МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
вычислительной техники
_____ И.Е. Чернецкая
«_21_» ____08____ 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: 16 балльная.

Критерии оценивания:

16 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.

8 баллов (или оценка «хорошо») 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.

4 балла (или оценка «удовлетворительно») выставляется обучающемуся, если он принимает участие в беседе по одному-двум наиболее простым обсуждаемым вопросам; корректно выслушивает иные мнения; неуверенно ориентируется в содержании обсуждаемых вопросов, порой допуская ошибки; в полемике предпочитает занимать позицию заинтересованного слушателя; строит краткие, но в целом логичные высказывания, сопровождаемые наиболее очевидными примерами; теряется при возникновении неожиданных ракурсов беседы и в этом случае нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») 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 №1 (для контроля результатов практической подготовки обучающихся в лабораторной работе № 4):

Установите сервер виртуальной частной сети (VPN).

Производственная задача №1 (для контроля результатов практической подготовки обучающихся в лабораторной работе № 5):

Включите рабочую станцию в домен.

Шкала оценивания: 8 балльная.

Критерии оценивания:

8 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.

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

4 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 ВОПРОСЫ К ЭКЗАМЕНУ

1 Моноалфавитный шифр подстановки – это …
2 Какие уровни в эталонной модели OSI являются четырьмя верхними
3 Какая часть IP-адреса 205.129.12.5 представляет хост-машину
4 Какой из перечисленных ниже алгоритмов не является симметричным
5 Как по-другому называется MAC-адрес
6 Какая из следующих функций используется маршрутизатором для пересылки пакетов данных между сетями
7 Какие протоколы использует протокол UDP для обеспечения надежности
8 Сколько бит содержит IP-адрес

9 Какое десятичное число является эквивалентом двоичного числа 11111111
10 Что происходит, если коммутатор (мост) обнаруживает, что адрес назначения, содержащийся в пакете данных, находится в том же сегменте сети, что и источник
11 Какое из описаний широковещания является наилучшим
12 Какое описание пяти этапов преобразования данных в процессе инкапсуляции при отправке почтового сообщения одним компьютером другому является правильным
13 Какое утверждение об асимметричных алгоритмах шифрования - истина
14 Будет ли безопасным использовать для хранения паролей пользователей алгоритмы симметричного шифрования вместо хеширования
15 Если необходимо отобразить имя домена на IP-адрес, то что надо сделать сначала
16 Для чего нужны номера портов
17 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
18 "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"
19 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
20 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
21 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.
22 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

23 Каков основной недостаток сигнатурной технологии обнаружения атак

24 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

25 "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"

26 Какое из перечисленных свойств сообщения не может быть гарантировано наличием цифровой подписи

27 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

28 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

29 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

30 Какая(ой) из перечисленных функций (алгоритмов) позволит создать образ, однозначно соответствующий паролю, но не позволяющий осуществить обратное преобразование (расшифровку)

31 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.

32 "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?"

33 Зачем в протоколе TCP используются открытые соединения с трехсторонним квитированием

34 Какую информацию дает проверка сети с помощью команды trace

35 Кто инициирует ARP-запросы

36 Какая информация добавляется во время инкапсуляции на третьем уровни модели OSI

37 Какой алгоритм используется при обмене ключами в протоколах Ipsec

38 Что позволяет достичь алгоритм Диффи-Хеллмана

39 Что позволяет организовать firewall прикладного уровня

40 Какой тип NAT используется для многократных переводов внутренних IP-адресов в единственную глобальную переменную, routable IP-адрес

41 Какой из перечисленных алгоритмов не является алгоритмом симметричного шифрования

42 "Вы опасаетесь возможности перехвата данных во время удаленной работы пользователей. Какая из перечисленных мер позволит минимизировать риск осуществления данной угрозы"

43 "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)"

44 "Политика безопасности компании требует разрешения только следующих сетевых сервисов: DNS, электронная почта, WWW. Какой из перечисленных типов брандмауэров позволит реализовать данную политику безопасности?"

45 "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"

46 "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?"

47 "Политика безопасности компании требует сокрытия схемы IP-адресации, используемой во внутренней сети. Какая из перечисленных технологий позволит решить поставленную задачу"

48 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»

49 "Для обеспечения безопасного обмена информацией и подтверждения подлинности используются цифровые сертификаты. Какой из перечисленных форматов цифровых сертификатов является наиболее распространенным"

50 "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"

51 Каким из перечисленных недостатков обладает система аутентификации Kerberos

52 "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"

53 "Для обеспечения безопасной работы мобильных пользователей решено использовать VPN подключения, для аутентификации пользователей - систему сертификатов. Какой из перечисленных протоколов позволит решить поставленную задачу"

54 "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"

55 "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"

56 Какую длину имеет секретный ключ в криптосистеме DES

57 "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"

58 Какая архитектура лежит в основе алгоритма DES?
59 Какая процедура распределения ключей не требует использования защищенного канала для передачи секретного ключа адресату?
60 Что такое односторонняя хэш-функция?
61 Чему равен результат вычисления хэш-функции по алгоритму SHA-1?
62 Проблема дискретного логарифма заключается …
63 Какие алгоритмы не используются для вычисления дайджеста сообщения?
64 Какая функция используется для реализации Ipsec
65 Какой из перечисленных протоколов обеспечения безопасности является частью протокола IPSec и выполняет функцию шифрования данных (обеспечение конфиденциальности
66 Какую функцию не выполняют защищенные виртуальные сети (VPN)
67 К какому классу преобразований относится система шифрования Вижинера?
68 Какие секретные ключи поддерживает алгоритм Rijndael
69 Какая трудноразрешимая задача лежит в основе алгоритма обмена ключами Диффи-Хэллмана
70 Какой вид электронной подписи не существует, в соответсвии с законодательством РФ
71 Чему равен результат вычисления хэш-функции по алгоритму MD5
72 В чем заключается фильтрация информационных потоков (трафика) межсетевым экраном?
73 Что такое аутентификация данных?

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*	*Оценка по 5-балльной шкале*

баллов по 100-балльной шкале	
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

Задача: Зашифровать свои ФИО шифром Виженера. Ключ указывается 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.