ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ "ЦЕНТР ОБУЧЕНИЯ "СПЕЦИАЛИСТ" УНЦ ПРИ МГТУ ИМ. Н.Э. БАУМАНА
(ОЧУ ДПО «СПЕЦИАЛИСТ»)
123317, г. Москва, Пресненская набережная, д 8, стр. 1, этаж 48, помещение 484с, комната 3,
ИНН 7701168244, ОГРН 1127799002990

Утверждаю:
Директор ОЧУ ДПО «Специалист»

_____/Е.В.Добрыднева/
«01» февраля 2018 года

Дополнительная профессиональная программа повышения квалификации « Linux (CentOS/Debian)/FreeBSD. Уровень 3. Обеспечение безопасности систем, сервисов и сетей»

город Москва

Программа разработана в соответствии с приказом Министерства образования и науки Российской Федерации от 1 июля 2013 г. N 499 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам".

Повышение квалификации слушателей, осуществляемое в соответствии с программой, проводится с использованием модульного принципа построения учебного плана с применением различных образовательных технологий, в том числе дистанционных образовательных технологий и электронного обучения в соответствии с законодательством об образовании.

Дополнительная профессиональная программа повышения квалификации, разработана образовательной организацией в соответствии с законодательством Российской Федерации, включает все модули, указанные в учебном плане.

Содержание оценочных и методических материалов определяется образовательной организацией самостоятельно с учетом положений законодательства об образовании Российской Федерации.

Структура дополнительной профессиональной программы соответствует требованиям Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утвержденного приказом Минобрнауки России от 1 июля 2013 г. N 499.

Объем дополнительной профессиональной программы вне зависимости от применяемых образовательных технологий, должен быть не менее 16 академических часов. Сроки ее освоения определяются образовательной организацией самостоятельно.

Формы обучения слушателей (очная, очно-заочная, заочная) определяются образовательной организацией самостоятельно.

К освоению дополнительных профессиональных программ допускаются:

- лица, имеющие среднее профессиональное и (или) высшее образование;
- лица, получающие среднее профессиональное и (или) высшее образование.

Для определения структуры дополнительной профессиональной программы и трудоемкости ее освоения может применяться система зачетных единиц. Количество зачетных единиц по дополнительной профессиональной программе устанавливается организацией.

Образовательная деятельность слушателей предусматривает следующие виды учебных занятий и учебных работ: лекции, практические и семинарские занятия, лабораторные работы, круглые столы, мастер-классы, мастерские, деловые игры, ролевые игры, тренинги, семинары по обмену опытом, выездные занятия, консультации, выполнение аттестационной, дипломной, проектной работы и другие виды учебных занятий и учебных работ, определенные учебным планом.

Аннотация.

Материал курса позволяет получить ключевые знания по обеспечению комплексной безопасности сетевой инфраструктуры, что позволит значительно уменьшить риск взлома сетей и сервисов предприятия или минимизировать последствия такого инцидента. Уникальной особенность курса являются лабораторные работы, позволяющие слушателям побывать по обе стороны «баррикад» - в роли хакеров и в роли администраторов безопасности сети. На занятиях слушатели будут производить сканирования, атаки, перехваты конфиденциальной информации, чтобы, впоследствии, научиться защищать системы от таких действий. Будет продемонстрирована уязвимость некоторых распространенных решений и предложены альтернативные и безопасные варианты. Все лабораторные работы максимально адаптированы под реальные условия, и легко могут быть перенесены в настоящую сеть предприятия.

1. Цель программы:

Данный курс предназначен для системных администраторов, которым требуется обеспечить комплексную безопасность сетевой инфраструктуры средствами свободного программного обеспечения (СПО), работающего под управлением систем Linux/FreeBSD, а также, для тех, кто планирует освоить смежную компетенцию специалиста по информационной безопасности.

