Негосударственное образовательное учреждение дополнительного профессионального образования
«Ростовский центр повышения квалификации в области информационных технологий и связи

СОГЛАСОВАНО

_____
_____

УТВЕРЖДАЮ
Директор НОУ ДПО «РЦПК ИТС»
_____Р.А.Забродин
“___”_____ 2014 г.

Учебный план

курсов повышения квалификации по программе:

«Администрирование системы защиты информации ViPNet (Win)»

Цель: Изучение актуальных вопросов обработки и защиты персональных данных в информационных системах персональных данных в соответствии с требованиями Российского законодательства. Обеспечение теоретической и практической подготовки специалистов в области защиты информации и защищенных компьютерных сетей. Приобретение умений и навыков для построения и модификации защищенных сетей по заданным схемам. Приобретение опыта в организации межсетевого взаимодействия защищенных сетей ViPNet.

Категория слушателей: Руководители и специалисты подразделений по защите информации, подразделений информационной безопасности, подразделений информационных технологий, подразделений, ответственных за работу с персоналом, системные и сетевые администраторы, администраторы безопасности.

Срок обучения: 40 часов
Форма обучения: учебные аудиторные занятия с отрывом от работы
Режим занятий: 5 дней в неделю по 8 часов (час. в день).

№	Наименование разделов и дисциплин	Аудиторные занятия, час				Форма конт-роля
		Всего	Лек-ции	Семинары	Практические	
1	2	3	4	5	6	7
1	**ВВЕДЕНИЕ В ТЕХНОЛОГИЮ VIPNET**	**4**	**4**			
1.1	Виды угроз информационной безопасности в телекоммуникационных системах	0.5	0.5			
1.2	Состав программного комплекса ViPNet.	0.5	0.5			
1.3	Логическая структура сети ViPNet.	3	3			
2	**VIPNET АДМИНИСТРАТОР 3.1**	**4**	**4**			
	Общие сведения, основные функции и назначение программы ViPNet [Администратор]	1	1			
2.1	Состав программного обеспечения. ЦУС и УКЦ.	0,5	0,5			
2.2	Особенности взаимодействия ЦУС и УКЦ.	0,5	0,5			

2.3	Основные понятия сетевого уровня	0,25	0,25			
2.4	Основные понятия прикладного уровня	0,25	0,25			
2.5	Разграничение доступа к конфиденциальной информации.	0,5	0,5			
2.6	Подсистема адресной администрации сети. Прикладная администрация (функциональное назначение, прикладные задачи).	1	1			
3	**СОЗДАНИЕ, УПРАВЛЕНИЕ И МОДИФИКАЦИЯ КЛЮЧЕВОЙ СТРУКТУРЫ VIPNET**	**8**	**3,25**	**0,25**	**4,5**	
3.1	Особенности ключевой структуры сети ViPNet	1	0,5		0,5	
3.2	Основные технические данные и характеристики СКЗИ	0,5	0,5			
3.3	Этапы формирования ключевой информации	1,5	0,5		1	
3.4	Управление ключевой информации в процессе функционирования сетей	1	0,5		0,5	
3.5	Последовательность установки и настройки ПО	1,5	0,25		1,25	
3.6	Основные действия администратора УКЦ	1,5	0,5		0,75	
3.7	Типовые варианты применения технологии ViPNet	1	0,5	0,25	0,5	
4	**ОРГАНИЗАЦИЯ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ. РАЗВЕРТЫВАНИЕ ВИРТУАЛЬНОЙ ЗАЩИЩЕННОЙ СЕТИ ЗАДАННОЙ КОНФИГУРАЦИИ**	**8**	**1,5**	**1,5**	**5**	
4.1	Виды межсетевых мастер-ключей (ММК)	2	1	1		
4.2	Развертывание виртуальной защищенной сети заданной конфигурации.	3	0,25	0,25	2,5	
4.3	Настройка, управление и модификация защищенной сети ViPNet	3	0,25	0,25	2,5	
5	**VIPNET [КЛИЕНТ]**	**8**	**2,75**	**1,5**	**3,75**	
5.1	Общие сведения, основные функции и назначение программы ViPNet [Клиент]	2	0,5	0,5	1	
5.2	Состав программного обеспечения.	0,25	0,25			
5.3	ViPNet-драйвер. Режимы работы ViPNet-драйвера.	0,75	0,5	0,25		
5.4	Фильтрация: критерии и правила. Виды фильтров. Настройка фильтров. Настройка фильтров для адресатов Защищенной сети. Настройка фильтров для IP-адресов в окне Открытая сеть.	2	0,5		1,5	
5.5	Журнал регистрации IP-трафика.	0,5	0,25	0,25		
5.6	Транспортный модуль MFTP. Виды каналов MFTP.	1		0,5	0,5	
5.7	Деловая почта. Назначение и функциональные возможности программы ViPNet [Деловая Почта]. Работа в Деловой почте.	0,5	0,25		0,25	
	ViPNet [Монитор]. Назначение и функциональные возможности программы ViPNet [Монитор]. Работа в администраторской и пользовательской части программы ViPNet [Монитор].	1	0,5		0,5	
6	**VIPNET [КООРДИНАТОР]**	**6**	**2**	**1,75**	**2,25**	

