МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование кафедры полностью)

_____ А.Л. Марухленко
(подпись)
«10» июня 2025г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости
и промежуточной аттестации обучающихся
по дисциплине
Информационная безопасность
(наименование дисциплины)

45.03.03 Фундаментальная и прикладная лингвистика, направленность (профиль) «Теоретическая и прикладная лингвистика»
(код и наименование ОПОП ВО)

Курск – 2025

Задания для проведения текущего контроля успеваемости

Вопросы для устного опроса

Тема 1. Основные понятия и анализ угроз информационной безопасности

1. Дайте определение трем ключевым свойствам информации (КЦД) и проиллюстрируйте каждое на реальном примере из жизни.
2. В чем принципиальная разница между угрозой, уязвимостью и риском? Приведите пример взаимосвязи этих понятий.
3. Назовите и охарактеризуйте три основных источника угроз информационной безопасности.
4. Что такое «модель нарушителя» и для чего она создается? Какие категории нарушителей обычно выделяют?
5. Опишите основные этапы процесса управления рисками ИБ.
6. Что такое «актив» в контексте ИБ? Приведите примеры активов разного типа (информационные, программные, аппаратные, человеческие).
7. Какие основные мотивы стоят за действиями внутреннего нарушителя (инсайдера)?
8. Объясните разницу между пассивной и активной угрозой. Приведите по два примера каждой.
9. Что такое «непреднамеренные угрозы» и чем они отличаются от преднамеренных?
10. Почему человеческий фактор часто называют самым слабым звеном в системе ИБ?

Тема 2. Проблемы информационной безопасности сетей

1. Перечислите и кратко охарактеризуйте основные уровни модели TCP/IP, на которых реализуются типовые угрозы.
2. В чем заключается суть атаки «IP-спуфинг» и какие меры защиты от нее существуют?
3. Опишите механизм атаки «Сниффинг пакетов» (Sniffing). Как можно защитить данные от перехвата в сети?
4. Что такое атака типа «отказ в обслуживании» (DoS) и ее распределенная версия (DDoS)? В чем цель такой атаки?
5. Объясните суть атаки «Man-in-the-Middle» (человек посередине). На каком принципе основана защита от нее (например, в HTTPS)?
6. Что такое SQL-инъекция и к каким последствиям она может привести? Какой общий принцип защиты от此类 атак?
7. В чем опасность использования нешифрованных протоколов (HTTP, FTP, Telnet) в современных сетях?
8. Что такое «сетевой сканер» и для каких легитимных и нелегитимных целей он используется?
9. Какие угрозы несет в себе использование публичных точек доступа Wi-Fi?
10. Почему сегментация сети считается хорошей практикой безопасности?

Тема 3. Политика безопасности

1. Дайте определение политики безопасности организации. Является ли это чисто техническим документом?
2. Назовите и охарактеризуйте три основных типа политик безопасности (по уровням детализации).
3. Кто является целевой аудиторией для политики безопасности? Почему она должна быть адресована разным группам по-разному?
4. Какие основные разделы обычно включает в себя политика безопасности верхнего уровня?
5. Что такое «регламент» и «инструкция» в иерархии документов ИБ? Чем они отличаются от политики?
6. Почему недостаточно просто разработать политику безопасности? Какие процессы должны ее сопровождать?
7. Какова роль высшего руководства организации в разработке и внедрении политики безопасности?
8. Что такое «зона допустимого риска» и как она связана с политикой безопасности?
9. Приведите пример конкретной политики (например, политика использования электронной почты, политика парольной защиты).
10. Что должно произойти, чтобы политика безопасности была пересмотрена и обновлена?

Тема 4. Криптографическая защита информации

1. В чем основное различие между симметричными и асимметричными криптосистемами? Их плюсы и минусы.
2. Объясните на примере, как работает электронная цифровая подпись (ЭЦП) на основе асимметричного шифрования.
3. Что такое хэш-функция? Какими свойствами она должна обладать и для каких задач защиты информации применяется?
4. Для чего в асимметричной криптографии используются сертификаты и что такое инфраструктура открытых ключей (PKI)?
5. Почему современные алгоритмы симметричного шифрования (например, AES) используют несколько раундов преобразований?
6. Что такое криптостойкость алгоритма и от чего она зависит?
7. Объясните принцип работы гибридной криптосистемы. Почему это наиболее распространенный подход на практике?
8. Что такое «имитозащита» и как она достигается с помощью кодов аутентификации сообщений (MAC)?
9. Назовите области применения криптографии: для защиты данных при передаче, при хранении и др.
10. В чем разница между стеганографией и криптографией?

Тема 5. Технологии аутентификации

1. Объясните разницу между понятиями: аутентификация, авторизация и идентификация.
2. Назовите три типа факторов аутентификации («что-то, что вы знаете/имеете/есть») и приведите по два примера каждого.
3. Что такое многофакторная аутентификация (MFA) и почему она значительно надежнее однофакторной?
4. Какие уязвимости присущи статическим паролям? Перечислите современные требования к политике создания паролей.
5. Опишите принцип работы одноразовых паролей (OTP), например, в приложениях-аутентификаторах.
6. Что такое биометрическая аутентификация? Какие ее виды вы знаете и в чем их преимущества и риски?
7. Что такое протокол RADIUS и для чего он используется в сетях?
8. Что такое «менеджер паролей» и как он помогает повысить безопасность?
9. Опишите возможные атаки на системы аутентификации (подбор, перехват, фишинг).
10. Что такое Single Sign-On (единый вход) и каковы его преимущества с точки зрения безопасности и удобства?

