МУиН позволит заказчику построить эффективную систему защиты своей ИС и, в конечном счете, сэкономить средства на ИБ

Основные задачи по защите ИС

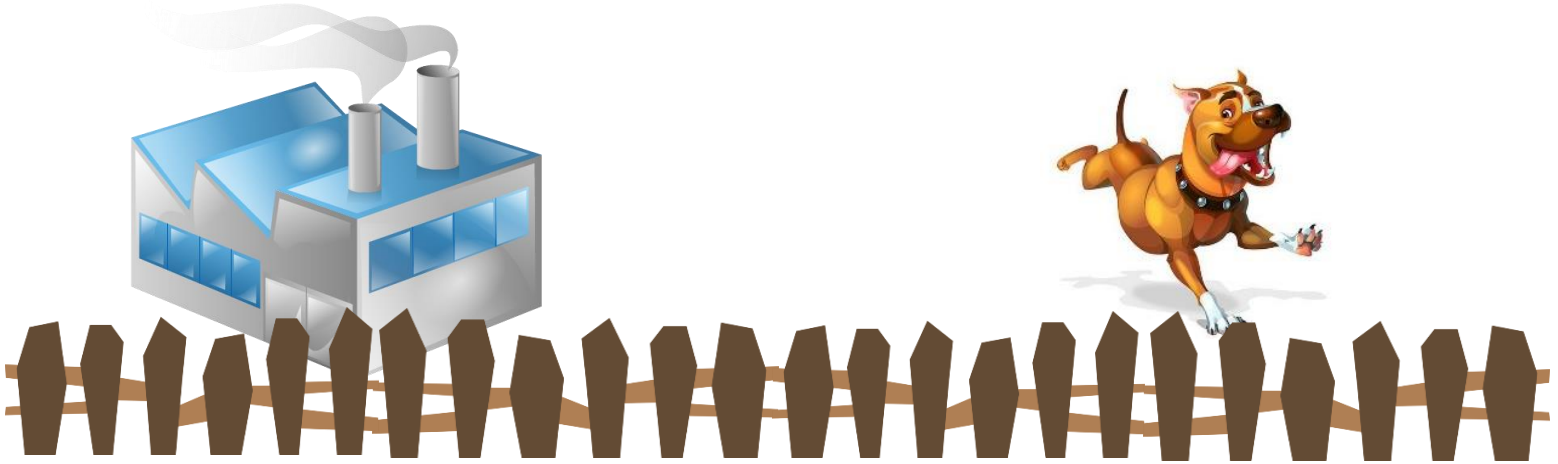
infotecs

❑ Внутреннее информационное взаимодействие

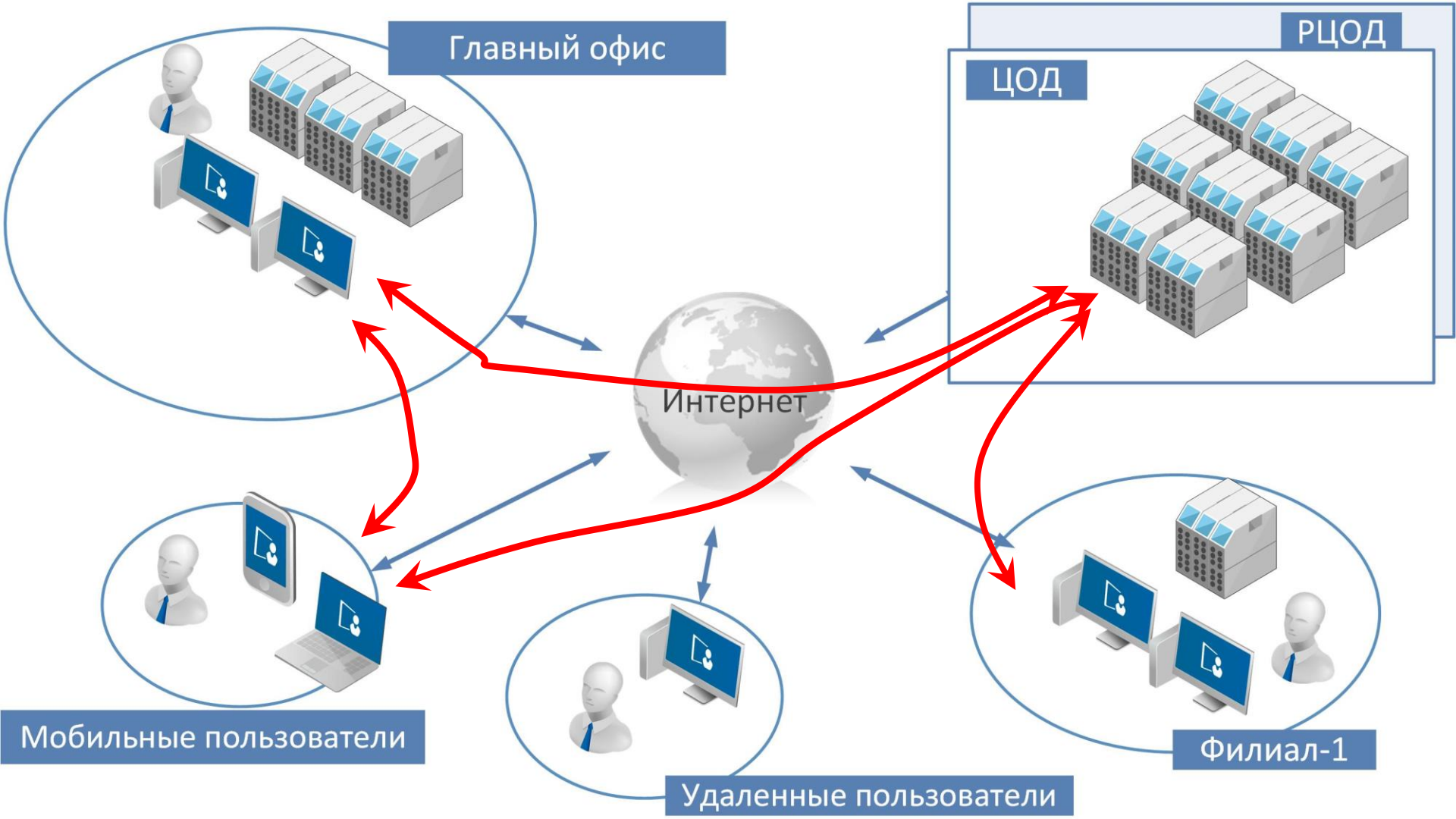
- ✓ обеспечения защищенного доступа сотрудников к ИР, в т.ч. удаленного доступа
- ✓ организация защищенного информационного взаимодействия сотрудников друг с другом

❑ Внешнее информационное взаимодействие

- ✓ организация защищенного информационного взаимодействия с ИС сторонних организаций



Типовая схема распределенной ИС с удаленным доступом



Взаимодействие с ИС сторонних организаций

- В рамках СМЭВ задача решается в соответствии с Техническими требованиями, утвержденными Приказом Минкомсвязи №190 от 27.12.2010 г.

- Для построения защищенного канала связи между своей ИС и системой взаимодействия должны использоваться сертифицированные СКЗИ класса не ниже КС3

