Министерство образования и науки Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ»

Институт **Компьютерных технологий и защиты информации**

Кафедра **Систем информационной безопасности**

УТВЕРЖДАЮ

Ответственный за ОП

_____ И.В. Аникин

«31» 08 2017 г.

Регистрационный номер 4050-17/130-9

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения промежуточной аттестации обучающихся по дисциплине (модулю) или практике

«Защита информации в системах беспроводной связи»

Индекс по учебному плану: **Б1.В.ДВ.10.02**

Направление подготовки: **10.03.01 «Информационная безопасность»**

Квалификация: **бакалавр**

Профиль: **Комплексная защита объектов информатизации**

Виды профессиональной деятельности: **эксплуатационная, проектно-технологическая, экспериментально-исследовательская, организационно-управленческая**

Заведующий кафедрой СИБ И.В. Аникин

Разработчик: к.т.н., доцент кафедры СИБ Л.А. Александрова

Казань 2017 г.

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

«Защита информации в системах беспроводной связи»

(наименование дисциплины)

Содержание фонда оценочных средств (ФОС) соответствует требованиям федерального государственного стандарта высшего образования (ФГОС ВО) по направлению 10.03.01 «Информационная безопасность», учебному плану направления 10.03.01 «Информационная безопасность».

Разработанные ФОС обладают необходимой полнотой и являются актуальными для оценки компетенций, осваиваемых обучающимися при изучении дисциплины «Защита информации в системах беспроводной связи». Разработанные ФОС полностью соответствуют задачам будущей профессиональной деятельности обучающихся, установленных ФГОС ВО по направлению 10.03.01 «Информационная безопасность». В составе ФОС присутствуют оценочные средства в виде тестовых заданий и контрольных вопросов различного уровня сложности, которые позволяют провести оценку порогового, продвинутого и превосходного уровней освоения компетенций по дисциплине.

ФОС обладают необходимой степенью приближенности к задачам будущей профессиональной деятельности обучающихся.

Существенные недостатки отсутствуют.

Заключение. Учебно-методическая комиссия делает вывод о том, что представленные материалы соответствуют требованиям ФГОС ВО по направлению 10.03.01 «Информационная безопасность» и рекомендуются для использования в учебном процессе.

Рассмотрено на заседании учебно-методической комиссии института КТЗИ от «31» августа 2017 г., протокол № 8.

Председатель УМК института КТЗИ _____ В.В. Родионов

Содержание

ВВЕДЕНИЕ 4

1. ФОРМЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ 5

2. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ 5

3. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ С УКАЗАНИЕМ ЭТАПОВ ИХ ФОРМИРОВАНИЯ В ПРОЦЕССЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ 5

4. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ НА РАЗЛИЧНЫХ ЭТАПАХ ИХ ФОРМИРОВАНИЯ, ОПИСАНИЯ ШКАЛЫ ОЦЕНИВАНИЯ 7

5. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРУ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ 11

6. КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ 13

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ 24

Введение

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Защита информации в системах беспроводной связи» – это комплект методических и контрольно-измерительных материалов, предназначенных для определения уровня сформированности компетенций, оценивания знаний, умений, владений на разных этапах освоения дисциплины для проведения промежуточной аттестации обучающихся по дисциплине.

ФОС ПА является составной частью учебного и методического обеспечения программы специалитета по направлению 10.03.01 «Информационная безопасность».

Задачи ФОС по дисциплине «Защита информации в системах беспроводной связи»:

– оценка запланированных результатов освоения дисциплины обучающимися в процессе изучения дисциплины, в соответствии с разработанными и принятыми критериями по каждому виду контроля;

– контроль и управление процессом приобретения обучающимися необходимых знаний, умений, навыков и формирования компетенций, определенных в ФГОС ВО по направлению подготовки

ФОС ПА по дисциплине «Защита информации в системах беспроводной связи» сформирован на основе следующих основных принципов оценивания:

– пригодности (валидности) (объекты оценки соответствуют поставленным целям обучения);

– надежности (использования единообразных стандартов и критериев для оценивания запланированных результатов);

– эффективности (соответствия результатов деятельности поставленным задачам).