Тема 6. Технологии межсетевых экранов (МЭ, firewall)

1. Какова основная функция межсетевого экрана? Дайте определение и приведите analogy.
2. В чем разница между сетевым экраном, работающим на сетевом уровне (packet filter) и на уровне приложений (application-level gateway)?
3. Что такое Stateful Inspection (статистическая проверка состояний) и почему она эффективнее простой фильтрации пакетов?
4. Объясните принцип работы трансляции сетевых адресов (NAT) и какой вклад в безопасность он вносит.
5. Что такое демилитаризованная зона (DMZ) и для каких целей она создается в корпоративной сети?
6. Как администратор создает правила для МЭ? Что означают понятия «белый список» и «черный список» в этом контексте?
7. В чем заключаются ограничения и недостатки классических межсетевых экранов?
8. Что такое система обнаружения и предотвращения вторжений (IDS/IPS) и чем она дополняет функционал МЭ?
9. Чем host-based firewall отличается от network-based?
10. Почему правило «запретить все, что не разрешено явно» является более безопасным, чем «разрешить все, что не запрещено»?

Тема 7. Технологии защиты от вирусов

1. Дайте расширенное определение «вредоносному программному обеспечению» (Malware). Назовите не менее 5 его основных разновидностей.
2. В чем отличие вируса, червя и троянской программы по механизму распространения и цели?
3. Опишите принцип работы антивирусного сканера, основанного на сигнатурах. В чем его главный недостаток?
4. Что такое эвристический анализ и как он помогает обнаруживать ранее неизвестные угрозы?
5. Как работает технология проактивной защиты (HIPS — Host-based Intrusion Prevention System)?
6. Что такое «антивирусный монитор» и «антивирусный сканер» и чем они отличаются по принципу работы?
7. Почему важно регулярно обновлять антивирусные базы и программное обеспечение?
8. Какие существуют методы сокрытия вредоносного кода от антивирусов (обфускация, полиморфизм)?
9. Что такое бэкдор (backdoor) и руткит (rootkit)? В чем их особая опасность?
10. Назовите неантивирусные меры защиты от вредоносных программ (например, на уровне ОС, браузера, пользователя).

Тема 8. Требования к системам защиты информации

1. Что такое «профиль защиты» и «задание по безопасности» в соответствии с common criteria (Общими критериями)?
2. Какие основные классы и семейства требований существуют в стандартах по безопасности (например, по «Оранжевой книге» TCSEC или Common Criteria)?
3. Что подразумевается под требованием «подотчетности» (accountability)?
4. Объясните разницу между дискреционным и мандатным управлением доступом. Какой из них считается более строгим?
5. Что такое гарантированность (assurance) в контексте оценки безопасности системы?
6. Какие требования предъявляются к аудиту безопасности (журналированию)?
7. Что такое модель безопасности и для чего она создается? (Например, модель Белла-ЛаПадулы).
8. Почему при разработке безопасной системы важно закладывать требования безопасности на ранних этапах (принцип «security by design»)?
9. Что такое доверенная вычислительная база (TCB)?
10. Как стандарты и требования к СЗИ связаны с процессом управления рисками?

Тема 9. Основы правового обеспечения защиты информации

1. Назовите основные российские законы и нормативные акты, регулирующие вопросы информационной безопасности.
2. Какая информация относится к персональным данным (ПДн) согласно закону? Назовите основные обязанности оператора ПДн.
3. Что такое государственная тайна и какая информация к ней относится? Назовите основные нормативные акты в этой сфере.
4. Что такое коммерческая тайна и как она охраняется законом?
5. Какие виды ответственности (дисциплинарная, административная, уголовная) предусмотрены за нарушение законодательства в области ИБ?
6. Что такое «уведомление о нарушении защиты персональных данных» (data breach notification) и в каких случаях оно требуется?
7. Каковы основные права субъекта персональных данных (например, право на доступ, уточнение, блокирование)?
8. Что такое Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры (КИИ)» и какие субъекты он регулирует?
9. В чем суть нормативного документа «Приказ ФСТЭК России № 21» и для кого он обязателен?
10. Как международное законодательство (например, GDPR) влияет на российские компании?

Критерии оценки:

7-12 баллов выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

1-6 балла выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

Контрольные вопросы для защиты лабораторных работ

Лабораторная работа 1: Шифрование методом прямой замены

1. В чем заключается главная криптографическая слабость всех шифров прямой (моноалфавитной) замены?
2. Как метод частотного анализа позволяет вскрыть шифр простой замены? Опишите шаги.
3. Чем шифр Цезаря является частным случаом шифра простой замены?
4. Какой вклад вносит знание лингвистических особенностей языка (частота букв, биграммы, триграммы) в криптоанализ этого метода?
5. Как можно модифицировать шифр прямой замены, чтобы немного усилить его стойкость? (Например, использование гомофонов).
6. Опишите алгоритм дешифрования текста, зашифрованного шифром Цезаря, без знания ключа (сдвига).
7. В чем разница между шифром Атбаш и шифром Цезаря с ключом K=3?
8. Почему данный метод уязвим для атаки по известному открытому тексту?
9. Какие исторические примеры использования шифров прямой замены вам известны?
10. Можно ли считать шифрование методом прямой замены надежным для защиты информации сегодня? Обоснуйте ответ.