Защита информации внутри ИС

infotecs

По каким требованиям

Если ИС – государственная → НПА по ЗИ

Если ИС – негосударственная → Отраслевые стандарты по ИБ

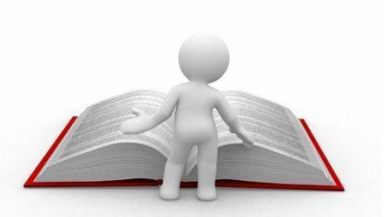
Защита информации внутри ИС

infotecs

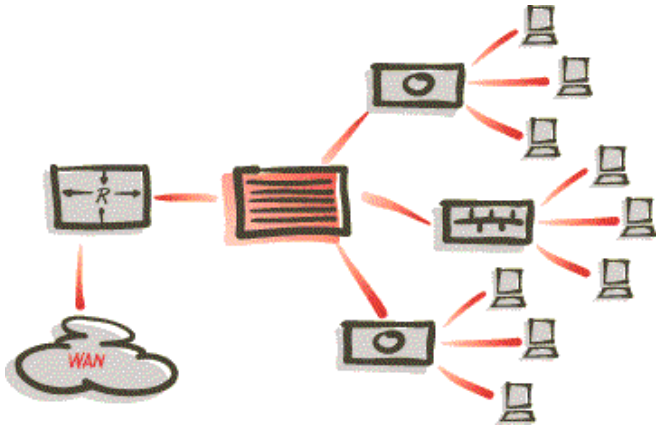
- **Отраслевые стандарты основаны на:**
  - ✓ 149-ФЗ Об И, ИТ и ЗИ (2006)
  - ✓ 98-ФЗ – О коммерческой тайне (2004 в ред.2014)
  - ✓ 152-ФЗ – О ПДн (2006 в ред. 2017)
  - ✓ РД НСД - АС/СВТ/МСЭ/НДВ
  - ✓ СТР-К Гостехкомиссии (ФСТЭК России)(2002)
  - ✓ ГОСТ АС, АСЗИ (34, 50, 51) … 51583, 51624 …РД 50-34.698-90
  - ✓ ПП-1119 – Требования к защите ПДн в ИСПДн (2012)
  - ✓ Приказ-17 ФСТЭК России - Требования о защите информации в ГИС (2013)
  - ✓ Приказ-21 ФСТЭК России - О составе и содержании орг-ттех мер по защите ПДн (2013)
  - ✓ Приказ-31 ФСТЭК России - Требования к обеспечению ЗИ в АСУ ТП на КВО (2014)
  - ✓ Приказ-27 ФСТЭК России – Изменения в Приказ-17 (2017)
  - ✓ БД УБИ (bdu.fstec.ru) – Банк данных угроз безопасности информации ФСТЭК России
  - ✓ ПКЗ-2005 ФСБ России – Положение о разработке и эксплуатации криптосредств
  - ✓ Приказ-378 ФСБ России - Об использовании СКЗИ при защите ПДн (2014)
  - ✓ Принципы разработки СКЗИ ТК26 – О проблемах при разработке и эксплуатации СКЗИ (2016) ……

Важнейшие характеристики ИС, влияющие на выбор класса СКЗИ

- Перечень объектов атак → информация, документация, объекты ИС



- Возможности нарушителей → сведения + ТС
- Место проведения атак → вне/внутри КЗ



Угроза НДВ

- наличие НДВ в СПО → СКЗИ класса КА
- наличие НДВ в ППО → СКЗИ класса КВ
- нет НДВ в СПО/ППО → СКЗИ класса ≥КС1

Зависимость класса СКЗИ от типа угроз НДВ

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз / класс СКЗИ					
			1 тип / СКЗИ		2 тип / СКЗИ		3 тип / СКЗИ	
ИСПДн-С	не сотрудники	≥100 000	УЗ 1	КА1	УЗ 1	≥КВ2	УЗ 2	≥КС1
		<100 000	УЗ 1	КА1	УЗ 2	≥КВ2	УЗ 3	≥КС1
	сотрудники	≥100 000	УЗ 1	КА1	УЗ 2	≥КВ2	УЗ 3	≥КС1
		<100 000	УЗ 1	КА1	УЗ 2	≥КВ2	УЗ 3	≥КС1
ИСПДн-Б	не сотрудники	≥100 000	УЗ 1	КА1	УЗ 2	≥КВ2	УЗ 3	≥КС1
		<100 000	УЗ 1	КА1	УЗ 2	≥КВ2	УЗ 3	≥КС1
	сотрудники	≥100 000	УЗ 1	КА1	УЗ 2	≥КВ2	УЗ 3	≥КС1
		<100 000	УЗ 1	КА1	УЗ 2	≥КВ2	УЗ 3	≥КС1
ИСПДн-И	не сотрудники	≥100 000	УЗ 1	КА1	УЗ 2	≥КВ2	УЗ 3	≥КС1
		<100 000	УЗ 1	КА1	УЗ 3	≥КВ2	УЗ 4	≥КС1
	сотрудники	≥100 000	УЗ 1	КА1	УЗ 3	≥КВ2	УЗ 4	≥КС1
		<100 000	УЗ 1	КА1	УЗ 3	≥КВ2	УЗ 4	≥КС1
ИСПДн-О	не сотрудники	≥100 000	УЗ 2	КА1	УЗ 2	≥КВ2	УЗ 4	≥КС1
		<100 000	УЗ 2	КА1	УЗ 3	≥КВ2	УЗ 4	≥КС1
	сотрудники	≥100 000	УЗ 2	КА1	УЗ 3	≥КВ2	УЗ 4	≥КС1
		<100 000	УЗ 2	КА1	УЗ 3	≥КВ2	УЗ 4	≥КС1