6.1	Общие сведения, основные функции и назначение программы ViPNet [Координатор].	1	0,5	0,5		
6.2	Логика взаимодействия абонентских пунктов с серверами (ViPNet [Координаторами]) и серверов между собой.	1	0,5	0,5		
6.3	Общие сведения и принцип работы ViPNet [Координатора] как сервер – маршрутизатор и сервер ViPNet-Firewall.	1	0,5	0,25	0,25	
6.4	Функция туннелирования открытого трафика локальной сети. Настройка туннеля и полутуннеля	4			2	
6.5	Назначение системы защиты от сбоев.	0,5	0,25	0,25		
6.6	Правила формирования виртуальных адресов.	0,5	0,25	0,25		
	Сертификационный тест	**2**				**тест**
	ВСЕГО	**40**	**17,5**	**5**	**15,5**	

Негосударственное образовательное учреждение дополнительного профессионального образования
«Ростовский центр повышения квалификации в области информационных технологий и связи

УЧЕБНАЯ ПРОГРАММА

«Администрирование системы защиты информации ViPNet версия 3.2»

1. ВВЕДЕНИЕ

Основным назначением сетевых решений, объединенных торговой маркой ViPNet, является повышение эффективности управления и функционирования предприятия или системы предприятий, использующих средства коммуникации для обмена информацией и управления.

Повышение эффективности достигается путем создания виртуальной частной сети (VPN) с большим количеством сервисных возможностей. Под VPN понимается совокупность компьютеров в локальной сети и Интернет, которые выполняют какие-либо функции в рамках определенной организации, и которые для отдельных потоков информации или целиком должны быть изолированы от других компьютеров. Общепринятым способом построения VPN является установка различных защитных средств на входе локальных сетей, объединяемых в VPN. В продукте ViPNet этот подход сочетается с возможностью установки средств для создания VPN непосредственно на компьютеры, требующие защиты.

В связи с этим подготовка администраторов защищенных сетей является важным и актуальным. В область задач, входящих для обучения технологии администрирования системы защиты информации ViPNet, входит целый перечень вопросов, связанных с созданием, модификацией виртуальных защищенных сетей.

В курсе рассматриваются теоретические и практические вопросы, связанные с созданием и управлением виртуальных защищенных сетей, использованием электронной цифровой подписи и инфраструктуры открытых ключей в прикладных системах организации (электронный документооборот, электронная почта, электронный бизнес), как необходимой основы для их защиты.

Большую часть времени занимают практические занятия слушателей на специальных стендах, позволяющих моделировать различные виды и варианты использования виртуальных защищенных сетей ViPNet.

