МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
вычислительной техники
_____ И.Е. Чернецкая
«_21_» ____05____ 20_23_ г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Защита информации
(наименование дисциплины)

09.03.01 Информатика и вычислительная техника,
код и наименование ОПОП ВО

Курск – 2023

1. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 Вопросы для собеседования

Раздел (тема) дисциплины: Основные понятия информационной безопасности.

1. Основные виды и источники атак на информацию.
2. Методы защиты информации.
3. Политики безопасности.
4. Категории информационной безопасности.
5. Понятие криптографии.
6. Криптоанализ.
7. Классификация методов шифрования информации.
8. Разновидности криптоаналитических атак.

Раздел (тема) дисциплины: Исторические шифры.

1. Шифрование моноалфавитными подстановками.
2. Частотный криптоанализ шифров-подстановок.
3. Шифрование полиалфавитными подстановками.
4. Индекс соответствия.
5. Шифрование многопетлевыми полиалфавитными подстановками.
6. Метод Казиски.
7. Шифрование перестановками.
8. Криптоанализ шифров-перестановок.

Раздел (тема) дисциплины: Поточные шифры.

1. Шифрование гаммированием.
2. Методы генерации гаммы.
3. Генераторы псевдослучайных последовательностей.
4. Одноразовая система шифрования

Раздел (тема) дисциплины: Блочные шифры.

1. Построение блочных шифров.
2. Сеть Фейстеля.
3. Стандарт шифрования данных DES.
4. Режимы применения блочных шифров. Электронная кодовая книга.
5. Сцепление блоков шифра.
6. Способы усиления блочных шифров.
7. Конечные поля. Определение и свойства.
8. Операции в конечных полях.
9. Понятие логарифма в конечном поле.
10. Программная реализация операций в конечном поле.
11. Стандарт шифрования данных AES.
12. Шифрование по ГОСТ.

Раздел (тема) дисциплины: Асимметричные криптосистемы.
1. Концепция криптосистемы с открытым ключом.
2. Однонаправленные функции.
3. Криптосистема шифрования данных RSA.
4. Схема шифрования Эль Гамаля.
5. Комбинированный метод шифрования.

Раздел (тема) дисциплины: Электронная цифровая подпись.
1. Однонаправленные хеш-функции.
2. Алгоритм хеширования SHA.
3. Схемы хеширования на основе симметричных блочных алгоритмов.
4. Алгоритм цифровой подписи RSA.
5. Алгоритм цифровой подписи Эль Гамаля.

Раздел (тема) дисциплины: Управление криптографическими ключами.
1. Требования к ключам.
2. Генерация ключей.
3. Хранение ключей.
4. Методы распределение ключей.
5. Протокол Kerberos.
6. Инфраструктура открытого ключа (Public Key Infrastructure).
7. Алгоритм распределения ключей Диффи-Хеллмана.

Раздел (тема) дисциплины: Защита компьютерных сетей.
1. Стек протоколов TCP/IP.
2. Процедуры открытия и закрытия TCP-соединения.
3. Разновидности сетевых атак. DDoS атаки.
4. Сетевые атаки с использованием протокола ICMP. Ping flood.
5. Сетевые атаки с использованием протокола TCP. Syn flood.
6. Межсетевые экраны.
7. Фильтрующий маршрутизатор.
8. Шлюз сетевого уровня.
9. Шлюз прикладного уровня.
10. Основные схемы сетевой защиты на базе межсетевых экранов.
11. Системы обнаружения вторжений.
12. Протокол SSL (Secire Socket Layer).
13. Протокол IPSec.
14. Сети VPN.

Раздел (тема) дисциплины: Администрирование сетей.
1. Логическая структура Active Directory.
2. Проектирование структуры.
3. Физическая структура сети с Active Directory.
4. Доверительные отношения в сетях Windows Server 2003.

5. Управление учетными записями в сетях Windows Server 2003.
6. Групповая политика в сетях Windows Server 2003 (GPO).

Раздел (тема) дисциплины: Безопасность операционных систем.
1. Основные понятия.
2. Разграничение доступа.
3. Разрешения NTFS.
4. Защита от вирусов.

Шкала оценивания: 2 балла за собеседование по разделу.