Возможности нарушителя и класс СКЗИ (1)

№	Возможности нарушителя	КС1	КС2	КС3	КВ1	КВ2	КА1
1	Создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ.	+	+	+	+	+	+
2	Создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ.	+	+	+	+	+	+
3	Проведение атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее – контролируемая зона).	+	+	+	+	+	+
4	Проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак: • внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и в совокупности представляющие среду функционирования СКЗИ (далее – СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ; • внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ.	+	+	+	+	+	+

Возможности нарушителя и класс СКЗИ (2)

№	Возможности нарушителя	КС1	КС2	КС3	КВ1	КВ2	КА1
5	**Проведение атак на этапе эксплуатации СКЗИ на следующие объекты:** • персональные данные; • ключевую, аутентифицирующую и парольную информацию СКЗИ; • программные компоненты СКЗИ; • аппаратные компоненты СКЗИ; • программные компоненты СФ; • аппаратные компоненты СФ (аппаратные средства, входящие в СФ, включая микросхемы с записанным микрокодом BIOS, осуществляющей инициализацию этих средств); • данные, передаваемые по каналам связи; • иные объекты, которые установлены при формировании совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак с учетом применяемых в информационной системе информационных технологий, аппаратных средств (далее – АС) и программного обеспечения (далее – ПО).	+	+	+	+	+	+

Возможности нарушителя и класс СКЗИ (3)

№	Возможности нарушителя	КС1	КС2	КС3	КВ1	КВ2	КА1
6	**Получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационная сеть «Интернет») информации об ИС, в которой используется СКЗИ.** **При этом может быть получена следующая информация:** • общие сведения об ИС, в которой используется СКЗИ • сведения об информационных технологиях, базах данных, АС, ПО, используемых в ИС совместно с СКЗИ • содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ; • общие сведения о защищаемой информации • сведения о каналах связи • все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от НСД орг-техническими мерами; • сведения обо все, нарушениях правил эксплуатации СКЗИ и СФ; • сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, неисправностях и сбоях аппаратных компонентов СКЗИ и СФ; • сведения, получаемые в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ.	+	+	+	+	+	+

Возможности нарушителя и класс СКЗИ (4)

№	Возможности нарушителя	КС1	КС2	КС3	КВ1	КВ2	КА1
7	Применение: • находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ; • специально разработанных АС и ПО.	+	+	+	+	+	+
8	Использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки: • каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами; • каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ;	+	+	+	+	+	+
9	Проведение на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеет выход в эти сети.	+	+	+	+	+	+
10	Использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ (далее – штатные средства).	+	+	+	+	+	+

Возможности нарушителя и класс СКЗИ (5)

№	Возможности нарушителя	КС1	КС2	КС3	КВ1	КВ2	КА1
11	Проведение атаки при нахождении в пределах контролируемой зоны.	-	+	+	+	+	+
12	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: • документацию на СКЗИ и компоненты СФ; • помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее – СВТ), на которых реализованы СКЗИ и СФ.	-	+	+	+	+	+
13	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: • сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; • сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; • сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ.	-	+	+	+	+	+
14	Использование штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	-	+	+	+	+	+

Возможности нарушителя и класс СКЗИ (6)

№	Возможности нарушителя	КС1	КС2	КС3	КВ1	КВ2	КА1
15	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ.	-	-	+	+	+	+
16	Возможность располагать аппаратными компонентами СКЗИ и СФ, ограниченная мерами, реализованными в ИС, в которой используется СКЗИ, и направленными на предотвращение и пресечение НСД.	-	-	+	+	+	+
17	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ.	-	-	-	+	+	+
18	Проведение лабораторных исследований СКЗИ, используемых вне КЗ, ограниченное мерами, реализованными в ИС, в которой используется СКЗИ, и направленными на предотвращение и пресечение НСД.	-	-	-	+	+	+
19	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак НДВ ППО.	-	-	-	-	+	+
20	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, включая анализ исходных текстов входящего в СФ прикладного ПО.	-	-	-	-	+	+
21	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак НДВ СПО.	-	-	-	-	-	+
22	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ.	-	-	-	-	-	+
23	Возможность располагать всеми аппаратными компонентами СКЗИ и СФ.	-	-	-	-	-	+