Курс разработан Отделом учебных программ ОАО "Инфотекс" и может быть рекомендован специалистам структурных подразделений, планирующим (расширяющим) использование технологии VPN и

внедряющим ЭП и элементы PKI в повседневную деятельность сотрудников своих предприятий и организаций, а также специалистам подразделений автоматизации и информационной безопасности, отвечающим за проектирование, развертывание, эксплуатацию и сопровождение (администрирование) виртуальных защищенных сетей ViPNet.

Нормативная трудоемкость Учебной программы составляет 40 академических часов. Форма обучения – очная.

Слушатели, полностью выполнившие программу обучения и успешно

Перечень требований к знаниям, умениям и навыкам слушателей:

Требования к подготовке администратора ViPNet версии 3.2

Предварительная подготовка

. Навыки установки и настройки программного обеспечения в среде Windows, . Навыки администрирования локальных сетей на основе Windows 2000/XP/Vista/7/Server 2008.

В результате обучения

Вы приобретете знания:

- о современном состоянии, тенденциях и перспективах развития в области телекоммуникаций;
- о структуре и организации различных видов телекоммуникаций;
- о строении корпоративной сети с использованием системы ViPNet;
- об общих принципах криптографии и особенностях криптосистемы в продуктах ViPNet;
- о составе ключевой информации;
- о принципах взаимодействия УКЦ и ЦУС;
- о программных модулях системы ViPNet.

Вы сможете:

- создавать и модифицировать защищенные сети по заданным схемам;
- организовывать межсетевое взаимодействие;
- обеспечить взаимодействие всех объектов VPN между собой и функционирования туннеля;
- обеспечивать работу сервера защищенных соединений;
- организовывать взаимодействие между серверами-маршрутизаторами и абонентскими пунктами.

2. ПЕРЕЧЕНЬ ТЕМ

Тема 1. Введение в технологию ViPNet.

Тема 2. Компоненты управления сети ViPNet.

Тема 3. Особенности криптосистемы и ключевой структуры ViPNet.

Тема 4. Организация межсетевого взаимодействия.

Тема 5. Клиентские продукты ViPNet.

Тема 6. Серверные продукты ViPNet.

3. РЕФЕРАТИВНОЕ ОПИСАНИЕ ТЕМ

Тема 1. Введение в технологию ViPNet.

Занятие 1.1. Способы и средства защиты информации. Технология построения виртуальных защищенных сетей (VPN)

1. Основные понятия, термины и определения.
2. Классификация виртуальных защищенных сетей.

Занятие 1.2. Состав программного комплекса ViPNet

1. Элементы управления.
2. Серверная часть.
3. Клиентское программное обеспечение.

Занятие 1.3 Логическая структура сети ViPNet.

1. Логика построения виртуальной защищенной сети ViPNet.
2. Основные виды конфигурации ViPNet-сети.

Тема 2 Компоненты управления сети ViPNet.

Занятие 2.1. Общие сведения, основные функции и назначение программы ViPNet Administrator

1. Состав программы ViPNet Administrator.
2. Основные функции.

Занятие 2.2. Основные функции и принципы работы программного комплексаViPNet StateWatcher.

1. Состав и назначение программного комплекса ViPNet State Watcher.
2. Основные принципы работы.

Занятие 2.3. Система управления ViPNet Policy Manager.

1. Состав и назначение программного комплекса ViPNet Policy Manager.
2. Формирование групп сетевых узлов и назначение политики безопасности.

Занятие 2.4. Состав программного обеспечения ViPNet Administrator. ЦУС и УКЦ.

1. Состав программного обеспечения ПО ViPNet Administrator.

2. Основные функции ЦУС и УКЦ.

Занятие 2.5. Особенности взаимодействия ЦУС и УКЦ.

1. Папки обмена служебными файлами между ЦУС и УКЦ.
2. Установка ЦУС и УКЦ на разные машины.

Занятие 2.6. Основные понятия сетевого уровня.

1. Понятие сетевого узла.
2. Сетевая группа.
3. Сервер-маршрутизатор и абонентский пункт.