Критерии оценивания:

2 баллов выставляется обучающемуся, если он принимает активное участие в беседе по большинству обсуждаемых вопросов (в том числе самых сложных); демонстрирует сформированную способность к диалогическому мышлению, проявляет уважение и интерес к иным мнениям; владеет глубокими (в том числе дополнительными) знаниями по существу обсуждаемых вопросов, ораторскими способностями и правилами ведения полемики; строит логичные, аргументированные, точные и лаконичные высказывания, сопровождаемые яркими примерами; легко и заинтересованно откликается на неожиданные ракурсы беседы; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

1 балл выставляется обучающемуся, если он принимает участие в обсуждении не менее 50% дискуссионных вопросов; проявляет уважение и интерес к иным мнениям, доказательно и корректно защищает свое мнение; владеет хорошими знаниями вопросов, в обсуждении которых принимает участие; умеет не столько вести полемику, сколько участвовать в ней; строит логичные, аргументированные высказывания, сопровождаемые подходящими примерами; не всегда откликается на неожиданные ракурсы беседы; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов выставляется обучающемуся, если он не владеет содержанием обсуждаемых вопросов или допускает грубые ошибки; пассивен в обмене мнениями или вообще не участвует в дискуссии; затрудняется в построении монологического высказывания и (или) допускает ошибочные высказывания; постоянно нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

1.2 ПРОИЗВОДСТВЕННЫЕ ЗАДАЧИ

Производственная задача для контроля результатов практической подготовки обучающихся в лабораторной работе № 1:

Зашифровать свои фамилию, имя и отчество шифром прямой замены.

Производственная задача для контроля результатов практической подготовки обучающихся в лабораторной работе № 2:

Зашифровать свои фамилию, имя и отчество шифром Вижинера.

Производственная задача для контроля результатов практической подготовки обучающихся в лабораторной работе № 3:

Производственная задача №4 (для контроля результатов практической подготовки обучающихся в лабораторной работе № 4):

Установите сервер виртуальной частной сети (VPN).

Производственная задача №5 (для контроля результатов практической подготовки обучающихся в лабораторной работе № 5):

Включите рабочую станцию в домен.

Шкала оценивания: 3 балльная.

Критерии оценивания:

3 баллов выставляется обучающемуся, если задача решена правильно, в установленное преподавателем время или с опережением времени, при этом обучающимся предложено оригинальное (нестандартное) решение, или наиболее эффективное решение, или наиболее рациональное решение, или оптимальное решение.

2 баллов (или оценка «хорошо») выставляется обучающемуся, если задача решена правильно, в установленное преподавателем время, типовым способом; допускается наличие несущественных недочетов.

1 балла (или оценка «удовлетворительно») выставляется обучающемуся, если при решении задачи допущены ошибки некритического характера и (или) превышено установленное преподавателем время.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если задача не решена или при ее решении допущены грубые ошибки.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ТЕСТОВЫХ ЗАДАНИЙ

2.1.1 ЗАДАНИЯ В ЗАКРЫТОЙ ФОРМЕ

1. Моноалфавитный шифр подстановки – это …	
шифр, при котором каждый символ открытого текста может быть заменен одним из нескольких возможных символов	состоит из нескольких шифров простой замены
шифр, при котором каждый символ открытого текста заменяется на некоторый, фиксированный при данном ключе символ алфавита шифрования.	шифрует информацию и выдает шифротекст по мере поступления, таким образом имея возможность обрабатывать текст неограниченного размера, используя фиксированный объем памяти
2. Какая часть IP-адреса 205.129.12.5 представляет хост-машину	
205	205.129
5	12.5