Рекомендации (нет НДВ в СПО/ППО)

- для защиты информации в каналах связи на границе ЛВС офисов необходимо устанавливать криптошлюзы класса не ниже КС3

- на внутренних каналах связи необходимо использовать СКЗИ класса КС1–КС3

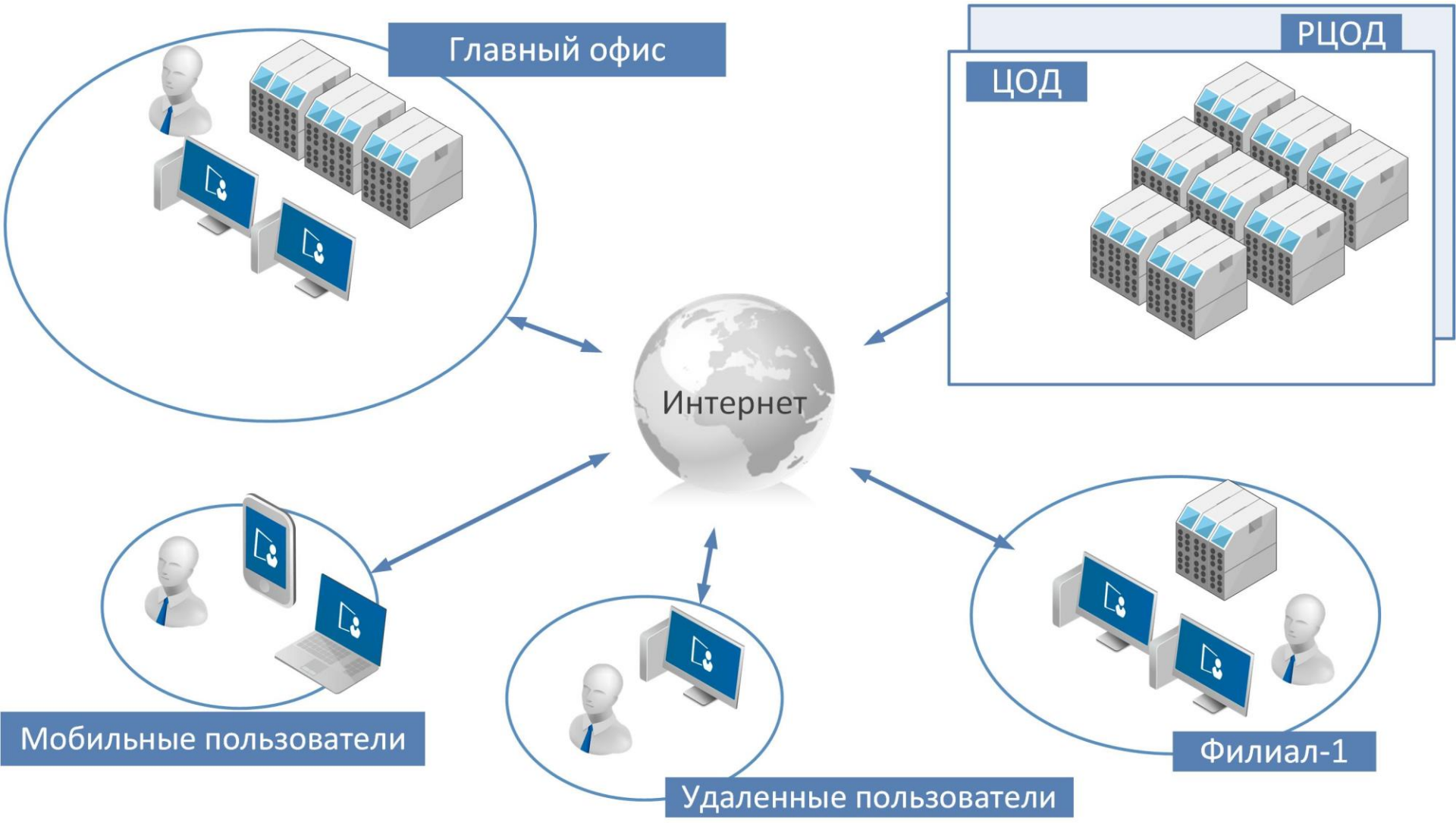
- на мобильные устройства, АРМ удаленных пользователей следует устанавливать СКЗИ класса КС1