ФОС ПА по дисциплине «Защита информации в системах беспроводной связи» разработан в соответствии с требованиями ФГОС ВО по направлению 10.03.01 «Информационная безопасность» для аттестации обучающихся на соответствие их персональных достижений требованиям поэтапного формирования соответствующих составляющих компетенций и включает контрольные вопросы (или тесты) и типовые задания, необходимые для оценки знаний, умений и навыков, характеризующих этапы формирования компетенций.

1. Формы промежуточной аттестации по дисциплине

Дисциплина «Защита информации в системах беспроводной связи» изучается в 7 семестре при очной форме обучения и завершается промежуточной аттестацией в форме экзамена.

2. Оценочные средства для промежуточной аттестации

Оценочные средства для промежуточной аттестации по дисциплине «Защита информации в системах беспроводной связи» при очной форме обучения.

Таблица 1

Оценочные средств для промежуточной аттестации
(очная форма обучения)

№ п/п	Семестр	Форма промежуточной аттестации	Оценочные средства
1.	7	Экзамен	ФОС ПА

3. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

Перечень компетенций и их составляющих, которые должны быть сформированы при изучении темы соответствующего раздела дисциплины «Защита информации в системах беспроводной связи», представлен в таблице 2.

Таблица 2

Перечень компетенций и этапы их формирования

в процессе освоения дисциплины

№ п/п	Этап формирования (семестр)	Наименование раздела	Код формируемой компетенции (составляющей компетенции)		Форма промежуточной аттестации
1.	7	Раздел 1. Основы защиты информации в компьютерных сетях	ПК-1 ПК-3	ПК-1.З ПК-3.З ПК-1.У ПК-3.У	экзамен
2.	7	Раздел 2. Средства защиты информации в компьютерных сетях	ПК-1 ПК-3	ПК-1.З ПК-3.З ПК-1.У ПК-3.У	экзамен
3	7	Раздел 3. Системы анализа защищенности компьютерных сетей	ПК-1 ПК-3 ПСК-3.4	ПК-1.З, ПК-1.У, ПК-1.В, ПК-3.З, ПК-3.У ПК-3.В, ПСК-3.4.З, ПСК-3.4.У, ПСК-3.4.В	экзамен

4. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описания шкалы оценивания

Показатели и критерии оценивания сформированности компетенций на экзамене, приведены в таблице 3.

Таблица 3

Показатели и критерии оценивания сформированности компетенций на зачете

№ п/п	Этап формирования (семестр)	Код формируемой компетенции (составляющей компетенции)		Критерии оценивания	Показатели оценивания (планируемые результаты обучения)		
					Пороговый уровень	Продвинутый уровень	Превосходный уровень
1.	7	ПК-1 ПК-3 ПСК-3.4	ПК-1.З ПК-1.У ПК-3.З ПК-3.У ПСК-3.4.З ПСК-3.4.У	Теоретические навыки	- Иметь представление об общих основах по вопросам настройки и обслуживания программных, программно-аппаратных и технических средств защиты информации. - Умение выполнять типовые работы по настройке технических и программно-аппаратных средств защиты информации - Иметь представление об основных технологиях администрирования подсистем информационной безопасности - Умение использовать основные информационные	- Владеть общими основами по вопросам установки, настройки и обслуживания программных, программно-аппаратных и технических средств защиты информации. - Умение выполнять типовые работы настройке и обслуживанию технических и программно-аппаратных средств защиты информации - Знание базовых технологий администрирования подсистем информационной безопасности	- Владеть системой знаний по вопросам установки, настройки и обслуживанию программных, программно-аппаратных и технических средств защиты информации. - Умение выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации - Владеть системой знаний о технологиях администрирования подсистем информационной безопасности - Умение применять современные, перспективные информационные технологии

					технологий по вопросам администрирования компьютерных сетей - Знание основ организации аттестации объектов информатизации, в соответствии с нормативными документами - Умение организовать аттестацию объектов информатизации в соответствии с базовыми требованиями сферы информационной безопасности	- Умение применять основные информационные технологии администрирования компьютерных сетей - Знание основ организации и сопровождения аттестации объектов информатизации в соответствии с требованиями сферы информационной безопасности - Умение организовать и сопровождать аттестацию объектов информатизации в соответствии с базовыми требованиями сферы информационной безопасности	администрирования компьютерных сетей - Знание основ организации и сопровождения аттестации объектов информатизации в соответствии с требованиями стандартов сферы информационной безопасности - Умение организовать и сопровождать аттестацию объектов информатизации в соответствии с требованиями стандартов сферы информационной безопасности