Лабораторная работа 2: Шифрование методом полиалфавитной замены

1. Как метод полиалфавитной замены устраняет главный недостаток моноалфавитных шифров?
2. Объясните принцип работы шифра Виженера с использованием таблицы Виженера (или формулы).
3. Что такое «ключевое слово» и как его длина влияет на стойкость шифра?
4. Опишите метод Касиски (или метод Фридмана) для определения длины ключевого слова. В чем его суть?
5. После определения длины ключа, как происходит окончательное вскрытие шифротекста?
6. В чем заключаются основные слабости упрощенных версий шифра Виженера, таких как шифр Гронсфельда?
7. Что такое «автоключ» в модификациях шифра Виженера и как он повышает стойкость?
8. Почему шифр Виженера долгое время считался «невзламываемым» (Le chiffre indéchiffrable)?
9. Какие современные алгоритмы шифрования используют принцип, аналогичный полиалфавитной замене? (Намек: режимы сцепления блоков).
10. Сравните стойкость шифра Виженера и шифра Цезаря. Во сколько раз, теоретически, первый сложнее второго?

Лабораторная работа 3: Шифрование методом перестановок

1. В чем основное отличие шифров перестановки от шифров замены?
2. Опишите алгоритм шифрования и дешифрования методом одинарной перестановки по ключу.
3. Как дешифровать сообщение, зашифрованное перестановкой, если ключ (порядок столбцов) неизвестен? Какие лингвистические подсказки можно использовать?
4. В чем слабость метода одинарной перестановки и как метод двойной перестановки пытается ее устранить?
5. Что такое «маршрутное шифрование»? Приведите пример (спираль, змейка и т.д.).
6. Как криптоаналитик может определить, что имеет дело с шифром перестановки, а не замены, просто взглянув на шифротекст? (Подсказка: анализ частотности символов).
7. Опишите принцип работы шифра с помощью карточки-решетки.
8. Какие практические применения находят шифры перестановки в современных криптосистемах? (Намек: часто используются в составе более сложных алгоритмов, например, в блоковых шифрах как элемент).
9. Как длина текста влияет на стойкость шифра перестановки?
10. Почему шифры перестановки, используемые самостоятельно, считаются нестойкими?

Лабораторная работа 4: Шифрование аналитическими методами

1. В чем суть метода частотного анализа для дешифрования?
2. Как выглядит эталонная частотная статистика букв для русского/английского языка?
3. Какие буквы/сочетания букв являются самыми частотными и самыми редкими в русском/английском языке? Знание каких лингвистических особенностей здесь критично?
4. Почему частотный анализ эффективен против шифров замены, но неэффективен против шифров перестановки?
5. Что такое биграммы и триграммы и как их анализ помогает уточнить дешифровку?
6. Опишите последовательность ваших действий при вскрытии шифра простой замены с помощью частотного анализа.
7. Какие дополнительные «ключи к разгадке» (помимо частотности) может использовать аналитик? (Намек: знаки препинания, однобуквенные слова, часто встречающиеся предлоги и союзы).
8. С какими трудностями можно столкнуться при анализе короткого текста?
9. Как можно затруднить применение частотного анализа к шифротексту? (Методы противодействия).
10. В чем заключается основная работа криптоаналитика-лингвиста на этапе «подгонки» гипотез после частотного анализа?

Лабораторная работа 5: Разделение секрета

1. В чем состоит практическая задача, решаемая методами разделения секрета?
2. Объясните суть пороговой схемы (k, n). Что означают числа k и n?
3. На каком математическом объекте основана схема Шамира? (Ответ: полиномы).
4. Почему для восстановления секрета в схеме Шамира требуется именно k долей, а k-1 долей недостаточно?
5. Опишите шаги участника при создании долей секрета по схеме Шамира.
6. Опишите шаги участников при восстановлении секрета из k долей.
7. Каковы преимущества схемы Шамира перед простым разрезанием секрета на n кусков?
8. Где находят применение такие схемы в современных системах безопасности? (Намек: secure multi-party computation, ключи от сейфов, корпоративные секреты).
9. Является ли схема Шамира совершенной? Объясните, что это означает (любые k-1 долей не дают никакой информации о секрете).
10. В чем заключается роль «доверенного дилера» в классической схеме и можно ли обойтись без него?

Лабораторная работа 6: Алгоритм шифрования RSA

1. К какому классу алгоритмов относится RSA (симметричные или асимметричные) и в чем его основное преимущество?
2. Опишите этапы генерации пары ключей (открытый и закрытый) в RSA.
3. Какие математические теоремы лежат в основе работы RSA? (Малая теорема Ферма / Теорема Эйлера).
4. Почему числа p и q должны быть большими и простыми? Что произойдет, если они будут малыми или не простыми?
5. Объясните, как происходит операция шифрования и дешифрования с помощью открытого и закрытого ключа.
6. В чем разница между использованием RSA для шифрования и для создания цифровой подписи?
7. Почему напрямую RSA шифруют только короткие сообщения? Как решается проблема шифрования больших данных? (Намек: гибридные криптосистемы, сеансовый ключ).
8. Какие основные вычислительные операции являются самыми трудоемкими в RSA и от чего зависит скорость работы алгоритма?
9. Назовите основные уязвимости и атаки на RSA (атака на малый модуль, малый открытый экспонент, атака по времени). Не вдаваясь в детали, объясните суть одной из них.
10. Где в реальной жизни мы сталкиваемся с использованием RSA? (Намек: защищенный веб-браузинг (HTTPS), электронная подпись, защита соединения в мессенджерах).

Критерии оценки:

13-24 баллов выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

1-12 балла выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

Ситуационные задачи

1. Технологии межсетевых экранов

Ситуация: Лингвистическая исследовательская группа «TextUmbrella» работает над созданием новой цифровой платформы для анализа древних манускриптов. Платформа состоит из:

- Веб-сервера с публичным каталогом оцифрованных текстов (доступен всем в интернете).
- Сервера базы данных, где хранятся сканы высокого разрешения и неопубликованные расшифровки.
- Рабочей станции лингвиста-исследователя для анализа текстов.