Занятие 2.7. Основные понятия прикладного уровня.

1. Коллектив, тип коллектива. Главный коллектив.
2. Связи коллективов.
3. Прикладные задачи.

Занятие 2.8. Разграничение доступа к конфиденциальной информации.

1. Полномочия пользователей.
2. Право подписи.

Тема 3. Особенности криптосистемы и ключевой структуры ViPNet.

Занятие 3.1. Особенности ключевой структуры сети ViPNet.

1. Состав и назначение дистрибутива ключей.
2. Ключи пользователя и ключи узла.
3. Внутрисетевые мастер-ключи.
4. Защита ключей.

Занятие 3.2. Основные технические данные и характеристики криптоядра Домен К.

1. Основные технические данные и характеристики СКЗИ Домен к.
2. Возможности встраивания криптоядра Домен К во внешние приложения.

Занятие 3.3. Этапы формирования ключевой информации.

1. Формирование ключевой информации при первоначальном развертывании сети.
2. Изменение ключевой информации при модификации сети.
3. Компрометация ключей. Действия пользователя и

администраторов при компрометации ключевой информации

Занятие 3.4. Управление ключевой информации в процессе функционирования сетей.

1. Управление ключами в собственной сети.
2. Добавление ключей при появлении новых связей. Удаление ключей при удалении связей.
3. Смена ключей пользователей. Смена ключей узла.
4. Смена ключей подписи.
5. Сертификация новых ключей ЭЦП.
6. Управление ключами при межсетевом взаимодействии.

Занятие 3.5. Последовательность установки и настройки ПО ViPNet.

1. Последовательность установки и настройки ПО.
2. Регистрация узлов и пользователей корпоративной сети, регистрация ЦР внешних пользователей.
3. Формирование защищенных справочников доступа для узлов сети и справочников связей узлов и абонентов для УКЦ при штатной эксплуатации и компрометации ключей пользователей.

Занятие 3.6. Основные действия администратора Ключевого центра.

1. Выполняемые функции.
2. Формирование ключевой информации сети.
3. Смена мастер-ключей.
4. Назначение администратора сети.

Занятие 3.7. Основные действия администратора Удостоверяющего центра.

1. Выполняемые функции.
2. Выпуск сертификатов для внутренних и внешних пользователей.
3. Отзыв, приостановление и возобновление действия сертификата.

Занятие 3.8. Типовые варианты применения технологии ViPNet.

1. Сценарии использовании сети ViPnet для защиты конфиденциальной информации организации.

Тема 4. Организация межсетевого взаимодействия.

Занятие 4.1. Виды межсетевых мастер-ключей (ММК).

1. Индивидуальный симметричный межсетевой мастер ключ, длина ключа, принципы использования.

2. Универсальный симметричный межсетевой мастер ключ.
3. Принципы использования асимметричного межсетевого мастер-ключа.

Занятие 4.2. Развертывание виртуальной защищенной сети заданной конфигурации.

1. Проработка схемы защищенной сети ViPNet.
2. Развертывание виртуальной защищенной сети.

Занятие 4.3. Настройка, управление и модификация защищенной сети ViPNet.

1. Управление защищенной сетью при межсетевом взаимодействии.
2. Модификация защищенной сети при межсетевом взаимодействии.

Тема 5. Клиентские продукты ViPNet.

Занятие 5.1. Общие сведения, основные функции и назначение программы ViPNet Client.

1. Функции ПО ViPNet Client.
2. Состав программного модуля ViPNet Client.
3. Основные режимы использования ViPNet Client.
4. Режимы безопасности в ViPNet Client.

Занятие 5.2. Состав программного обеспечения.

1. Состав программного модуля ViPNet Client.
2. Требования к оборудованию и базовому программному обеспечению.

Занятие 5.3. ViPNet-драйвер. Режимы работы ViPNet-драйвера.

1. Назначение и функции ViPNet-драйвера.
2. Режимы работы ViPNet-драйвера.