- для защиты критической информации на АРМ сотрудников необходимо использовать СКЗИ класса КС1 и выше

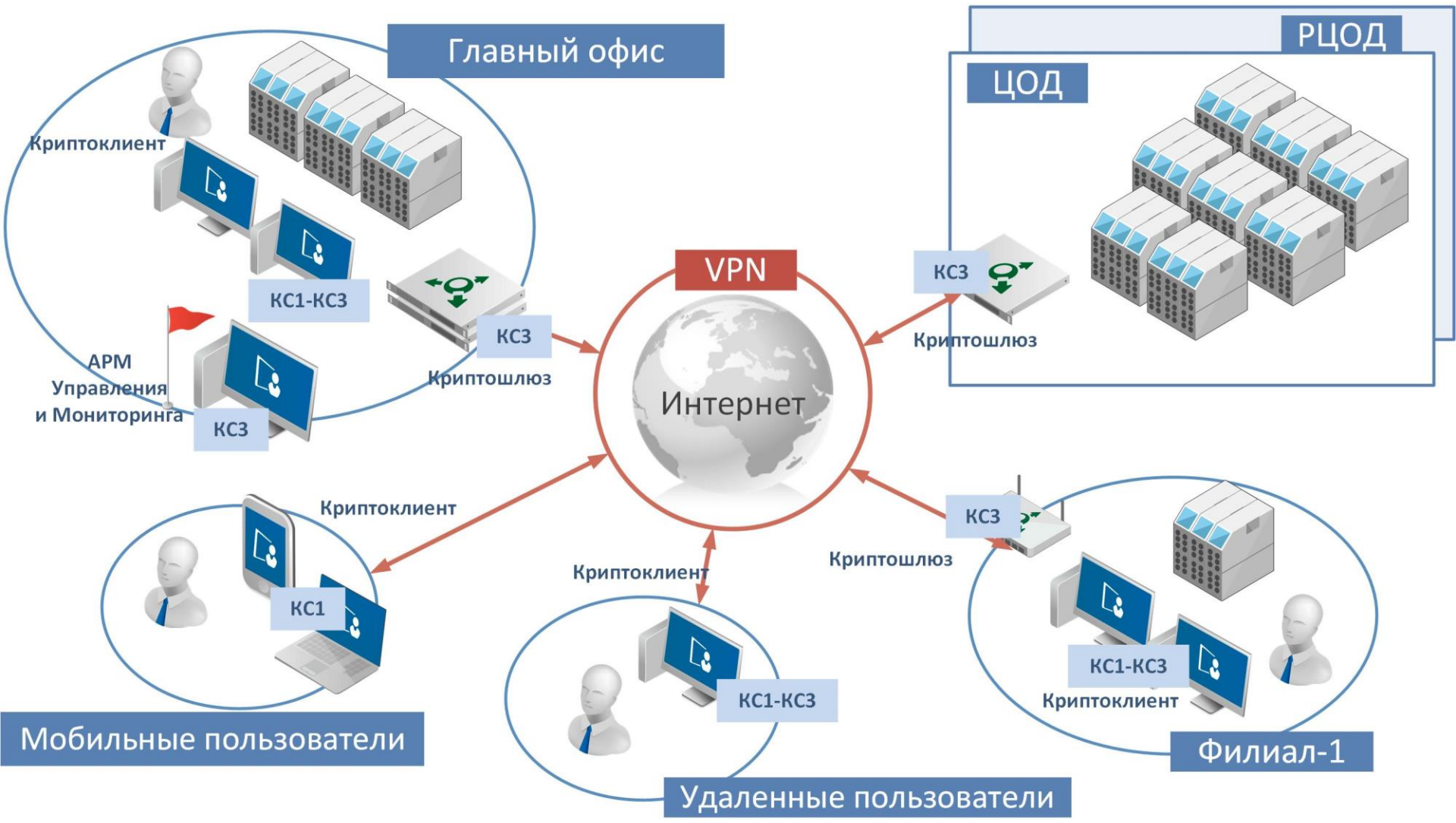
- для определения и анализа состояния узлов ИС, выявления критических событий и оповещения о них администраторов безопасности следует использовать Средства Мониторинга