Планируемый результат обучения:

Лица, успешно освоившие программу, должны овладеть следующими компетенциями:

Совершенствуемые компетенции

№	Компетенция	Направление подготовки ФГОС ВО ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 09.03.04 «ПРОГРАММНАЯ ИНЖЕНЕРИЯ (УРОВЕНЬ БАКАЛАВРИАТА) Код компетенции
1	Владение навыками использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения методов и языков формальных спецификаций, систем управления базами данных	ПК-2
2	Владение концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества	ПК-4

Совершенствуемые компетенции в соответствии с трудовыми фикциями профессионального стандарта «СИСТЕМНЫЙ АДМИНИСТРАТОР ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ», утвержденного приказом Минтруда и социальной защиты РФ от 05 октября 2015 г. N 684н

№	Компетенция	Направление подготовки Трудовые функции (код)
	ОТФ	ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ «СИСТЕМНЫЙ АДМИНИСТРАТОР ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ» Утвержден приказом Минтруда России от 05.10.2015 N 893н» (Зарегистрировано в Минюсте России 19 октября 2015 г. N 39361) Наименование вида ПД: Обеспечение требуемого качественного бесперебойного режима работы инфокоммуникационной системы
А	Администрирование структурированной	Документирование инфраструктуры СКС и ее составляющих А/01.4

	кабельной системы (СКС)	Мониторинг СКС с целью локализации неисправностей A/02.4
B	Администрирование прикладного программного обеспечения инфокоммуникационной системы организации	Установка прикладного программного обеспечения B/01.5
		Оценка критичности возникновения инцидентов при работе прикладного программного обеспечения B/02.5
		Оптимизация функционирования прикладного программного обеспечения B/03.5
		Интеграция прикладного программного обеспечения в единую структуру инфокоммуникационной системы B/04.5
		Реализация регламентов обеспечения информационной безопасности прикладного программного обеспечения B/05.5
		Разработка нормативно-технической документации на процедуры управления прикладным программным обеспечением B/06.5
		Разработка требований к аппаратному обеспечению и поддерживающей инфраструктуре для эффективного функционирования прикладного программного обеспечения B/07.5
C	Управление программно-аппаратными средствами информационных служб инфокоммуникационной системы организации	Установка персональных компьютеров, учрежденческой автоматической телефонной станции (УАТС), подключение периферийных и абонентских устройств C/01.6
		Управление доступом к программно-аппаратным средствам информационных служб инфокоммуникационной системы C/02.6
		Мониторинг событий, возникающих в процессе работы инфокоммуникационной системы C/03.6

		Восстановление работоспособности программно-аппаратных средств инфокоммуникационной системы и/или ее составляющих после сбоев C/04.6
		Протоколирование событий, возникающих в процессе работы инфокоммуникационной системы C/05.6
		Ввод в эксплуатацию аппаратных, программно-аппаратных и программных средств инфокоммуникационной инфраструктуры совместно с представителями поставщиков оборудования C/06.6
		Обслуживание периферийного оборудования C/07.6
		Организация инвентаризации технических средств C/08.6
D	Администрирование сетевой подсистемы инфокоммуникационной системы организации	Настройка сетевых элементов инфокоммуникационной системы D/01.6
		Контроль использования ресурсов сетевых устройств и программного обеспечения D/02.6
		Управление безопасностью сетевых устройств и программного обеспечения D/03.6
		Диагностика отказов и ошибок сетевых устройств и программного обеспечения D/04.6
		Контроль производительности сетевой инфраструктуры инфокоммуникационной системы D/05.6
		Проведение регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы D/06.6
E	Администрирование систем управления базами данных инфокоммуникационной системы организации	Инсталляция (установка) системы управления базой данных (СУБД) E/01.7
		Мониторинг работы СУБД E/02.7

		Настройка систем резервного копирования и восстановления баз данных E/03.7
F	Администрирование системного программного обеспечения инфокоммуникационной системы организации	Установка системного программного обеспечения F/01.7
		Оптимизация работы дисковой подсистемы (подсистемы ввода-вывода) F/02.7
		Администрирование файловых систем F/03.7
		Оценка критичности возникновения инцидентов для системного программного обеспечения F/04.7
		Реализация регламентов обеспечения информационной безопасности системного программного обеспечения инфокоммуникационной системы организации F/05.7
G	Управление развитием инфокоммуникационной системы организации	Анализ системных проблем обработки информации на уровне инфокоммуникационной системы G/01.7
		Подготовка предложений по развитию инфокоммуникационной системы G/02.7
		Разработка нормативной и технической документации на аппаратные средства и программное обеспечение G/03.7
		Контроль обновления версий аппаратных, программно-аппаратных и программных средств G/04.7

Планируемый результат обучения:

Лица, успешно освоившие программу, должны овладеть следующими компетенциями: Владение навыками использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения методов и языков формальных спецификаций, систем управления базами данных.