3. Как по-другому называется MAC-адрес	
Адрес TCP/IP	Физический адрес
Двоичный адрес	Восьмеричный адрес
4. Какая из следующих функций используется маршрутизатором для пересылки пакетов данных между сетями	
Никакая из упомянутых	Приложение и передающая среда
Широковещание и обнаружение коллизий	Определение пути и коммутация
5. Какое из описаний широковещания является наилучшим	
Отправка одного кадра многим станциям одновременно	Отправка одного кадра всем концентраторам и мостам одновременно
Отправка одного кадра всем маршрутизаторам одновременно	Отправка одного кадра всем маршрутизаторам для одновременного обновления таблиц маршрутизации
6. Какое утверждение об асимметричных алгоритмах шифрования - истина	
Они используют один ключ для шифрования и дешифрования данных	Они используют один ключ для дешифрования, но различные ключи для шифрования данных
Они используют различные ключи для шифрования и дешифрования данных	Они используют различные ключи для дешифрования, но один ключ для шифрования данных
7. Будет ли безопасным использовать для хранения паролей пользователей алгоритмы симметричного шифрования вместо хеширования	
Да, если выбрать длину ключа не менее 2048 бит	Нет
Да, если длина пароля составляет не менее 12 символов	Да, при условии неразглашения пароля
8. Для чего нужны номера портов	
Системы-отправители генерируют их для прогнозирования адресов пунктов назначения	Порты позволяют различным программам и сетевым службам на одном хосте получать данные в IP-пакетах независимо друг от друга
Служат для подключения сетевых устройств	Конечные системы используют их для динамического приписывания пользователей к конкретному хосту
9. Какая из перечисленных технологий аутентификации предполагает хранение в системе базы идентификаторов пользователей и их паролей, причем при регистрации пользователя происходит проверка переданных пользователем в процессе аутентификации реквизитов с данными, хранящимися в базе	
Аутентификация с использованием многоразовых паролей	Аутентификация с использованием сертификатов
Биометрическая аутентификация	Аутентификация с использованием одноразовых паролей
10. "Для реализации безопасного доступа к файловому серверу руководство компании предоставило список ресурсов, пользователей и набор разрешений вида “ресурс-пользователь”. Какая из перечисленных моделей управления доступом позволит решить поставленную задачу	
Ролевая модель управления доступом	Классификационная модель управления доступом

Иерархическая модель управления доступом	Дискреционная модель управления доступом
11. Злоумышленник перехватывает трафик аутентификации, направленный от клиента серверу, при этом вносит в него некоторые изменения. Дальнейший обмен данными между клиентом и сервером также перехватывается и модифицируется. При этом и клиент и сервер предполагают, что обмен данными происходит напрямую. Какая из перечисленных атак была реализована злоумышленником	
Человек посередине (Man in the Middle)	Атака повторением (Replay Attack)
Прослушивание (Sniffing)	Отказ в обслуживании (Denial of Service)
12. Группа разработчиков создала для внутреннего использования в компании систему электронного документооборота. Один из программистов, участвовавших в проекте, включил программный код, с помощью которого можно получить доступ к ресурсам системы. О сделанных изменениях никому сообщено не было. Какой из перечисленных типов атак может быть реализован в данном случае	
Червь (Worm)	Лазейка (Back Door)
Переполнение буфера (Buffer Overflow)	Вирусы (Virus)
13. Как называется модель управления доступом, при которой для каждого объекта создается список контроля доступа, в котором определяются субъекты и уровень доступа конкретного субъекта к объекту безопасности? Кроме этого, каждый объект имеет владельца, который обладает неограниченным доступом по отношению к объекту владения.	
Ролевая модель управления доступом	Мандатная модель управления доступом
Дискреционная модель управления доступом	Иерархическая модель управления доступом
14. Принято решение внедрить систему обнаружения атак (Intrusion Detection System). Основная задача системы - своевременно предотвращать изменения, вносимые в критически важные системные файлы. Какой тип систем обнаружения вторжений позволит решить поставленную задачу	
Обманные системы (Deception Systems)	Мониторы регистрационных (журналов) файлов (Log Files Monitors)
Системы обнаружения атак на сетевом уровне (Network IDS)	Системы контроля целостности (System Integrity Verifiers)
15. Каков основной недостаток сигнатурной технологии обнаружения атак	
Высокие требования к системным ресурсам	Сложность и комплексность настройки
Количество обнаруживаемых атак ограничено числом известных атак	Высокая вероятность ложного срабатывания
16. Злоумышленник реализовал атаку, при которой на сервер баз данных компании было отправлено большое количество запросов. В результате атаки сервер прекратил обслуживание авторизованных пользователей. Какая из перечисленных атак была реализована злоумышленником	
Отказ в обслуживании (Denial of Service)	Атака повторением (Replay Attack)
Пинг смерти (Ping of death)	Затопление (Flooding)
17. Некоторые сотрудники компании получили подмененные письма, якобы отправленные от своих коллег. В результате работа нескольких департаментов была приостановлена. Какой из перечисленных методов защиты следует использовать для предотвращения таких атак в дальнейшем	
Шифрование писем при отправке	Цифровая подпись