- для повышения уровня защищенности ИС, ЦОД (РЦОД), АРМ, серверов и коммуникационного оборудования использовать СОВ/СОА

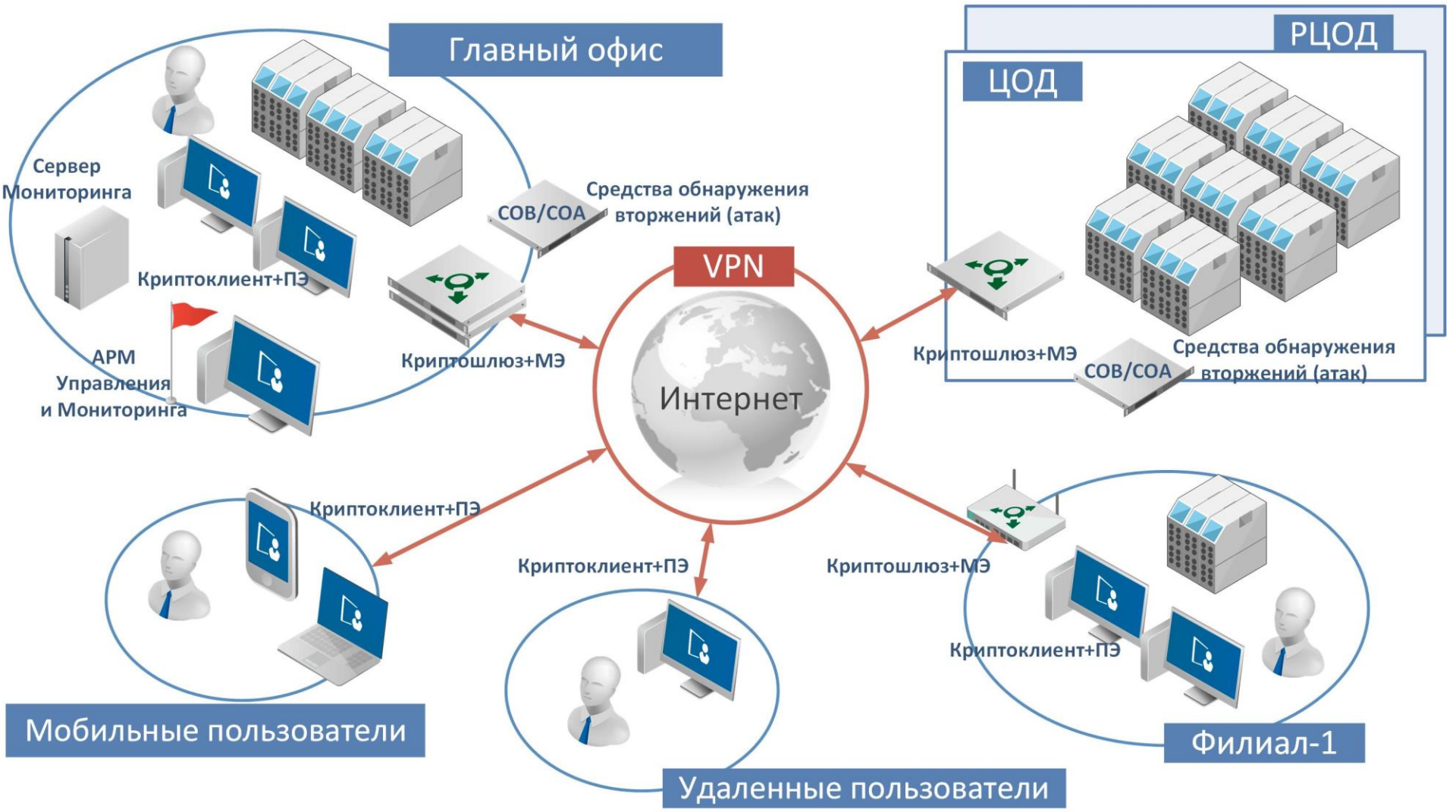