Администратор настроил межсетевой экран (firewall) со следующими правилами:

№	Протокол	Источник	Назначение	Порт	Действие
1	TCP	Любой	Веб-сервер	80	Разрешить
2	TCP	Любой	Веб-сервер	443	Разрешить
3	TCP	Веб-сервер	Сервер БД	1433	Разрешить
4	TCP	Рабочая станция	Сервер БД	1433	Разрешить
5	TCP	Любой	Сервер БД	1433	Запретить
6	TCP	Рабочая станция	Любой	3389	Разрешить
...	...	...	...	...	(Все остальное запрещено)

Задача для студента:

1. Объясните логику каждого из правил (1-6) простым языком. Для чего оно нужно?
2. Проанализируйте уязвимость. Исследователь открыл на своей рабочей станции вредоносный файл, который активировал троянскую программу. Злоумышленник получил удаленный доступ к рабочей станции. Используя это, сможет ли он теперь напрямую атаковать и получить доступ к серверу базы данных? Обоснуйте свой ответ, ссылаясь на конкретные правила фильтрации.
3. Предложите улучшение. Какое правило вы бы добавили, изменили или удалили, чтобы минимизировать риск подобной атаки в будущем, не мешая рабочему процессу?

2. Технологии защиты от вирусов

Ситуация: Студентка-лингвистка Мария пишет дипломную работу по неологизмам в социальных сетях. Для сбора данных она активно посещает тематические форумы, паблики и скачивает пользовательские комментарии в виде файлов (.txt, .docx, .csv). На ее личном ноутбуке установлен антивирус «DefenderPlus».

Однажды она получает по электронной почте от «коллеги-исследователя» архив linguistic_data.zip. Внутри два файла:

1. research_data.csv – легитимный файл с данными.
2. linguistic_analyzer.exe – исполняемый файл с описанием «новая портативная программа для анализа частотности слов, просто запусти».

Антивирус «DefenderPlus» моментально помещает весь архив в карантин, сработала сигнатура-based защита.

Задача для студента:

1. Объясните, почему антивирус среагировал на .exe-файл, но проигнорировал .csv? В чем разница в потенциальной опасности этих типов файлов с точки зрения антивирусного ПО?

2. Мария очень заинтересована в программе. Она решает временно отключить антивирус, чтобы извлечь и запустить linguistic_analyzer.exe. Опишите три риска, на которые она сознательно идет, совершая это действие.

3. Какие два более безопасных альтернативных действия она могла бы предпринять, чтобы проверить файл, не отключая систему защиты?

3. Шифрование аналитическими методами

Ситуация: В рамках изучения истории криптографии лингвистический кружок анализирует старый зашифрованный манускрипт, предположительно написанный на основе английского языка. Известно, что использовалась моноалфавитная подстановка (один символ алфавита всегда заменяется на один и тот же символ шифра). Фрагмент шифртекста:

J XJMM TPMWFE B CPWU MFW FOHJOF...

Задача для студента:

1. Используя свои знания лингвистики, проведите частотный анализ приведенного фрагмента. Составьте таблицу частоты встречаемости каждого символа в шифртексте.

2. Сопоставьте полученные данные с известной частотностью букв в английском языке (например, самые частые буквы: E, T, A, O, I, N...). Предположите, какая буква английского алфавита может скрываться под символом J, M и E?

3. Попробуйте дешифрировать первую фразу: J XJMM TPMWFE B CPWU MFW FOHJOF.... Какое слово, скорее всего, стоит после «I»? Какое слово из трех букв является одним из самых распространенных в английском языке (артикль)? Используйте эти подсказки.

(Подсказка: в исходном тексте использовался заглавный регистр, пробелы и пунктуация сохранены. Расшифровка первой фразы: "I will spend a lot of time...")

Критерии оценки:

7-12 баллов выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

1-6 балла выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные

определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

Типовые задания для проведения промежуточной аттестации обучающихся

Задания в закрытой форме

Задание №1

Какая угроза информационной безопасности является пассивной?

1. Копирование секретных данных.
2. Внедрение вредоносного программного обеспечения.
3. Кража носителей информации.
4. Удаление файла.

Задание №2

Угрозы нарушения целостности информации приводят к следующему результату:

1. Изменение, искажение или уничтожение информации.
2. Информация становится известной лицам, которые не должны иметь к ней доступ.
3. Снижается работоспособность автоматизированной системы, либо блокируется доступ к ее ресурсам.
4. Злоумышленнику становятся известны параметры автоматизированной системы.

Задание №3

К какому уровню доступа к информации в автоматизированной системе относится перехват данных, передаваемых по каналам связи?

1. Уровень средств взаимодействия с носителем.
2. Уровень носителей информации.
3. Уровень представления информации.
4. Уровень содержания информации.

Задание №4

Какая сетевая атака связана с превышением допустимых пределов функционирования сети?

1. Отказ в обслуживании (DoS –атака).
2. Подслушивание (Sniffing).
3. Атака Man in – the – Middle (человек в середине).
4. Угадывание ключа.

Задание №5

Какая сетевая атака является характерной именно для беспроводных сетей?

1. Вещание радиомаяка.
2. Подслушивание (Sniffing).
3. Атака Man in – the – Middle (человек в середине).
4. Отказ в обслуживании (DoS –атака).

Задание №6

Основной защитой от фишинга являются:

1. Фильтры.
2. Антивирусные программы.
3. Криптографические системы.
4. Системы видеонаблюдения.