2.	7	ПК-1 ПК-3 ПСК-3.4	ПК-1.В ПК-3.В ПСК- 3.4.В	Практические навыки	- Владение базовыми технологиями в сфере проведения работ по настройке технических и программно-аппаратных средств защиты информации - Владение основными понятиями администрирования подсистемами информационной безопасности - Владение основными технологиями организации аттестации объектов информатизации в соответствии с базовыми требованиями сферы информационной безопасности	- Владение основными технологиями проведения работ по настройке и обслуживанию технических и программно-аппаратных средств защиты информации - Владение базовыми технологиями администрирования подсистемами информационной безопасности - Владение основными технологиями организации и сопровождения аттестации объектов информатизации в соответствии с требованиями информационной безопасности	- Владение технологиями проведения работ по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации - Владение современными технологиями администрирования подсистемами информационной безопасности - Владение технологиями организации и сопровождения аттестации объектов информатизации в соответствии требованиями стандартов сферы информационной безопасности

Формирование оценки при промежуточной аттестации по итогам освоения дисциплины зависит от уровня освоения компетенций, которые обучающийся должен освоить по данной дисциплине. Связь между итоговой оценкой и уровнем освоения компетенций (шкала оценивания) представлена в таблице 4.

Таблица 4

Описание шкалы оценивания

Шкала оценивания		Описание оценки в требованиях к уровню и объему компетенций
Словесное выражение	Выражение в баллах	
Отлично	от 86 до 100	Освоен **превосходный** уровень всех компетенций (составляющих компетенций)
Хорошо	от 71 до 85	Освоен **продвинутый** уровень всех компетенций (составляющих компетенций)
Удовлетворительно	от 51 до 70	Освоен **пороговый** уровень всех компетенций (составляющих компетенций)
Неудовлетворительно	до 51	Не освоен **пороговый** уровень всех компетенций (составляющих компетенций)

5. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формирование оценки по результатам текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины «Защита информации в системах беспроводной связи» приведено в таблице 5.

Таблица 5

Формирование оценки по итогам освоения дисциплины

Наименование контрольного мероприятия	Рейтинговые показатели				
	I аттестация	II аттестация	III аттестация	по результатам текущего контроля	по итогам промежуточной аттестации (зачета /экзамена)
Раздел 1. Основы информационной безопасности в сетях связи	**10**			**10**	
Тест текущего контроля по разделу	10			10	
Раздел 2. Обеспечение безопасности в системах подвижной сотовой связи		**10**		**10**	
Тест текущего контроля по разделу		5		5	
Защита лабораторных работ		5		5	
Раздел 3. Обеспечение безопасности в беспроводных системах связи стандарта IEEE 802.11x, IEEE 802.16 (WiFi, WiMax)			**30**	**30**	
Тест текущего контроля по разделу			10	10	
Защита лабораторных работ			20	20	
Промежуточная аттестация (Экзамен):					**50**
– тест промежуточной аттестации по дисциплине					20
– ответы на контрольные вопросы в письменной форме по билетам					**30**

6. Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения дисциплины

6.1. Тестовые задания

Метод перехвата трафика без подключения к беспроводной сети?
Глушение сигналов
Подслушивание
Создание помех в эфире
Сканирование устройств

Методы глушения сигналов в беспроводной сети (уберите лишний ответ)
Атака типа DOS
Атака на порты
Глушение клиентской станции
Глушение базовой станции

Криптографический механизм обеспечения безопасности стандарта 802.11, который разработан с единственным статическим ключом
WPA
WPA2
WEP
TKIP

Процесс определение источника информации, то есть конечного пользователя или устройства (центрального компьютера, сервера, коммутатора, маршрутизатора и т. д.).
Аутентификация,
Идентификация,
Верификация,
Авторизация.

Метод изменения информации таким образом, что прочитать ее не может никто, кроме адресата, который должен ее расшифровать.
Кодирование,
Преобразование,
Растрирование,
Шифрование.

Цифровой код, который может использоваться для шифрования и расшифровки информации, а также для ее подписи.

Преамбула,
Код,
Ключ,
Хэш.

Математический расчет, результатом которого является последовательность битов (цифровой код). Имея этот результат, невозможно восстановить исходные данные, использованные для расчета.
Ключ,
Шифр,
Хэш-функция,
Код.