Архивирование почтовых сообщений	Использование средств антиспамовой защиты
18. Какое из перечисленных свойств сообщения не может быть гарантировано наличием цифровой подписи	
Конфиденциальность сообщения	Подлинность сообщения (сообщение не было подменено во время передачи)
Подлинность отправителя	Целостность сообщения (сообщение не было изменено во время передачи)
19. В компании существовали прецеденты, когда злоумышленник получал физический доступ к серверам и реализовывал ряд атак. Какая из перечисленных мер позволит минимизировать риск осуществления данной угрозы	
Установить пароли BIOS	Переместить серверы в защищенное помещение
Использовать биометрические системы аутентификации	Использовать мультифакторную аутентификацию
20. Некоторые сотрудники компании установили на своих компьютерах нелицензионное программное обеспечение. Через некоторое время сеть компании подверглась ряду атак. В ходе расследования было выяснено, что некоторое из самовольно установленного программного обеспечения содержало видоизмененный код, дающий злоумышленнику возможность осуществления атаки. Какую из перечисленных мер необходимо предпринять для исключения возможности такого рода атак в дальнейшем	
Использовать системы обнаружения вторжений (Intrusion Detection Systems)	Использовать политики безопасности, запрещающие самовольную установку программного обеспечения пользователями
Использовать антивирусные программы, для предварительной проверки программного обеспечения	Использовать для проверки программного обеспечения утилиты категории AntiSpyware
21. В компании используется дискреционная модель доступа к файловым ресурсам. Системный администратор, воспользовавшись правом владения, получил доступ к секретной финансовой информации. Какая из перечисленных мер позволит минимизировать риск осуществления данной угрозы	
Удалить административные учетные записи из списков контроля доступа	Использовать биометрические системы аутентификации
Передать право владения доверенным пользователям	Использовать криптографическую защиту
22. Какая(ой) из перечисленных функций (алгоритмов) позволит создать образ, однозначно соответствующий сообщению, но не позволяющий осуществить обратное преобразование (расшифровку)	
Асимметричное шифрование	Цифровая подпись
SHA	Хеш-функция
23. Как называется модель управления доступом, при использовании которой, администратор назначает объектам и субъектам безопасности классификационные метки (например: публичный, конфиденциальный, секретный), определяющие их место в иерархии? Субъект может получить доступ к объекту только в том случае, если его классификационная метка находится в иерархии не ниже, чем классификационная метка объекта.	
Ролевая модель управления доступом	Иерархическая модель управления доступом

Мандатная модель управления доступом	Классификационная модель управления доступом
24. В компании была похищена конфиденциальная информация. Во время проведения расследования было выяснено: 1) Злоумышленники заранее смогли выяснить имя пользователя и пароль для проникновения в сеть; 2) за некоторое время до атаки пользователи компании получили письмо с привлекательными рекламными предложениями. Некоторые пользователи письмо открыли. Предполагается, что программа злоумышленников, с помощью которой они узнали имена пользователей и пароли, была установлена на компьютеры компании в результате открытия вышеуказанных почтовых сообщений. Какой из перечисленных типов программ был использован злоумышленником?	
Троянский конь	Вредоносное ПО (Malware)
Руткит	Червь (Worm)
25. Зачем в протоколе TCP используются открытые соединения с трехсторонним квитированием	
Для преобразования двоичных ответов на команду ping в информацию для более высоких уровней модели OSI	Для восстановления данных, если потом возникнут проблемы
Для определения объема информации, который принимающая станция может принять за один раз	Для эффективного использования пользователями полосы пропускания
26. Какую информацию дает проверка сети с помощью команды trace	
Определяет правильность функционирования приложений верхнего уровня	Определяет наличие записи в таблице маршрутизации для намеченного маршрутизатора
Определяет, работает ли протокол канала	Показывает каждый маршрутизатор, который проходит пакет на пути к пункту
27. Кто инициирует ARP-запросы	
Бездисковые рабочие станции с пустым кэшем	Устройство, которое не может обнаружить MAC-адреса пункта назначения в своей ARP-таблице
RARP-сервер, в ответ на запрос устройства, работающего со сбоями	Устройство, которое не может обнаружить IP-адрес назначения в своей ARP-таблице
28. Какая информация добавляется во время инкапсуляции на третьем уровни модели OSI	
MAC адрес источника и получателя	Прикладной протокол источника и получателя
Номер порта источника и получателя	IP адрес источника и получателя
29. Какой алгоритм используется при обмене ключами в протоколах Ipsec	
Вижинера	Рида — Соломона
RSA	Диффи-Хеллмана
30. Что позволяет достичь алгоритм Диффи-Хеллмана	
Установить основную политику безопасности между инициатором и респондентом	Проверить идентификационные данные коллеги
Установить симметричный совместно используемый ключ через обменный процесс с открытым ключом	Организовать асимметричное шифрование с открытым ключом