Задание №7

Под политикой безопасности организации понимают:

1. Совокупность документированных управленческих решений, направленных на защиту информации.
2. Совокупность юридических законов в области защиты информации.
3. Процедура безопасности.
4. Руководство по архитектуре безопасности.

Задание №8

Политика удаленного доступа – это:

1. Специализированная политика безопасности.
2. Базовая политика безопасности.

3. Процедура безопасности.
4. Руководство по архитектуре безопасности.

Задание №9

Политики безопасности разделяют на уровни:

1. Верхний, средний и нижний.
2. Верхний и нижний.
3. Обобщенный и детальный.
4. Нет разделения на уровни.

Задание №10

Какая криптосистема шифрования является ассиметричной?

1. Алгоритм шифрования RSA.
2. Шифр Виженера.
3. Американский стандарт шифрования AES.
4. Стандарт шифрования ГОСТ 28147-89.

Задание №11

При шифровании методом Виженера слова «Банк» получилось зашифрованное сообщение «ВГТЛ». Какой был использован ключ?

1. 1-3-5
2. 2-6
3. 6-1-4
4. 8-5-2-3

Задание №12

Для проверки электронной цифровой подписи необходимо знать:

1. Открытый ключ отправителя.
2. Секретный ключ отправителя.
3. Два ключа отправителя: секретный и открытый.
4. Не требуется знания никаких ключей.

Задание №13

Под аутентификацией понимают:

1. Процедуру проверки подлинности заявленного пользователя, процесса, устройства.
2. Процедуру распознавания пользователя по его идентификатору.
3. Процедуру предоставления субъекту определенных полномочий и ресурсов в сети.
4. Регистрацию действий пользователя в сети.

Задание №14

Вероятность угадывания PIN –кода из 4 десятичных цифр за 3 попытки равна:

1. 0,0003.
2. 0,003
3. 0,00003.
4. 0,0004.

Задание №15

Различают следующие виды систем идентификации и аутентификации:

1. Электронные, биометрические и комбинированные.
2. Электронные и биометрические.
3. Электронные, биометрические и механические.
4. Электронные, биометрические и криптографические.

Задание №16

Какую функцию не может выполнять межсетевой экран?

1. Лечение файлов, зараженных вирусами.
2. Фильтрация трафика.
3. Трансляция сетевых адресов.
4. Регистрация событий.

Задание №17

Какой межсетевой экран обеспечивает наиболее высокий уровень безопасности?

1. Комплексный межсетевой экран.
2. Экранирующий маршрутизатор.
3. Шлюз сеансового уровня.
4. Прикладной шлюз.

Задание №18

Различают следующие варианты исполнения межсетевых экранов:

1. Программный и программно-аппаратный.
2. Программный и аппаратный.
3. Аппаратный и программно – аппаратный.
4. Существуют только программные межсетевые экраны.

Задание №19

Какая вредоносная программа не размножается, но способна удаленно управлять компьютером и воровать пароли?

1. Троянская программа.
2. Червь.
3. Файловый вирус.
4. Макровирус.

Задание №20

Какая антивирусная программа не конфликтует с другими антивирусами, но не имеет функции автоматического обновления антивирусной базы?

1. Dr. Web Curelt.
2. Kaspersky Internet Security.
3. Eset NOD 32 Antivirus.
4. Avira AntiVir Personal.

Задание №21

Какой метод выявления вируса позволяет обнаруживать только известные вирусы?

1. Обнаружение, основанное на сигнатурах.
2. Обнаружение программ подозрительного поведения.
3. Обнаружение вирусов при помощи эмуляции работы программы.
4. Эвристический анализ.

Задание №22

Сколько существует классов защищенности средств вычислительной техники от несанкционированного доступа?

1. 7.
2. 5.
3. 9.
4. 6.

Задание №23

Какой класс защищенности автоматизированных систем предъявляет наиболее высокие требования к информационной безопасности?

1. 1А
2. 1Г
3. 3Б
4. 3А

Задание №24

Вторая группа классов защищенности автоматизированных систем включает автоматизированные системы:

1. В которых работают несколько пользователей и все они имеют одинаковые права доступа к информации.
2. В которых работают несколько пользователей, и они имеют

различные права доступа к информации.

3. В которых работает только один пользователь.

4. В которых работает один пользователь или несколько пользователей, имеющих одинаковые права доступа к информации.

Задание №25

В каком законе определены принципы и порядок засекречивания информации?

1. Закон “О государственной тайне”.

2. Закон “О безопасности”.

3. Закон “Об информации, информационных технологиях и о защите информации”.

4. Закон “Об авторском праве и смежных правах”.

Задание №26

Какой вид деятельности предприятий подлежит лицензированию ФСБ?

1. Эксплуатация негосударственными предприятиями шифровальных средств, предназначенных для криптографической защиты информации, не содержащих сведений, составляющих государственную тайну.

2. Сертификация, сертификационные испытания защищенных технических средств обработки информации (ТСОИ).

3. Аттестование систем информатизации, систем связи и передачи данных, технических средств приема, систем передачи и обработки информации, подлежащей защите.

4. Проведение специальных исследований на побочные электромагнитные излучения и наводки (ПЭМИН) ТСОИ.

Задание №27

Является объектом авторского права, но не признается патентоспособным изобретением:

1. База данных.

2. Устройство.

3. Способ.
4. Вещество.

Задание №28

Основная масса угроз приходится на:

1. Шпионские программы.
2. Троянские программы.
3. Черви.

Задание №29

Какой вид идентификации и аутентификации является наиболее распространённым:

1. Одноразовые пароли.
2. Постоянные пароли.
3. системыPKI.