После окончания обучения Слушатель будет знать:

- Теорию и практику использования средств криптографической защиты;
- Правила размещения информационных ресурсов в сети предприятия;
- Особенности настройки сервисов предприятия с точки зрения безопасности;

- Современные средства изоляции/контейнеризации и управления ресурсами сервисов;

После окончания обучения Слушатель будет уметь:

- Использовать сканеры для оценки безопасности систем, сервисов и сетей;
- Использовать механизмы защиты систем от вредоносных действий пользователей и скомпрометированного ПО;
- Осуществлять настройку сервисов сети предприятия с точки зрения безопасности и конфиденциальности данных;
- Разворачивать удостоверяющий центр предприятия;
- Использовать сертификаты для идентификации пользователей и шифрования трафика;
- Безопасным способом связывать в единую сеть несколько филиалов;
- Безопасным способом предоставлять доступ к сетевым ресурсам предприятия удаленным пользователям;
- Осуществлять активную защиту периметра сети с помощью систем IDS и IPS;
- Проводить аудит систем сервисов и сетей предприятия с точки зрения безопасности.

Учебный план:

Категория слушателей: Данный курс предназначен для системных администраторов, которым требуется обеспечить комплексное развитие инфраструктуры сети предприятия с использованием средств свободного программного обеспечения (СПО), работающего под управлением систем Linux а также, для тех, кто планирует освоить смежную компетенцию специалиста по информационной безопасности.

Требования к предварительной подготовке:

Знакомство с администрированием систем Linux или FreeBSD;
Знакомство с администрированием сервисов и сетей Linux или FreeBSD.

Рекомендуемая подготовка:

Успешное окончание курса «Linux (CentOS/Debian). Уровень 2. Администрирование сервисов и сетей», или эквивалентная подготовка.

Знание английского языка на уровне необходимом для чтения профессиональной литературы.

Срок обучения: 36 академических часов, в том числе 24 аудиторных с преподавателем.
Самостоятельные занятия (СРС): предусмотрены (12 час.).
Форма обучения: очная, очно-заочная, заочная. По желанию слушателя форма обучения может быть изменена и/или дополнена.
Режим занятий: дневной, вечерний, группы выходного дня.

№ п/п	Наименование модулей по программе	Общая трудоемкость (акад. часов)	В том числе аудиторных			СРС	Форма ПА [1]
			Всего	Лекций	Практических занятий		
1	Модуль 1: Периметры безопасности и размещение сервисов в сети предприятия	6	4	2	2	2	Практическая работа
2	Модуль 2: Анализ информационных систем предприятия с точки зрения безопасности	6	4	2	2	2	Практическая работа
3	Модуль 3: Защита систем предприятия на уровне ОС	6	4	2	2	2	Практическая работа
4	Модуль 4: Защита сервисов предприятия	6	4	2	2	2	Практическая работа
5	Модуль 5: Защита сети предприятия	6	4	2	2	2	Практическая работа
6	Модуль 6: Использование VPN в сети предприятия	6	4	2	2	2	Практическая работа
	Итого:	**36**	**24**	**12**	**12**	**12**	
	Итоговая аттестация	Тестирование/выполнение задания					

Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут. Количество аудиторных занятий при очно-заочной форме обучения составляет 20-25% от общего количества часов.

Форма Промежуточной аттестации – см. в ЛНА «Положение о проведении промежуточной аттестации слушателей и осуществлении текущего контроля их успеваемости» п.3.3.

2. Календарный учебный график

Календарный учебный график формируется при осуществлении обучения в течение всего календарного года. По мере набора групп слушателей по программе составляется календарный график, учитывающий объемы лекций, практики, самоподготовки, выезды на объекты.

[1] ПА – промежуточная аттестация

Неделя обучения	1	2	3	4	5	6	7	Итого часов
	пн	вт	ср	чт	пт	сб	вс	
1 неделя	3	3	-	-	-	-	-	6
СРС	2	2	-	-	-	-	-	4
2 неделя	2	2	-	-	-	-	-	4
СРС	3	3	-	-	-	-	-	6
3 неделя	2	2	-	-	-	-	-	4
СРС	3	3	-	-	-	-	-	6
4 неделя	2	2	-	-	-	-	-	4
СРС	2	2	-	-	-	-	-	4
5 неделя	2	4ИА	-	-	-	-	-	6
СРС	2	2	-	-	-	-	-	4
Итого:	23	25	-	-	-	-	-	24/12

3. Рабочие программы учебных предметов

Модуль 1: Периметры безопасности и размещение сервисов в сети предприятия

- Обзор моделей безопасности и обязанностей администратора безопасности компьютерной сети.
- Выбор конфигурации сети предприятия
- Разделение сервисов сети предприятия с точки зрения аудитории