31. Что позволяет организовать firewall прикладного уровня	
Улучшает защиту от атаки DoS	Организует защиту от компьютерных вирусов
Обеспечивает высокоэффективную фильтрацию	Поддерживает большое количество приложений
32. Какой тип NAT используется для многократных переводов внутренних IP-адресов в единственную глобальную переменную, routable IP-адрес	
static NAT	dynamic NAT
NAPT	policy PAT
33. Какой из перечисленных ниже алгоритмов не является симметричным	
Вижинер	Blowfish
DES	RSA
34. Вы опасаетесь возможности перехвата данных во время удаленной работы пользователей. Какая из перечисленных мер позволит минимизировать риск осуществления данной угрозы	
Использовать протокол 3DES	Использовать протокол 802.1x
Использовать VPN соединения	Использовать протокол EAP
35. Пользователь пытается получить доступ к защищенному разделу веб-сайта компании, набрав в строке браузера http://company-site.com/confident, и получает сообщение об ошибке. Какие изменения необходимо внести пользователю для успешного подключения (для защиты коммуникаций с конфиденциальными разделами сайта использовался протокол SSL	
http://username:password@company-site.com/confident	https://company-site.com/confident
ssl://company-site.com/confident	http://company-site.com/confident:443
36. Политика безопасности компании требует разрешения только следующих сетевых сервисов: DNS, электронная почта, WWW. Какой из перечисленных типов брандмауэров позволит реализовать данную политику безопасности?	
Брандмауэр пакетной фильтрации	Брандмауэр уровня приложений
Proxy сервер	NAT
37. Веб-сайт компании доступен для публичного доступа, но некоторые разделы сайта предназначены для только работников компании и партнеров. Требуется обеспечить возможность безопасных подключений к этим разделам. Какой из перечисленных протоколов позволит решить поставленную задачу	
EAP	HTTP
802.1x	SSL
38. "В компании разрабатывается схема аутентификации пользователей. Были выработаны следующие требования: Клиент должен проходить аутентификацию единожды, после этого прозрачно получать доступ к любым разрешенным ресурсам, в независимости от их местонахождения; протокол аутентификации должен быть платформенно-независимым; аутентификация должна быть централизованной. Какой из перечисленных протоколов аутентификации позволит решить поставленную задачу?"	
Kerberos	EAP
PAP	CHAP
39. Политика безопасности компании требует сокрытия схемы IP-адресации, используемой во внутренней сети. Какая из перечисленных технологий позволит решить поставленную задачу	

Proxy сервер	Брандмауэр пакетной фильтрации
NAT	PAT
40. Как называется технология, при которой происходит обмен информацией с удаленной локальной сетью по виртуальному каналу через сеть общего пользования с имитацией частного подключения «точка-точка»	
VPN	CAN
WAN	LAN
41. Для обеспечения безопасного обмена информацией и подтверждения подлинности используются цифровые сертификаты. Какой из перечисленных форматов цифровых сертификатов является наиболее распространенным	
802.1x	IDEA
CA	X.509
42. Политика безопасности компании запрещает пользователям посещение некоторых сайтов. Адреса сайтов занесены в черные списки, которые периодически обновляются. Кроме того, требуется блокировка любых баннеров. Какой из перечисленных типов брандмауэров позволит реализовать данную политику безопасности	
Брандмауэр пакетной фильтрации	PAT
RADIUS сервер	Брандмауэр уровня приложений
43. Каким из перечисленных недостатков обладает система аутентификации Kerberos	
Сильное увеличение загрузки сети	Использование простых криптографических алгоритмов
Отсутствие достаточной поддержки со стороны производителей операционных систем и программного обеспечения	Централизованное хранение всех секретных ключей системы
44. Межсетевой экран, разграничивающий доступ к узлам сети на основании IP-адреса или номера TCP/UDP порта; исходящий и входящий трафик анализируется и фильтруется; пропускается только разрешенный трафик; запросы, не соответствующие правилам, отклоняются. Какой из перечисленных типов брандмауэров соответствует приведенных характеристикам?	
Фильтрующий маршрутизатор	Маршрутизатор, использующий списки контроля доступа
Брандмауэр приложений	Proxy Server
45. Для обеспечения безопасной работы мобильных пользователей решено использовать VPN подключения, для аутентификации пользователей - систему сертификатов.	
PPTP	L2TP
HTTPS	EAP
46. Некоторым сотрудникам компании руководство решило предоставить возможность подключения к сети компании из дома. При этом необходимо обеспечить конфиденциальность доступа и безопасный обмен данными. Какой(ая) из перечисленных протоколов(технологий) позволит решить поставленную задачу	
RDP	VNC
SSH	VPN
47. Требуется установить брандмауэр, позволяющий разграничить доступ пользователей к Интернет на основании следующих правил: доступ по времени, контроль ширины канала, аутентификация пользователей. Какой из перечисленных типов брандмауэров соответствует приведенных характеристикам	
Кэширующий Proxy сервер	Proxy сервер