Занятие 5.4. Фильтрация: критерии и правила.

1. Виды фильтров.
2. Настройка фильтров.
3. Настройка фильтров для адресатов Защищенной сети.
4. Настройка фильтров для IP-адресов Открытой сети.

Занятие 5.5. Журнал регистрации IP-трафика.

1. Регистрация ip-пакетов.
2. Журнал блокированных ip-пакетов.
3. Настройка журнала ip-пакетов.

Занятие 5.6 Транспортный модуль MFTP. Виды каналов MFTP.

1. Функции транспортного модуля MFTP.
2. Типы каналов MFTP.
3. Настройка работы транспортного модуля по каналу SMTP/POP3.

Занятие 5.7. ViPNet Деловая почта.

1. Назначение и функциональные возможности программы ViPNet Деловая Почта.
2. Работа в Деловой почте.
3. Автопроцессинг.

Занятие 3.8. ViPNet Монитор. Назначение и функциональные возможности программы ViPNet Монитор. Работа в администраторской и пользовательской части программы ViPNet Монитор.

1. Средство управления ViPNet драйвером.
2. Назначение и функциональные возможности программы ViPNet Client Монитор.
3. Работа с правами администратора сетевых узлов.

Занятие 3.9. Состав и назначение криптопровайдера ViPNet CSP.

1. Назначение криптопровайдера ViPNet CSP.
2. Встраивание алгоритмов шифрования и подписания во внешние приложения.

Занятие 3.10. Шифрование и подпись документов с использованием ViPNet CSP.

1. Использование ViPNet CSP для подписания и шифрования документов в MS Outlook.
2. Подписание документов в MS Word.

Тема 6. Серверные продукты ViPNet.

Занятие 6.1. Общие сведения, основные функции и назначение программы ViPNet Coordinator.

1. Функциональный состав программного обеспечения ViPNet.
2. Функции программного модуля ViPNet Coordinator.

Занятие 6.2. Линейка программно-аппаратных комплексов ViPNet Coordinator HW.

1. Программно-аппаратный комплекс ViPNet Coordinator HW 100.
2. Программно-аппаратный комплекс ViPNet Coordinator HW 1000 и HW 2000.
3. ViPNet Coordinator HW-VPNM и NME-RVPN ViPNet.

Занятие 6.3. Логика взаимодействия абонентских пунктов с серверами (ViPNet Coordinator) и серверов между собой.

1. Логика взаимодействия абонентских пунктов с серверами-маршрутизаторами.
3. Взаимодействие серверов между собой.
4. Режимы работы ViPNet Coordinator.

Занятие 6.4. Общие сведения и принцип работы ViPNet Coordinator как сервер – маршрутизатор и сервера ViPNet-Firewall.

1. Функции сервера-маршрутизатора.
2. Функции ViPNet Coordinator как сервера ViPNet-Firewall.

Занятие 6.5. Функция туннелирования открытого трафика локальной сети. Настройка туннеля и полутуннеля.

1. Понятие туннеля и полутуннеля.
2. Функции туннелирования открытого трафика.
3. Настройки туннеля и полутуннеля.

Занятие 6.6. Назначение системы защиты от сбоев.

1. Функции и принципы работы кластера горячего резервирования.
2. Общие принципы работы Windows Cluster.

Занятие 6.7 Правила формирования виртуальных адресов.

1. Принцип назначения виртуальных IP-адресов.
2. Стартовый пул виртуальных адресов.

4. НАИМЕНОВАНИЯ ВИДОВ ЗАНЯТИЙ

В том числе: аудиторная работа		40 ч.
Из них:	лекции	20 ч.
	практ. занятия	20 ч.

Нормативная трудоемкость Учебной программы составляет 40 академических часов.

Форма итогового контроля – сертификационный тест.

Слушатели, полностью выполнившие программу обучения и успешно сдавшие экзамен, получают **Сертификат Администратора ViPNet ver.3.2**.