Модуль 2: Анализ информационных систем предприятия с точки зрения безопасности

- Методы анализа безопасности сети и сервисов предприятия

Модуль 3: Защита систем предприятия на уровне ОС

- Обзор технологий повышающих безопасность систем на уровне ОС
- Аудит состояния систем с точки зрения безопасности

Модуль 4: Защита сервисов предприятия

- Методы защиты сетевых сервисов от вредоносных действий

Модуль 5: Защита сети предприятия

- Обзор решений пассивной и активной защиты периметра сети предприятия

Модуль 6: Использование VPN в сети предприятия

- Варианты организации сетей VPN

4. Организационно-педагогические условия

Соблюдение требований к кадровым условиям реализации дополнительной профессиональной программы:

а) преподавательский состав образовательной организации, обеспечивающий образовательный процесс, обладает высшим образованием и стажем преподавания по изучаемой тематике не менее 1 года и (или) практической работы в областях знаний, предусмотренных модулями программы, не менее 3 (трех) лет;

б) образовательной организацией наряду с традиционными лекционно-семинарскими занятиями применяются современные эффективные методики преподавания с применением интерактивных форм обучения, аудиовизуальных средств, информационно-телекоммуникационных ресурсов и наглядных учебных пособий.

Соблюдение требований к материально-техническому и учебно-методическому обеспечению дополнительной профессиональной программы:

а) образовательная организация располагает необходимой материально-технической базой, включая современные аудитории, библиотеку, аудиовизуальные средства обучения, мультимедийную аппаратуру, оргтехнику, копировальные аппараты. Материальная база соответствует санитарным и техническим нормам и правилам и обеспечивает проведение всех видов практической и дисциплинарной подготовки слушателей, предусмотренных учебным планом реализуемой дополнительной профессиональной программы.

б) в случае применения электронного обучения, дистанционных образовательных технологий каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронной информационно-образовательной среде, содержащей все электронные образовательные ресурсы, перечисленные в модулях дополнительной профессиональной программы.

5. Формы аттестации и оценочные материалы

Образовательная организация несет ответственность за качество подготовки слушателей и реализацию дополнительной профессиональной программы в полном объеме в соответствии с учебным планом.

Оценка качества освоения дополнительной профессиональной программы слушателей включает текущий контроль успеваемости, промежуточную и итоговую аттестацию.

Промежуточная аттестация проводится в форме выполнения практических работ и/или тестирования, к итоговой аттестации допускаются слушатели, выполнившие все практические работы.

Результаты итоговой аттестации слушателей ДПП в соответствии с формой итоговой аттестации, установленной учебным планом, выставляются по двух бальной шкале («зачтено»/«не зачтено»), «зачтено» - не менее 70% правильных ответов.

Слушателям, успешно освоившим дополнительную профессиональную программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации.

Слушателям, не прошедшим итоговой аттестации или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть дополнительной профессиональной программы и (или) отчисленным из образовательной организации, выдается справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому образовательной организацией.

Итоговая аттестация проводится по форме выполнения задания и/или тестирования в соответствии с учебным планом. Результаты итоговой аттестации заносятся в соответствующие документы.

<u>Промежуточная аттестация:</u>

№п/п	***Тематика практического занятия***	***Форма ПА***
Модуль 1.	Развертывание шлюза и сетей предприятия	Практическая работа

Модуль 2.	Использование сканеров безопасности	Практическая работа
Модуль 3.	Аудит состояния и защита систем предприятия	Практическая работа
Модуль 4.	Защита сетевых сервисов предприятия	Практическая работа
Модуль 5.	Защита периметра сети предприятия	Практическая работа
Модуль 6.	Управление доступом к внутренним ресурсам сети предприятия	Практическая работа

Итоговая аттестация (выполнение задания):

Вопрос 1

Сайт с информацией о деятельности предприятия следует расположить

Выберите один ответ:

в сети DMZ

в локальной сети

в managment сети

Вопрос 2

Файловый сервер предприятия следует расположить

Выберите один ответ:

в сети DMZ

в локальной сети

в managment сети

Вопрос 3

Рекурсивный кэширующий DNS сервер предприятия следует расположить

Выберите один ответ:

в сети DMZ

в локальной сети

в managment сети

Вопрос 4

Авторитетный DNS сервер, отвечающий за домен предприятия, следует расположить

Выберите один ответ:

в сети DMZ

в локальной сети

в managment сети

Вопрос 5

Контроллер домена предприятия, следует расположить

Выберите один ответ:

в сети DMZ

в локальной сети

в managment сети

Вопрос 6

Почтовый сервер предприятия следует расположить

Выберите один ответ:

в сети DMZ

в локальной сети

в managment сети

Вопрос 7

Систему мониторинга оборудования предприятия следует расположить

Выберите один ответ:

в сети DMZ

в локальной сети

в managment сети

Вопрос 8

Удостоверяющий центр предприятия следует расположить

Выберите один ответ:

в сети DMZ

в локальной сети

в managment сети

Вопрос 9

Выберите верное утверждение: разрешено устанавливать соединения

Выберите один ответ:

из сети DMZ в сеть WAN

из сети DMZ в сеть LAN

из сети WAN в сеть LAN

Вопрос 10

Выберите верное утверждение: запрещено устанавливать соединения

Выберите один ответ:

из сети DMZ в сеть WAN

из сети DMZ в сеть LAN

из сети LAN в сеть DMZ

Анализ информационных систем предприятия с точки зрения безопасности

Вопрос 11

Какой пакет используется для сканирования открытых портов системы?

Выберите один ответ:

nmap

ettercap

john the ripper

chkrootkit

Вопрос 12

Какой пакет используется для перехвата трафика между системами?

Выберите один ответ:

nmap

ettercap

john the ripper

chkrootkit

Вопрос 13

Какой пакет используется для взлома паролей?

Выберите один ответ:

nmap

ettercap

john the ripper

chkrootkit

Вопрос 14

Какой пакет используется для поиска закладок в системе?

Выберите один ответ:

nmap

ettercap

john the ripper

chkrootkit

Вопрос 15

Какой пакет используется для сканирования системы на наличие уязвимостей?

Выберите один ответ:

tripwire

openvas

tcpdump

auditd

Вопрос 16

Какой пакет используется для поиска изменений в системе?

Выберите один ответ:

tripwire

openvas

tcpdump

auditd

Вопрос 17

Какой пакет используется для анализа сетевого трафика в системе?

Выберите один ответ:

tripwire

openvas

tcpdump

auditd

Вопрос 18

Какой пакет используется для анализа событий в системе?

Выберите один ответ:

tripwire

openvas

tcpdump

auditd

Защита систем предприятия на уровне ОС

Вопрос 19

Какая из перечисленных технологий позволяет реализовать принудительный контроль доступа?

Выберите один ответ:

UNIX права доступа

UNIX ACL

Linux LSM

Вопрос 20

Какая из перечисленных технологий позволяет реализовать принудительный контроль доступа?

Выберите один ответ:

UNIX права доступа

UNIX ACL

FreeBSD MAC

Вопрос 21

Какая из перечисленных технологий реализует избирательный контроль доступа?

Выберите один ответ:

UNIX права доступа

FreeBSD MAC

Linux LSM

Вопрос 22

Какая из перечисленных технологий реализует избирательный контроль доступа?

Выберите один ответ:

UNIX ACL

FreeBSD MAC

Linux LSM

Вопрос 23

Какая из перечисленных технологий не использует LSM?

Выберите один ответ:

AppArmor

FreeBSD MAC

SELinux

Вопрос 24

Какой режим профиля AppArmor используется для отладки?

Выберите один ответ:

complain

enforce

disable

Вопрос 25

Какой режим профиля AppArmor используется для ограничения приложения?

Выберите один ответ:

complain

enforce

disable

Вопрос 26

Какое утверждение верно для меток модуля mls системы безопасности FreeBSD MAC?

Выберите один ответ:

процесс с меткой большего значения не может читать файл с меткой меньшего значения

процесс с меткой большего значения не может писать в файл с меткой меньшего значения

Вопрос 27

Какое утверждение верно для меток модуля biba системы безопасности FreeBSD MAC?

Выберите один ответ:

процесс с меткой большего значения не может читать файл с меткой меньшего значения

процесс с меткой большего значения не может писать в файл с меткой меньшего значения

Вопрос 28

Какой механизм безопасности SELinux используется по умолчанию в дистрибутиве CentOS?

Выберите один ответ:

Type Enforcement

DAC

multi-level security

Вопрос 29

Какая из перечисленных технологий используется для управления ресурсами?

Выберите один ответ:

namespaces

cgroup

Вопрос 30

Какая из перечисленных технологий используется для изоляции процессов?

Выберите один ответ:

namespaces

cgroup

Вопрос 31

Какая из перечисленных технологий не использует namespaces?