Маршрутизатор, использующий списки контроля доступа	Брандмауэр пакетной фильтрации
48. Какую длину имеет секретный ключ в криптосистеме DES	
С учетом контрольных разрядов – 56.	С учетом контрольных разрядов – 48.
С учетом контрольных разрядов – 64.	С учетом контрольных разрядов – 128.
49. Сотрудникам требуется организовать удаленное подключение к внутренней сети компании на базе VPN. Руководство компании выдвинуло основные требования безопасности этих подключений: Обеспечение конфиденциальности данных; обеспечение целостности данных; защита от повторения. Какой из перечисленных протоколов позволит реализовать выполнение данных требований?	
TCP	HDLC
HTTP	SSL
50. Какая архитектура лежит в основе алгоритма DES?	
В основе DES лежит 48-раундовая структура сети Фейстеля.	В основе DES лежит 16-раундовая структура сети Фейстеля.
В основе DES лежит использование мультипликативных операций для межраундовых модификаций шифруемого блока	В основе DES лежит метод комбинирования с ключевым элементом с помощью операции аддитивной группы с последующим выполнением подстановок
51. Какая процедура распределения ключей не требует использования защищенного канала для передачи секретного ключа адресату?	
Распределение ключей с участием центра распределения ключей.	Метод Эль Гамаля
Прямой обмен ключами между пользователями	Метод Диффи – Хеллмана
52. Что такое односторонняя хэш-функция?	
Устанавливает однозначное соответствие между исходными данными и хеш-кодом.	Используется для вычисления контрольной суммы CRC.
Функция, являющаяся вычислительно необратимой функцией	Называется такая функция, которая отображает каждый ключ из набора S в множество целых чисел без коллизий.
53. Чему равен результат вычисления хэш-функции по алгоритму SHA-1?	
160 битам	128 битам
64 битам	200 битам
54. Проблема дискретного логарифма заключается …	
является отыскание числа, которое возведено в степень.	является отыскание результата возведения неизвестного числа в неизвестную степень.
является отыскание не числа, которое возведено в степень, а то, в какую степень возведено известное число.	Такой проблемы не существует.
55. Какие алгоритмы не используются для вычисления дайджеста сообщения?	
MD5	SHA-1
AES	ГОСТ Р34.11-94
56. Какая функция используется для реализации Ipsec?	
Использование IKE, чтобы согласовать SA	Использование PKI для pre-shared key аутенификации
Использование SHA для шифрования	Использование кода Рида-Соломона для