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО РЕАЛИЗАЦИИ УЧЕБНОЙ ПРОГРАММЫ

Обучение слушателей по настоящей Учебной программе направлено на повышение их квалификации по вопросам администрирования системы защиты информации ViPNet.

Подготовка слушателей проводится по очно-заочной форме (с отрывом от работы) в составе учебной группы. Численность группы - до 25 человек.

Нормативная трудоемкость Учебной программы составляет 40 академических часа аудиторной работы. При этом из общего объема аудиторных занятий 40% составляют лекционные, а 60% семинарские и практические занятия. Общий объем учебной нагрузки в день очного обучения - 8 учебных часов.

В качестве материальной базы использованно учебно-методическое обеспечение и лабораторное оборудование ОАО «"Информационные технологии и коммуникационные системы"» (Далее ОАО «ИнфоТеКС») или аналогичное оборудование на базе заказчика обучения. Компьютерное оборудование включает все необходимое для эксплуатации тренировочного стенда.

По окончании обучения проводиться экзамен, являющийся заключительным этапом изучения настоящей Учебной программы и имеющий цель проверить и оценить уровень полученных знаний, навыки и умения применить полученные знания в решении практических задач.

На сдачу экзамена отводиться по 2 часа на учебную группу. Экзамен проводится в виде электронного теста. Успешным считается результат равный 75% и более.

В основу подготовки специалистов положено изучение различных аспектов функционирования системы защиты информации ViPNet версии 3.2.

Использованы следующие основные виды учебных занятий: лекцию, семинар и лабораторное занятие.

На лекциях даются основы знаний по изучаемым вопросам, детально изучается законодательная база и требования нормативных документов. В ходе занятий раскрываются наиболее сложные вопросы учебного материала, уделяя особое внимание их творческому осмыслению.

Семинары проводятся по основным и наиболее сложным темам в целях углубления и закрепления знаний слушателей, полученных ими на лекциях и в процессе самостоятельной работы над учебным материалом.

На семинарских и практических занятиях слушателям прививаются практические навыки. Для повышения эффективности практических занятий преподаватель заранее выдает слушателям задания на практические занятия.

На семинарских (практических) занятиях отводится время для проверки знаний и навыков слушателей по пройденному материалу и усвоению изучаемой темы.

В целях повышения эффективности учебного процесса широко используются схемы, макеты, реальная аппаратура, образцы установленных форм документов и другие наглядные пособия.

4. Самостоятельная работа
Контрольные вопросы

1. Из каких модулей состоит ViPNet Custom?
2. Назовите основные функции ЦУС и УКЦ.
3. Что является единицей разграничения доступа в защищенной сети ViPNet?
4. Где задаются полномочия (права доступа) для работы с программой ViPNet?
5. Из чего состоит идентификатор коллектива?
6. Из чего состоит идентификатор типа коллектива?
7. Для каких прикладных задач задаются полномочия?
8. В какой ПЗ задается уровень полномочий для работы с программой «Деловая почта»?
9. В какой ПЗ устанавливается уровень полномочий для работы с ViPNet-драйвером?
10. Что происходит при нажатии кнопки «Сформировать все справочники» в ЦУС?
11. Что такое сетевой узел?
12. Уполномоченное лицо в Удостоверяющем и Ключевом Центре – зачем оно?
13. Что содержится в dst-файле?
14. Что находится в файле ключей пользователя?
15. Для чего служат ключи узла?
16. Для чего служат файлы, входящие в состав КП?
17. При смене имени пользователя в ЦУСе в УКЦ все пункты, отвечающие за генерацию ключей, отключены. Почему?
18. Зачем при установке ЦУС и УКЦ на рабочее место администратора устанавливается ViPNet Client?
19. Вы – администратор. Что делать, если посланное обновление не прошло?
20. Что делать, если пароль на вход в УКЦ утерян?
21. Что изменится в файле-дистрибутиве отдельного АП при связывании его с новым СУ?
22. Для чего в ЦУСе при рассылке обновлений можно выбирать конкретное время принятия обновлений?
23. Что такое «Откат» в журнале запросов и ответов?
24. В каком случае для передачи данных используется протокол IP/241, а в каком случае IP/UDP?
25. Какие подзадачи регистрируются в ПЗ «Сервер IP-адресов»?