Методы шифрования при котором применяется один ключ для зашифрования данных и их расшифровки?
Симметричное
Ассиметричное,
Дуплексное,
Симплексное.

Методы шифрования, при котором применяются разные ключи для зашифрования данных и их расшифровки?
Ассиметричное,
Симметричное,
Дуплексное,
Симплексное.

На каком алгоритме основано шифрование WEP?
SHA,
MD5,
CRC,
RC4.

Какие типы шифрования применяются в WEP?
Потоковое шифрование,
Блочное шифрование,
Оба метода,
Не один из методов не верен.

Какую длину имеет вектор инициализации при шифрование WEP?
24 бита,
48 бит,
64 бита,
128 бит.

Методы активных сетевых атак на точки доступа
Повторным использованием вектора инициализации,
Манипуляции битами,
Оба метода не возможны,
Оба метода возможны.

Стандарт IEEE 802.11 с традиционной безопасностью предусматривает два механизма аутентификации беспроводных абонентов:
Назначения идентификатора беспроводной локальной сети и аутентификация абонента по его MAC адресу,
Открытую аутентификацию и аутентификацию по его MAC адресу,
Открытую аутентификацию и аутентификацию с общим ключом,
Аутентификацию с общим ключом и его MAC адресу.

Предусмотрено ли стандартом IEEE 802.11 аутентификация абонента по его MAC-адресу?
Предусмотрено,
Не предусмотрено.

Функция, которую легко рассчитать, но обратное восстановление практически невозможно, так как требует непропорционально больших усилий?
Геометрическая функция,
Алгебраическая функция,
Хэш-функция,

PKI это?
Инфраструктура открытых ключей,
Хэш-функция,
Метод шифрования,
Алгоритм ЭЦП.

Какой метод используют поточное и блочное шифрование в алгоритме wep?
Метод обратной связи,
Метод имитовставки,
Метод электронной кодовой книги,
Метод переснатовки.

К каким видам атаки относится индуктивное вычисление секретного ключа шифрования WEP?
Активные,
Пассивные,
Сквозные.

Предусмотрены ли в алгоритме WEP механизмы управления ключами шифрования?
Предусмотрены,
Не предусмотрены,
Предусмотрены в расширенных версиях.

В чем заключается уязвимость аутентификации по MAC адресу?
У многих устройств MAC адреса могут совпадать,
Злоумышленник может подменить свой MAC адрес на адрес легитимного пользователя,
MAC адрес подключаемого пользователя периодически меняется,
MAC адрес клиенту присваивает подключаемая станция.

Временный протокол целостности ключа реализованный в WPA
AES,
DES,
TKIP,
IDEA.

Какой алгоритм применён в WPA для контроля целостности?
MIC,
MD5,
SHA,
ROOT.

В каких режимах может работать WPA?
Оба ответа не верны,
Оба ответа верны,
Режим Enterprise,
Режим Pre-Shared Key.

Стандарт повышенной безопасности 802.11i
WPA,
WEP,
WEP2,
WPA2.

Использует ли стандарт 802.11i шифрование AES?
Нет,
Да,

AES в стандарте 802.11i является блочным шифром, оперирующий блоками данных по
32 бит,
64 бит,

128 бит,
512 бит.

В каких режимах может работать WPA2?
Режим Pre-Shared Key,
Режим Enterprise,
Оба ответа верны,
Оба ответа не верны.

Архитектура IEEE 802.1x включат в себя следующие обязательные логические элементы (уберите лишний вариант):
Клиент,
Идентификатор,
Аутентификатор,
Сервер аутентификации.

Где находиться аутентификатор?
На подключаемом устройстве,
На Radius сервере,
В сети интернет,
На точке доступа.

Сообщение сервера RADIUS-ACCEPT при аутентификации на точке доступа означает:
Успешную авторизацию клиента на Radius сервере,
Неудачную авторизацию клиента на Radius сервере,
Запрос на переавторизацию,
Запрос на разрыв соединения.

На каком уровне модели OSI работает протокол IPSec?
Канальный,
Сетевой,
Транспортный,
Представления.

На каком уровне модели OSI работает протокол L2TP?
Канальный,
Сетевой,
Транспортный,
Представления.