Задание №30

Под какие системы вирусы распространяются наиболее динамично:

1. Windows.
2. Mac OS.
3. Android.
4. Linux.

Задание №31

Заключительный этап построения системы защиты:

1. Планирование.
2. Сопровождение.
3. Анализ уязвимых мест.
4. Отчётность.

Задание №32

Какие угрозы безопасности информации являются преднамеренными:

1. Открытие электронного письма, содержащего вирус.
2. Ошибка персонала.
3. Не авторизированный доступ.
4. Открытие сайта.

Задания в открытой форме

1. Персональные данные – это

2. Доступностью информации называется

3. К объектам информационной безопасности на предприятии относятся

4. Целостностью информации называется

5. Конфиденциальностью информации называется

6. К коммерческой тайне относится информация

7. Информационной безопасностью предприятия является

8. В состав системы защиты информации входят обеспечивающие подсистемы

9. Под угрозой безопасности информации понимается

10. Причинами информационных угроз являются

11. Основные компьютерные вирусы

12. К основным законам информационной безопасности РФ относятся законы

13. Основными принципами политики безопасности являются

14. Политика безопасности верхнего уровня включает

15. Удаленный доступ к сервису организован

16. Политика управления паролями включает

17. Системный подход к защите информации базируется на принципах

18. Для ИБ используются программные средства

19. Метод принуждения от метода побуждения отличается

20. Криптография занимается

21. Электронная подпись используется для

22. В состав организационно-технических мер входит

23. Межсетевые экраны применяют для

24. Технические средства противодействия классифицируются

25. В состав службы безопасности входят подразделения

26. К мерам по защите информации в интернете относятся

27. Межсетевые экраны-брандмауэры используются для

28. Для защиты электронной почты используется

29. Для защиты от вирусов можно использовать

30. К антивирусным программам относятся

31. Основные источники проникновения вирусов

32. В корпоративной сети необходимо защищать

33. Основные этапы построения системы защиты

34. План защиты включает

35. Ответственным за определение уровня классификации информации является

36. Ответственность за гарантии того, что данные классифицированы и защищены несёт

37. Политики безопасности – это

38. Естественные угрозы безопасности информации вызваны

39. Искусственные угрозы безопасности информации вызваны

40. К посторонним лицам - нарушителям информационной безопасности относятся

41. К основным непреднамеренным искусственным угрозам автоматизированным систем обработки информации относятся

42. К внутренним нарушителям информационной безопасности относится

Задания на установление соответствия

1. Установить соответствие названиям функций

1	Mozilla	А	Стандартная программа Windows
2	Winrar	Б	База данных
3	Блокнот	В	Программа-архиватор
4	Картотека учащихся	Г	Программа-браузер

2. Установить соответствие топологии сети её характеристике

1	Общая шина	А	Каждая рабочая станция сети соединяется с несколькими другими рабочими станциями этой же сети
2	Звезда	Б	В данной топологии все рабочие станции соединены друг с другом с помощью центрального концентратора
3	Кольцо	В	В основе топологии лежит общий кабель (магистраль), к которому подсоединяются все рабочие станции
4	Комбинированные решения	Г	Топология, в которой каждая рабочая станция соединяется только с двумя соседними

3. Установить соответствие между компьютерными изобретениями и именами учёных

1	Всемирная паутина	А	Нейман
2	Компьютерная мышь	Б	Касперский
3	Первая ЭВМ	В	Тим Бернерс-Ли
4	Антивирус	Г	Дуглас Энгельбарт

4. Установить соответствие названиям устройств ПК назначение

1	Модем	А	Устройство для вывода текстов на экран
2	Клавиатура	Б	Устройство для хранения файлов
3	Монитор	В	Устройство для обмена информацией между ПК и провайдером через сеть
4	Жесткий диск	Г	Устройство для ввода символов

5. Установить соответствие названия ОС её назначению

1	NetWare	А	Серверная операционная система для поддержки виртуальных машин, включая виртуальные машины на Linux.
2	LANtastic	Б	Серверная операционная система с объектно-ориентированный

			интерфейсом OS/2 для создания мощного набора графических средств администратора.
3	Windows Server 2019	В	Сетевая операционная система и набор сетевых протоколов для взаимодействия с компьютерами-клиентами, подключёнными к сети
4	LAN server	Г	Сетевая операционная система для DOS, Windows,OS/2 с поддержкой технологии Ethernet, ARCNET и Token Ring

6. Установить соответствие типа файлов именам

1	…….doc	А	Файл запуска программы
2	…….exe	Б	Текстовый файл
3	…….bmp	В	Каталог
4	Сотрудники	Г	Графический файл

7. Установить соответствие имени рабочей области таблицы

1	Строки	А	Специальные символы
2	Столбцы	Б	Сочетание буквы и цифры
3	Ячейки	В	Английские буквы
4	Цифры	Г	Русские буквы

8. Установить соответствие расширения файла типу хранимой информации

1	…….jpg	А	Документ MS Word
2	…….txt	Б	Электронная таблица
3	…….doc	В	Текстовый документ
4	…….xls	Г	Фотография

9. Установить соответствие между способами и видами информации

1	По способу кодирования	А	Цифровая, аналоговая
2	По способу представления	Б	Визуальная, звуковая, документ
3	По способу обработки	В	Текстовая, графическая, числовая
4	По способу восприятия	Г	Непрерывная, дискретная

10. Установить соответствие названия протокола его назначению

1	FTP	А	Протокол передачи данных
2	SMTP	Б	Протокол передачи файлов
3	TCP/IP	В	Протокол передачи гипертекста
4	HTTP	Г	Протокол передачи почты