26. Какой атрибут в «Журнале запросов и ответов» свидетельствует о вступлении обновлений на АП и СМ в силу?
27. Что нужно сделать в ЦУС, чтобы заново начать генерацию dst-файлов?
28. Как проводится процедура смены мастер-ключа?
29. Где хранится Мастер-Ключ?
30. Назовите уровни ключей защиты, которые используются в СКЗИ «Домен-К».
31. Что такое номер ключа и вариант ключа?
32. Чем защищают ключи узла каждого пользователя защищенной сети?
33. Какие ключи ЭП и какой длины находятся в файле ключей пользователя?
34. Какие ГОСТы используются для работы с ключами шифрования и ЭП?
35. Какая хэш-функция используется для формирования парольных ключей?
36. Какие виды шифрования используются в ПО ViPNet?
37. Что будет, если сменить ключи подписи Уполномоченного лица?
38. Нужно ли создавать новый мастер-ключ при удалении или добавлении нового пользователя защищенной сети?
39. Какие запросы на сертификаты можно сделать в УКЦ?
40. В чём различия сетевой, иерархической и «мостовой» моделей установления доверительных отношений между УЦ?
41. Какую ключевую информацию должен пересоздать Администратор УКЦ при изменении Списка Отозванных Сертификатов (СОС)?
42. Какие программные модули комплекса ViPNet CUSTOM используются при построении иерархических структур Удостоверяющих Центров? Каковы их функции?
43. Можно ли установить в рамках одной ViPNet-сети два ПО ViPNet-Администратора (два ЦУСа и два УКЦ) для управления этой ViPNet-сетью?
44. Что такое компрометация ключей? Какие события с ней связаны?
45. Какую ключевую информацию необходимо обновить при компрометации ключей пользователя?
46. По какому каналу Администратор УКЦ должен передать пользователю обновление ключевой информации в связи с компрометацией ключей пользователя?
47. Каков порядок действий при компрометации ключей УКЦ?
48. Как выбрать шаблон для создания сертификата ЭЦП пользователя? Каков порядок действий Администратора УКЦ при издании сертификата пользователя?
49. Где фиксируются все события по работе с УКЦ и как их просмотреть?
50. Требуется ли при связывании двух защищённых сетей ViPNet заново генерировать основной мастер-ключ?

51. Какого типа может быть межсетевой мастер-ключ? В каких случаях используется каждый отдельный тип ММК?
52. Требуется ли генерация индивидуального симметричного межсетевого мастер-ключа при связывании двух защищенных сетей асимметричным межсетевым мастер-ключом?
53. Зачем нужен шлюз в защищенной сети ViPNet при установке межсетевого взаимодействия?
54. Что должен сделать администратор при смене асимметричного межсетевого мастер-ключа?
55. Где хранится асимметричный межсетевой мастер-ключ?
56. Для чего необходим экспорт ЭЦП уполномоченного лица при установлении межсетевого взаимодействия?
57. Что такое плановая смена ММК и каковы действия Администраторов сетей при подобной смене ключей?
58. Для чего нужен пароль для импорта ММК, и можно ли от него отказаться?

3. ПЕРЕЧЕНЬ РАЗДАТОЧНЫХ МАТЕРИАЛОВ

1. Чефранова А.О., Кабакова Н.В., Уривский В.А., Алабина Ю.Ф. Система защиты информации ViPNet: курс лекций. – М.: Горячая линия – Телеком, 2014.
2. Чефранова А.О., Кабакова Н.В., Алабина Ю.Ф. Система защиты информации ViPNet: практикум. – М.: Горячая линия – Телеком, 2014.
3. CD с учебными материалами и программным обеспечением.