IDS это?
Протокол передачи данных,
Протокол тунелирования,
Система обнаружения вторжений,

Система реагирования на вторжения

IPS это?
Протокол передачи данных,
Протокол тунелирования,
Система обнаружения вторжений,
Система реагирования на вторжения

Запрос на аутентификацию абонента радиоточки:
Authentication Request,
Authentication Reply,
Association Request,
Association Response.

Подтверждение аутентификации от радиоточки:
Authentication Request,
Authentication Reply,
Association Request,
Association Response.

Фрейм ассоциации от абонента в случае удачной аутентификации:
Authentication Request,
Authentication Reply,
Association Request,
Association Response.

Фрейм подтверждения ассоциации от радиоточки к абоненту:
Authentication Request,
Authentication Reply,
Association Request,
Association Response.

В процессе открытой аутентификации происходит обмен сообщениями двух типов (уберите лишний ответ):
Запрос аутентификации (Authentication Request),
Запрос MAC адреса (MAC Rwquest),
Подтверждение аутентификации (Authentication Response).

Злоумышленник обычно подменяет идентификацию одного из сетевых ресурсов. Когда жертва атаки инициирует соединение, мошенник перехватывает его и затем завершает соединение с требуемым ресурсом, а потом пропускает все соединения с этим ресурсом через свою станцию. При этом, атакующий может посылать информацию, изменять или подслушивать все переговоры и потом расшифровывать их. О каком типе атаки идет речь?

типа MITM (man in the middle, «человек посередине»)
типа MMTM
атака типа DOS

Верно ли утверждение? Глушение клиентской станции дает возможность мошеннику подставить себя на место заглушенного клиента.
Верно,
Не верно.

Криптографические средства применяются для обеспечения целостности и конфиденциальности информации.
В проводных сетях,
В беспроводных сетях,
Варианты а и б.

Устройства беспроводного доступа к сети должны быть
Маленькими,
Переносимыми (КПК, Ноутбуки)
Устойчивыми к погодным условиям
Верны ответы а и б,
Верны ответы б и в.

Цифровой код, который может использоваться для шифрования и расшифровки информации, а также для ее подписи.
Хеш функция,
Ключ шифрования,
Контрольная сумма.

Как называется метод изменения информации таким образом, чтобы прочитать ее никто не смог, кроме адресата, который должен ее расшифровать?
Кодирование,
Хеширование,
Шифрование,
Нормирование.

Криптографические механизмы существуют в виде:
Алгоритма (математической функции),
Секретной величины (ключа),
Не верны оба ответа,
Верны а и б.

Какими из перечисленных типов криптографических функций обеспечивается целостность и конфиденциальность данных?
Симметричным шифрованием,

Асимметричным шифрованием,
Хэш-функциями,
Верны а, б и в.

Верно ли утверждение? Симметричное шифрование называют шифрованием с помощью общего ключа, при котором используются разные, но взаимно дополняющие друг друга ключи и алгоритмы шифрования и расшифровки.
Да, верно,
Нет, не верно.

Общий формат широко распространенного сертификата X.509, включает следующие элементы: (выбрать лишнее).
Номер версии;
Серийный номер сертификата;
Эмитент информации об алгоритме;
Эмитент сертификата;
Даты начала и окончания действия сертификата;
Информацию об алгоритме общего ключа субъекта сертификата;
Закрытый ключ.

Ядро алгоритма RC4 (Rivest's Cipher v.4, код Ривеста) состоит из:
Функции генерации ключевого потока,
Функции инициализации,
Функции сложения по модулю два,
Верны только а и б,
Верны а, б и в.

Атаки на зашифрованные данные с помощью технологии WEP можно подразделить на методы:
Активные сетевые атаки,
Пассивные сетевые атаки,
Верны а и б.

Верно ли утверждение? SSID ни в коей мере не обеспечивает конфиденциальность данных, равно как и не аутентифицирует абонента по отношению к точке радиодоступа беспроводной локальной сети.
Да, верно,
Нет, не верно.

При открытой аутентификации возможен доступ любого абонента к беспроводной локальной сети.
Утверждение верно,
Утверждение не верно.

В процессе открытой аутентификации происходит обмен сообщениями двух типов:
Запрос аутентификации (Authentication Request),
Отказ в аутентификации,
Подтверждение аутентификации (Authentication Response),
Верны а и б,
Верны а и в.