Выберите один ответ:

chroot

LXC

Docker

Вопрос 32

Какую из перечисленных технологий безопаснее использовать для реализации VPS?

Выберите один ответ:

chroot

LXC

AppArmor

Вопрос 33

Какую из перечисленных технологий безопаснее использовать для реализации VPS?

Выберите один ответ:

chroot

FreeBSD MAC

FreeBSD Jail

Вопрос 34

Какую из перечисленных технологий удобнее использовать для изоляции приложений?

Выберите один ответ:

chroot

SELinux

Docker

Вопрос 35

В каком дистрибутиве Linux (из перечисленных) удобнее использовать технологии предполагающие накладывание специализированных патчей на ядро?

Выберите один ответ:

Gentoo

Debian

CentOS

Защита сервисов предприятия

Вопрос 36

В каком файле конфигурации определяется соответствие между именем службы и номером порта и протоколом?

Выберите один ответ:

/etc/shells

/etc/protocols

/etc/services

Вопрос 37

В поле shell учетной записи пользователя допустимо использовать

Выберите один ответ:

только командный интерпретатор

любую программу

Вопрос 38

В сервисе SSH не рекомендуется сокрытие версии по причине использования ее клиентскими программами для:

Выберите один ответ:

согласования протоколов

сбора статистики

Вопрос 39

Для какого протокола необходим серверный SSL сертификат?

Выберите один ответ:

ftps

sftp

scp

ftp

Вопрос 40

Выберите верное утверждение: для создания цифровой подписи используется

Выберите один ответ:

закрытый ключ

открытый ключ

сессионный ключ

Вопрос 41

Выберите верное утверждение: для шифрования трафика в SSL/TLS используется

Выберите один ответ:

закрытый ключ

открытый ключ

сессионный ключ

Вопрос 42

Выберите верное утверждение: для шифрования сессионного ключа в SSL/TLS используется

Выберите один ответ:

закрытый ключ

открытый ключ

сессионный ключ

Вопрос 43

Выберите верное утверждение: для расшифровки сессионного ключа используется

Выберите один ответ:

приватный ключ

публичный ключ

сессионный ключ

Вопрос 44

Какой атрибут не содержится в запросе на сертификат?

Выберите один ответ:

Имя владельца

Период действия

Код страны

Вопрос 45

Назовите атрибут, который может не играть роли при проверке серверного сертификата?

Выберите один ответ:

FQDN

Подпись

Период действия

Адрес электронной почты

Вопрос 46

Назовите атрибут, который может не играть роли при использовании PKI в корпоративной переписке по электронной почте?

Выберите один ответ:

Имя владельца

Подпись

Период действия

Адрес электронной почты

Имя компании

Вопрос 47

Выберите правильное продолжение предложения: Файлы стандарта PKCS#12 не используются для хранения

Выберите один ответ:

Приватного ключа

Сертификата

Списка отозванных сертификатов

Сессионного ключа

Вопрос 48

Для ограничения доступа к сервису без включения firewall можно использовать решение

Выберите один ответ:

tcpwrap

fail2ban

portsentry

Вопрос 49

Для защиты сервиса от подбора учетных данных можно использовать решение

Выберите один ответ:

tcpwrap

fail2ban

portsentry

Вопрос 50

В качестве безопасной приманки для злоумышленников можно использовать решение

Выберите один ответ:

tcpwrap

fail2ban

portsentry

Вопрос 51

Выберите наиболее точную формулировку: сервис fail2ban предназначен для

Выберите один ответ:

анализа трафика и блокировки нарушителей

анализа журналов и блокировки нарушителей

анализа журналов и выполнения настроенных действий

Защита сети предприятия

Вопрос 52

Какой модуль пакета netfilter позволяет ограничивать количество одновременных соединений?

Выберите один ответ:

persist table

conntrack

iptables

Вопрос 53

Какой элемент конфигурации пакета pf позволяет ограничивать количество одновременных соединений?

Выберите один ответ:

persist table

conntrack

max-src-conn-rate

Вопрос 54

Выберите наиболее точную формулировку: сервис snort предназначен для

Выберите один ответ:

анализа трафика и протоколирования нарушений

анализа журналов и блокировки нарушителей

Использование VPN в сети предприятия

Вопрос 55

Какой из пакетов не годится для предоставления авторизованного доступа к внутренним ресурсам сети предприятия?

Выберите один ответ:

OpenVPN

OpenSSH

OpenSSL