	исправления ошибок в блоках
57. Какой из перечисленных протоколов обеспечения безопасности является частью протокола IPSec и выполняет функцию шифрования данных (обеспечение конфиденциальности	
3DES	ESP
AH	RSA
58. Какую функцию не выполняют защищенные виртуальные сети (VPN)	
коммутацию трафика	криптографическое закрытие
аутентификация взаимных сторон	подтверждение подлинности и целостности информации
59. К какому классу преобразований относится система шифрования Вижинера	
Шифрование методом перестановки	Полиалфавитный шифр подстановки
Шифрование методом гаммирования	Шифрование с помощью аналитических преобразований
60. Какие секретные ключи поддерживает алгоритм Rijndael	
кратные 256 битам	кратные 32 битам
произвольной длины	секретный ключ не используется
61. Какая трудноразрешимая задача лежит в основе алгоритма обмена ключами Диффи-Хэллмана	
Задача дискретного логарифмирования	Задача дифференцирования
Задача возведения в степень	Задача интегрирования
62. Какой вид электронной подписи не существует, в соответствии с законодательством РФ	
Простой	Сложной
Квалифицированной	Неквалифицированной
63. Чему равен результат вычисления хэш-функции по алгоритму MD5?	
56 бит	256 бит
128 бит	64 бит
64. В чем заключается фильтрация информационных потоков (трафика) межсетевым экраном?	
В адресации пакета из одной сети в другую.	В анализе информации (адреса, порты, идентификаторы и т.д.) по заданным правилам.
В сборе пакетов, удовлетворяющим определенным правилам.	В фильтрации информационных потоков, с целью определения оптимального маршрута следования пакета.
65. Что такое аутентификация данных?	
Процедура проверки подлинности данных и субъектов информационного взаимодействия.	Процедура определения субъектов информационного взаимодействия.
Процедура проверки целостности данных.	Процедура восстановления данных.
66. Каким образом складывают элементы конечных полей характеристики 2?	
Суммируют биты элементов конечных полей по модулю 2	Выполняют поразрядную коньюнкцию бит элементов
Выполняют поразрядную дизьюнкцию бит элементов	Суммируют биты элементов конечных полей по модулю 2 в степени расширения поля

67. Как программно реализуют умножение элементов конечного поля?	
Путем вычисления квадрата разности элементов поля	С использованием конечных разностей
С использованием инверсии элементов конечного поля	С использованием таблиц логарифмов и антилогарифмов элементов конечного поля
68. Какое из чисел может быть числом элементов простого поля	
6	4
7	9
69. Какое из чисел может быть числом элементов расширенного поля	
8	6
5	10
70. Какое утверждение об асимметричных алгоритмах шифрования - истина	
Они используют различные ключи для шифрования и дешифрования данных	Они используют один ключ для дешифрования, но различные ключи для шифрования данных
Они используют один ключ для шифрования и дешифрования данных	Они используют различные ключи для дешифрования, но один ключ для шифрования данных
71. Выберите вид антивирусных программ, перехватывающих «вирусоопасные» ситуации и сообщающих об этом пользователю	
сканер	блокировщик
CRC-сканер	иммунизатор
72. Какой из перечисленных алгоритмов не является алгоритмом симметричного шифрования	
RSA	AES
DES	Blowfish
73. Какие протоколы используют протокол UDP	
Межсетевые протоколы	Протоколы сетевого уровня
Протоколы уровня приложений	Протоколы управления передачей
74. Для поля из 16 элементов можно сказать, что	
его характеристика равна 1, степень расширения равна 16	его характеристика равна 16, степень расширения равна 1
его характеристика равна 2, степень расширения равна 4	его характеристика равна 3, степень расширения равна 5

2.1.2 ЗАДАНИЯ В ОТКРЫТОЙ ФОРМЕ

1. Верхним уровнем ЭМВОС является _____ уровень.
2. Адресное поле протокола IP v.4 содержит _____ бит.
3. Нижним уровнем ЭМВОС является _____ уровень.
4. Адресное поле протокола IP v.6 содержит _____ бит.
5. Сетевые функции реализуются _____ и _____ уровнями.
6. Десятичным эквивалентом двоичного числа 11111111 является число _____ .
7. Протокол UDP работает поверх протокола _____ .

8. Если коммутатор обнаруживает, что станция назначения находится в том же сегменте сети, что и станция отправитель, он выполняет _____ .
9. Если коммутатор обнаруживает, что станция назначения находится в сегменте сети, отличном от сегмента станции отправителя, он выполняет _____ .
10. Процесс наложения по определенному закону гамма-шифра на открытые данные называется _____ .
11. Алгоритм хеширования SHA предназначен для использования совместно с алгоритмом цифровой подписи _____ .
12. В процедуре проверки подписи используется _____ _____ отправителя.
13. Функции, для которых легко вычислить прямое отображение и нельзя найти обратное называются _____ .
14. Для расширения двоичного поля используют _____ многочлен.
15. Порядком простого конечного поля является _____ число.
16. Для «сжатия» произвольного сообщения служат криптографические _____ - функции.
17. Как называют в криптографии сменный элемент шифра, который применяется для шифрования конкретного сообщения? _____.
18. При использовании классических криптографических алгоритмов ключ шифрования и ключ дешифрования совпадают и такие криптосистемы называются: _____.
19. Для контроля целостности передаваемых по сетям данных используется _____ .
20. Системы, где с помощью открытого ключа шифруют ключ блочного криптоалгоритма, а само сообщение шифруют с помощью этого симметричного секретного ключа, называют: _____ .