11. Установить соответствие оборудования его назначению

1	Репитер	А	Устройство для объединения ПК в сетях Ethernet
2	Концентратор	Б	Устройство для высокоскоростной коммутации пакетов между портами
3	Коммутатор	В	Устройство для подключения и соединения нескольких локальных сетей
4	Маршрутизатор	Г	Повторитель, усилитель сигналов

12. Установить соответствие между элементами ПК и функциями элементов

1	Процессор	А	Хранение информации
2	Оперативная память	Б	Обработка информации
3	Жесткий диск	В	Отображение информации
4	Монитор	Г	Ввод информации

Задания на установление правильной последовательности

1. Установить этапы разработки программного обеспечения:

1. Разработка алгоритма
2. Написание программы
3. Постановка задачи
4. Разработка математической модели

2. Установить этапы защиты от угроз безопасности:

1. Предоставление персоналу защищенный удаленный доступ к информационным ресурсам
2. Обеспечение безопасного доступа к открытым ресурсам внешних сетей и Internet
3. Защита внешних каналов передачи информации
4. Разработка политики информационной безопасности
5. Анализ угрозы безопасности

3. Установить этапы стадии исполнения компьютерных вирусов:

1. Выполнение деструктивных функций
2. Передача управления программе-носителю вируса
3. Поиск жертвы
4. Заражение найденной жертвы
5. Загрузка вируса в память

4. Установить этапы построения системы антивирусной защиты сети:

1. Реализация плана антивирусной безопасности
2. Проведение анализа объекта защиты и определение основных принципов обеспечения антивирусной безопасности
3. Разработка политики антивирусной безопасности
4. Разработка плана обеспечения антивирусной безопасности

5. Установить этапы разработки модели:

1. Построение модели

2. Объект

3. Корректировка модели

4. Анализ результатов

5. Исследование модели на компьютере

6. Установить в порядке убывания единицы измерения памяти:

1. 2 байта

2. 4 байта

3. 3 бита

4. 1 байт

7. Установить этапы построения программы обеспечения безопасности:

1. Проведение разъяснительных мероприятий и обучения персонала для поддержки требуемых мер безопасности

2. Регулярный контроль пошаговой реализации плана безопасности

3. Установление уровня безопасности

4. Формирование политики безопасности организации

5. Определение ценности технологических и информационных активов организации

8. Установить действия этапа анализа рисков:

1. Оценка вероятности того, что угроза будет реализована на практике

2. Оценка рисков технологических и информационных активов

3. Идентификация и оценка стоимости технологических и информационных активов

4. Анализ угроз, для которых технологические и информационные активы являются целевым объектом

9. Установить последовательность процессов для обнаружения и выдачи сигнала тревоги:

1. Одно системное событие не является неизбежно достаточным, чтобы

утверждать, что это опасность

2. Если результат этой совокупности превышает пороговую величину, выдается сигнал тревоги

3. Совокупность событий должна сравниваться с заранее установленной пороговой величиной

4. Каждое нарушение безопасности должно генерировать системное событие

10. Установить в порядке увеличения единицы измерения количества информации:

1. 1 ТБ

2. 30 Гбайт

3. 50 Килобайт

4. 100 Мегабайт

11. Установить в порядке возрастания функциональных возможностей:

1. WordPad

2. Блокнот

3. Microsoft Office Word

4. Corel Ventura Publisher

12. Расположить параметры для группировки данных на сервере сбора информации об атаке:

1. Дата, время

2. Протокол

3. Порт получателя

4. Номер агента

5. IP-адрес атакующего

6. Тип атаки

13. Расположить в порядке возрастания даты разработки стандартов информационной безопасности:

1. ISO 27001:2005

2. ISO/IEC 17799

3. ISO/IEC 15408

4. «Критерии оценки доверенных компьютерных систем»

14. Расположить этапы процесса управления рисками информационной безопасности:

1. Классификация рисков, выбор методологии оценки рисков и проведение оценки

2. Анализ угроз и их последствий, определение слабостей в защите

3. Выбор, реализация и проверка защитных мер

4. Оценка остаточного риска

5. Идентификация активов и ценности ресурсов, нуждающихся в защите

6. Выбор анализируемых объектов и степени детальности их рассмотрения

15. Расположить этапы проведения аудита информационной безопасности:

1. Разработка рекомендаций по повышению уровня защиты автоматизированной системы

2. Анализ полученных данных

3. Сбор исходных данных

4. Разработка регламента проведения аудита

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) 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

следующим образом:

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

Компетентностно-ориентированные задачи

1. Задача: Анализ политики допустимого использования (AUP)

- Ситуация: Вы — консультант по коммуникациям. Вам дали на ревью проект «Политики использования электронной почты и мессенджеров» для крупной компании. Текст написан техническим специалистом и перегружен сложными формулировками и жаргоном.
- Задание: Переработайте текст политики. Ваша цель — сделать его четким, понятным и однозначным для всех сотрудников (юристов, менеджеров, курьеров). Выделите 5 ключевых запретов и 5 разрешений, сформулировав их простым императивным языком. Объясните, почему ясность формулировок в таких документах является элементом безопасности.

2. Задача: Частотный анализ и дешифровка

- Ситуация: В историческом романе обнаружен зашифрованный дневник персонажа. Из контекста известно, что это моноалфавитный шифр (прямая замена) на английском языке. Фрагмент шифртекста: "BQQMZF, JMDFWJ! ZMFYMFE XJHWJY XYFD TZY NSAJX TWLJ ZSFQD..."
- Задание:

1. Проведите частотный анализ приведенного текста.
2. Сопоставьте с эталонной частотностью букв английского языка.
3. Предположите, какими буквами могут быть самые частотные символы.
4. Дешифруйте первую фразу, опираясь на знания языка (ищите артикли, предлоги, частотные слова).