Типовая схема распределенной ИС



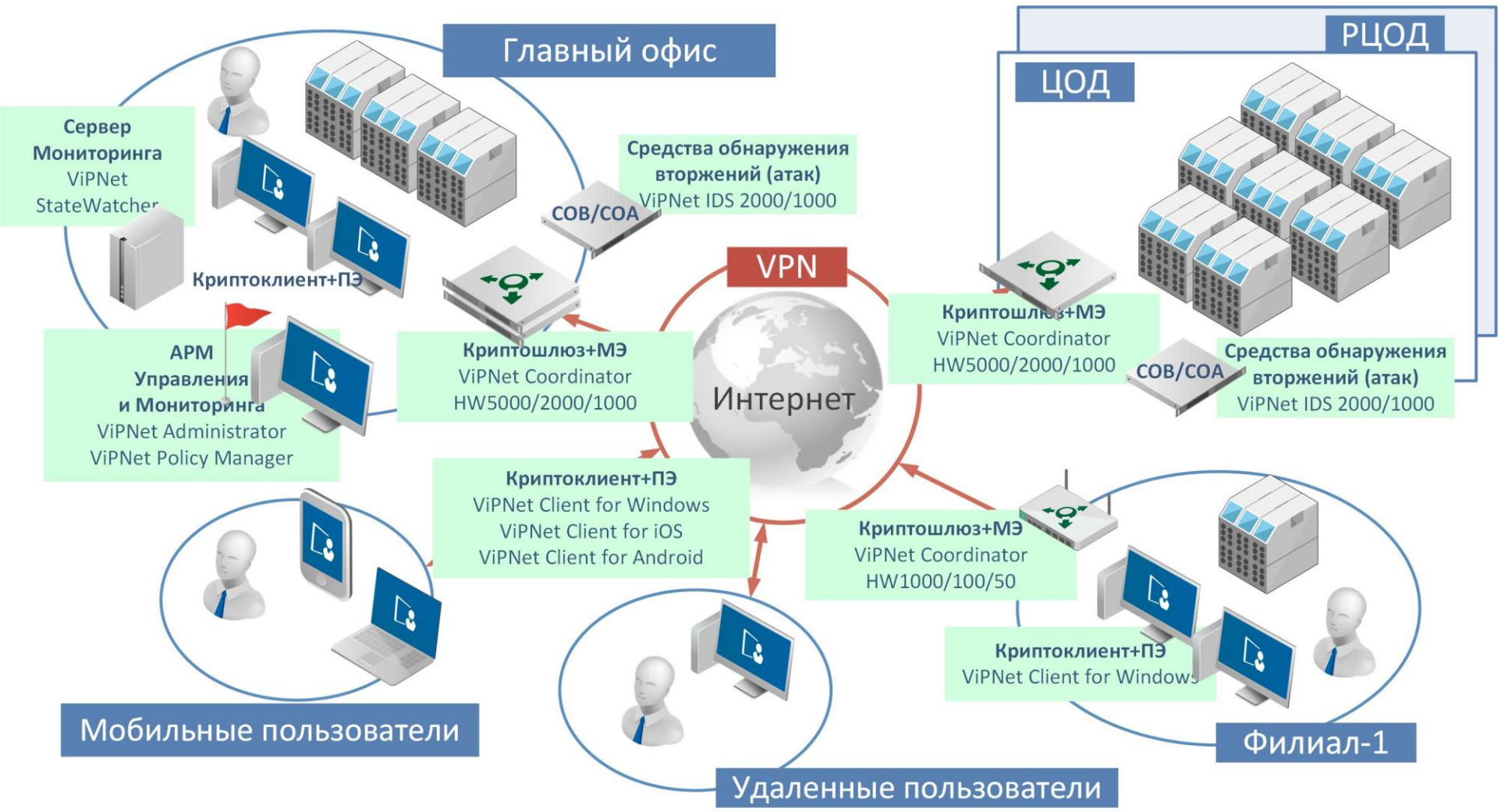
Класс криптозащиты



Построение СиЗИ



Технологии ViPNet при построении СиЗИ




Спасибо!