2.1.3 ЗАДАНИЯ НА УСТАНОВЛЕНИЕ ПРАВИЛЬНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

1. Выберите правильную последовательность уровней ЭМВОС начиная с верхнего	
Физический, канальный, сетевой и транспортный	Приложений, представлений сеансовый и транспортный
Физический, сетевой, транспортный и приложений	Приложений, сеансовый, сетевой и физический
2. Если необходимо отобразить имя домена на IP-адрес, то что надо сделать сначала	
Активизировать службу DNS	Идентифицировать имена хост-машин
Задать сервер имен	Обратиться в службу DNS за IP-адресом этого устройства
3. Выберите правильную последовательность инкапсуляции данных при передаче их в сеть	
Пакеты, сегменты, данные, биты, кадры	Сегменты, пакеты, кадры, биты, данные

Биты, кадры, пакеты, сегменты, данные	Данные, сегменты, пакеты, кадры, биты
4. Выберите правильную последовательность уровней ЭМВОС начиная с нижнего	
Физический, канальный, сетевой и транспортный	Приложений, представлений сеансовый и транспортный
Физический, сетевой, транспортный и приложений	Приложений, сеансовый, сетевой и физический

Шкала оценивания результатов тестирования: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 баллов (установлено положением П 02.016).

Максимальный балл за тестирование представляет собой разность двух чисел: максимального балла по промежуточной аттестации для данной формы обучения (36 или 60) СТУ 02.02.005–2021 и максимального балла за решение компетентностно-ориентированной задачи (6).

Балл, полученный обучающимся за тестирование, суммируется с баллом, выставленным ему за решение компетентностно-ориентированной задачи.

Общий балл по промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по *5-балльной* шкале:

Соответствие 100-балльной и 5-балльной шкал *Сумма баллов по 100-балльной шкале*	*Оценка по 5-балльной шкале*
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

Задача 1: зашифровать свои ФИО шифром Виженера. Ключ указывается в экзаменационном билете.

Задача 2: зашифровать свои ФИО шифром моноалфавитной подстановкой. Ключ указывается в экзаменационном билете.

Задача 3: зашифровать свои ФИО шифром гаммированием. Гамма указывается в экзаменационном билете.

Задача 4: зашифровать свои ФИО шифром перестановкой. Ключ указывается в экзаменационном билете.

Задача 5: зашифровать свои ФИО многопетлевой полиалфавитной подстановкой. Ключи указываются в экзаменационном билете.

Шкала оценивания решения компетентностно-ориентированной задачи: максимальное количество баллов за решение компетентностно-ориентированной задачи – 6 баллов.

Балл, полученный обучающимся за решение компетентностно-ориентированной задачи, суммируется с баллом, выставленным ему по результатам тестирования.

Общий балл промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале.

Критерии оценивания решения компетентностно-ориентированной задачи:

6-5 баллов выставляется обучающемуся, если решение задачи демонстрирует глубокое понимание обучающимся предложенной проблемы и разностороннее ее рассмотрение; свободно конструируемая работа представляет собой логичное, ясное и при этом краткое, точное описание хода решения задачи и формулировку доказанного, правильного вывода (ответа); задача решена в установленное преподавателем время или с опережением времени.

4-3 балла выставляется обучающемуся, если решение задачи демонстрирует понимание обучающимся предложенной проблемы; задача решена типовым способом в установленное преподавателем время; имеют место несущественные недочеты в описании хода решения и (или) вывода (ответа).

2-1 балла выставляется обучающемуся, если решение задачи демонстрирует поверхностное понимание обучающимся предложенной проблемы; осуществлена попытка шаблонного решения задачи, но при ее решении допущены ошибки и (или) превышено установленное преподавателем время.

0 баллов выставляется обучающемуся, если решение задачи демонстрирует непонимание обучающимся предложенной проблемы и (или) задача не решена.