3. Задача: Составление сценария фишингового письма

- Ситуация: Для проведения учебных учений по безопасности нужно создать правдоподобное фишинговое письмо, имитирующее рассылку от внутреннего IT-отдела с требованием «сменить пароль».
- Задание: Напишите текст такого письма. Проанализируйте и примените в тексте лингвистические маркеры, типичные для фишинга: (1) создание чувства срочности, (2) имитация официального стиля, (3) грамматические или стилистические ошибки, (4) призыв к немедленному действию. *После этого* поясните, по каким именно языковым признакам получатель мог бы опознать эту атаку.

4. Задача: Лингвистическая экспертиза инцидента

- Ситуация: В компании произошла утечка информации. Есть подозрение на внутреннего нарушителя. В распоряжении службы безопасности есть два документа: конфиденциальный меморандум и пост анонимного пользователя в соцсети, где раскрывается эта информация. Стилистически они очень похожи.
- Задание: Составьте перечень лингвистических параметров, по которым можно провести стилометрический анализ для установления авторства (например: лексические предпочтения, длина предложений, использование определенных синтаксических конструкций, знаков препинания, характерные ошибки). Не проводя сам анализ, объясните, как каждый параметр может

помочь в расследовании.

5. Задача: Проектирование инструкции для создания паролей

- Ситуация: Многие сотрудники используют слабые пароли по типу CompanyName2024!. Нужно создать новую, понятную инструкцию.
- Задание: Разработайте методичку «Как создать надежный и запоминающийся пароль». В основе методики должен лежать лингвистический принцип: преобразование запоминающейся фразы (например, строки из песни, пословицы) в пароль по определенным правилам (напр., Я люблю гулять в парке летом! -> #YlvgvpL2024!). Объясните, почему пароли, созданные на основе фраз, более устойчивы к взлому и удобны для запоминания, чем бессмысленные наборы символов.

6. Задача: Аудит правил межсетевого экрана

- Ситуация: Вам дан список правил файрвола для сервера, где размещен корпоративный сайт и база данных с локализациями продуктов (тексты на разных языках). Правила написаны на техническом языке: Разрешить TCP любой -> IP_сервера порт 80, Разрешить TCP IP_админ -> IP_БД порт 5432, Запретить TCP любой -> IP_БД порт 5432.
- Задание: Переведите эти правила с технического языка на естественный русский язык. Объясните смысл каждого правила простыми словами для нетехнического руководителя проекта. Например: «Это правило позволяет любому пользователю из интернета заходить на наш сайт».

7. Задача: Анализ угроз для лингвистического стартапа

- Ситуация: Стартап разрабатывает революционную нейросеть для перевода. Его ключевые активы: (1) уникальный набор данных для обучения (параллельные тексты), (2) алгоритмы, (3) база клиентов.
- Задание: Проведите мозговой штурм и составьте структурированный список качественных угроз для каждого актива. Сформулируйте угрозы не технически («DDOS-атака»), а в рамках бизнес-процессов и человеческого фактора («Уход ключего лингвиста-разработчика к конкурентам с копией датасета», «Нелегальное копирование данных партнерами для обучения собственных моделей», «Публикация исходного кода на GitHub по ошибке разработчика»).

8. Задача: Расшифровка сообщения с помощью шифра Виженера

- Ситуация: Известно, что сообщение XUOG JNTQZP ZC ZMZY XUOG зашифровано с помощью шифра Виженера. Ключевое слово — KEY.
- Задание: Используя таблицу Виженера (или алгебраический метод), расшифруйте сообщение. Опишите пошаговый процесс преобразования для первой буквы. Объясните, почему данный шифр устойчив к простому частотному анализу, который работает против шифра Цезаря.

9. Задача: Разработка сценария обучения по безопасности

- Ситуация: Нужно провести 15-минутный инструктаж для переводчиков по работе с конфиденциальными документами.
- Задание: Разработайте структуру и ключевые тезисы этого инструктажа. Включите в него не только правила («не пересылать на личную почту»), но и разбор реальных кейсов и формулировок, которые могут использоваться в социальной инженерии (например, как может звучать запрос злоумышленника, выдающего себя за коллегу из другого офиса). Сформулируйте эти примеры.

10. Задача: Оценка риска при внедрении нового инструмента

- Ситуация: Команда лингвистов просит разрешить использовать облачный онлайн-сервис на основе AI для проверки грамматики. Сервис бесплатный, но его политика конфиденциальности гласит, что «все загружаемые тексты могут использоваться для улучшения сервиса».
- Задание: Составьте краткий меморандум на имя руководителя проекта. Проанализируйте риски использования этого сервиса для обработки текстов, содержащих персональные данные или коммерческую тайну. Предложите альтернативы или условия использования (например, заключение NDA с вендором, использование только для неконфиденциальных текстов).

Шкала оценивания решения компетентностно-ориентированной задачи: 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 (установлено положением П 02.016).

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 следующим образом:

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

Критерии оценивания решения компетентностно-ориентированной задачи (нижеследующие критерии оценки являются примерными и могут корректироваться):

6-15 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 (последовательности (или выполнения) необходимых трудовых действий) и формулировку доказанного, правильного вывода (ответа); при этом обучающимся предложено несколько вариантов решения или оригинальное, нестандартное решение (или наиболее эффективное, или наиболее рациональное, или оптимальное, или единственно правильное решение); 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 общие фразы и (или) 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) значительное место занимают общие фразы и голословные рассуждения, и (или) задача не решена.