Выберите правильное утверждение:
Открытая аутентификация позволяет точке радиодоступа определить, является ли абонент легитимным или нет,
Открытая аутентификация не позволяет точке радиодоступа определить, является ли абонент легитимным или нет.

Основные усовершенствования, внесенные протоколом TKIP(выберите неверный ответ):
Пофреймовое изменение ключей шифрования. WEP - ключ быстро изменяется, и для каждого фрейма он другой,
Контроль целостности сообщения. Обеспечивается эффективный контроль целостности фреймов данных с целью предотвращения проведения тайных манипуляций с фреймами и воспроизведения фреймов,
Встроенный модуль шифрования,
Усовершенствованный механизм управления ключами.

WPA может работать в двух режимах (выберите лишнее)
Enterprise (корпоративный),
Pre-Shared Key (персональный),
Limited (ограниченный).

Приведите в соответствие режим с его описанием.
1. Enterprise (корпоративный),
2. Pre-Shared Key (персональный),
А Хранение базы данных и проверка аутентичности по стандарту 802.1x в больших сетях осуществляются специальным RADIUS сервером.
Б Этот режим предполагает введение одного пароля на каждый узел беспроводной сети,
1 соответствует А, 2 соответствует Б,
1 – Б, 2 – А
1 – А и Б.
Нет верных ответов

Архитектура IEEE 802.1x включат в себя следующие обязательные логические элементы (выберите лишнее):
Клиент (Supplicant) – находится в операционной системе абонента,

Аутентификатор (Authenticator) - находится в программном обеспечении точки радиодоступа,
Сервер аутентификации (Authentication Server) - находится на RADIUS-сервере,
Верны ответы а и б,
Верны все ответы.

Оценка практических умений и навыков:

Даны две точки доступа D-Link AP2100, рабочее место с ПК и инструкция пользователя.

Задание: Создайте мостовое соединение по протоколу WDS.
Для этого:

1. Сбросьте настройки точек доступа к заводским.

2. Задайте соответствующие диапазоны IP адресов.

3. Обеспечьте прозрачность передачи данных по мосту.

4. Решите задачу фильтрации по mac адресам.

5. Протестируйте мостовое соединение измерьте среднюю скорость передачи данных при расстояниях прямой видимости 3-5 метров и 15-20 метров.

6. Результаты работы занесите в отчёт.

6.2. Контрольные вопросы

1. Методы воздействия на сети Wi-Fi
2. Механизм шифрования WEP
3. Алгоритм инициализации RC4
4. Потоковое шифрование WEP
5. Блочное шифрование WEP
6. Вектор инициализации (IV)
7. Шифрования с обратной связью WEP
8. Уязвимость в WEP, пассивные сетевые атаки
9. Уязвимость в WEP, активные сетевые атаки
10. Атака: Повторное использование вектора инициализации (Алгоритм)
11. Атака: Манипуляция битами (алгоритм)

12. Принцип аутентификации абонента в IEEE 802.11
13. Открытая аутентификация и Аутентификация по MAC-адресу
14. Аутентификация с общим ключом
15. Уязвимость открытой аутентификации и аутентификации по MAC-адресу
16. Уязвимость аутентификации с общим ключом
17. Спецификация WPA
18. Основные усовершенствования, внесенные протоколом TKIP
19. Пофреймовое изменение ключей шифрования, процесс пофреймового изменения ключа, этапы
20. Механизм шифрования TKIP
21. Процесс дешифрования TKIP, меры противодействия MIC
22. Контроль целостности сообщения, алгоритм Michael
23. Стандарт сети 802.11I с повышенной безопасностью (WPA2), стандарт 802.1X/EAP (ENTERPRISE-режим)
24. Архитектура IEEE 802.1x
25. Механизм аутентификации 802.1x
26. Варианты EAP их описание и характеристики
27. Топологии беспроводных виртуальных сетей
28. Протокол IPSec, Протокол PPTP, Протокол L2TP
29. Системы обнаружения вторжения в беспроводные сети, архитектура систем обнаружения вторжения
30. События, фиксируемые системами обнаружения вторжений и их классификация

Лист регистрации изменений и дополнений

№ п/п	№ страницы внесения изменений	Дата внесения изменения	Краткое содержание изменений (основание)	Ф.И.О., подпись	«Согласовано» заведующий кафедрой, ведущей дисциплину