МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование ф-та полностью)
М.О. Таныгин
(подпись, инициалы, фамилия)
«. *29* » . *августа* .2023 г.

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

Прикладные математические задачи информационной безопасности
(наименование учебной дисциплины)

10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы »
(код и наименование ОПОП ВО)

Курск – 2023

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

Тема 1. Введение

1. Что такое искусственный интеллект и как он связан с нейронными сетями?
2. Какие преимущества и вызовы представляет собой использование нейронных сетей?
3. Каковы основные принципы функционирования нейронных сетей?
4. Какие области применения и потенциальные выгоды имеют нейронные сети?
5. Какова история развития искусственного интеллекта и нейронных сетей?
6. Какие факторы способствовали росту интереса к нейронным сетям в последние годы?
7. Какие были основные прорывы в исследовании искусственного интеллекта, приведшие к появлению нейронных сетей?
8. Какая роль нейронных сетей сыграла в развитии машинного обучения и глубокого обучения?
9. Какие исторические моменты в сфере искусственного интеллекта и нейронных сетей стали вехами в их развитии?
10. Какие вызовы и проблемы искусственного интеллекта и нейронных сетей были преодолены за последние годы?

Тема 2. Искусственные нейронные сети

1. Что является входом искусственного нейрона?
2. Что такое множество весовых значений нейрона?
3. Что означает величина NET?
4. Что означает величина OUT?
5. Что такое искусственный интеллект и как он связан с нейронными сетями?
6. Какие преимущества и вызовы представляет собой использование нейронных сетей?
7. Каковы основные принципы функционирования нейронных сетей?
8. Какие области применения и потенциальные выгоды имеют нейронные сети?
9. Какие компоненты составляют структуру искусственной нейронной сети?
10. Каким образом веса и смещения влияют на работу искусственной нейронной сети?

Тема 3. Алгоритмы обучения нейронных сетей

1. Сетью без обратных связей называется сеть?
2. Какие сети характеризуются отсутствием памяти?
3. Входом персептрона являются
4. Теорема о двухслойности персептрона утверждает, что?
5. Что такое искусственный интеллект и как он связан с нейронными сетями?
6. Какие преимущества и вызовы представляет собой использование нейронных сетей?
7. Каковы основные принципы функционирования нейронных сетей?
8. Какие области применения и потенциальные выгоды имеют нейронные сети?
9. Какие методы и стратегии можно применять для инициализации весов в нейронных сетях перед обучением?
10. Какие меры принимаются для предотвращения переобучения нейронных сетей?

Тема 4. Многослойные сети с обратным распространением информации

1. Какой должна быть активационная функция, для того чтобы возможно было применять алгоритм обратного распространения?
2. Обобщенным многослойным персептроном называется
3. Входным слоем обобщенного многослойного персептрона называется?
4. Скрытым слоем обобщенного многослойного персептрона называется?
5. Что такое искусственный интеллект и как он связан с нейронными сетями?
6. Какие преимущества и вызовы представляет собой использование нейронных сетей?
7. Каковы основные принципы функционирования нейронных сетей?
8. Какие области применения и потенциальные выгоды имеют нейронные сети?
9. Что такое градиентный спуск и как он применяется в обратном распространении ошибки?
10. Какие функции активации чаще всего используются в многослойных нейронных сетях и почему?

Тема 5. Нейронные сети в защите информации

1. Как называется информация, которую следует защищать (по нормативам, правилам сети, системы)?
2. Разновидностями угроз безопасности (сети, системы) являются
3. Относятся к правовым методам, обеспечивающим информационную безопасность
4. Основные источники угроз информационной безопасности

5. Что такое искусственный интеллект и как он связан с нейронными сетями?

6. Какие преимущества и вызовы представляет собой использование нейронных сетей?

7. Каковы основные принципы функционирования нейронных сетей?

8. Какие области применения и потенциальные выгоды имеют нейронные сети?

9. Какие методы аутентификации и идентификации могут быть улучшены с помощью нейронных сетей?

10. Какая роль играют нейронные сети в обнаружении аномалий и вредоносных программ в системах защиты информации?

Критерии оценки:

7-12 баллов (или оценка «отлично») 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.

2-6 баллов (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

1 балл (или оценка «удовлетворительно») 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 (или оценка «неудовлетворительно») 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.

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа № 1 «Функции активации нейронных сетей»

1. Активационной функцией называется
2. Матричное умножение XW вычисляет
3. Активационная функция применяется для
4. Значение активационной функции является
5. Что такое функция активации в контексте нейронных сетей?
6. Какие основные типы функций активации используются в нейронных сетях?
7. Как выбрать подходящую функцию активации для конкретной задачи машинного обучения?
8. Какие преимущества и недостатки у разных функций активации?
9. Как функции активации влияют на процесс обучения нейронной сети?
10. Какие новые функции активации были представлены в последние годы и какие преимущества они имеют?

Практическая работа № 2 «Геометрический метод обучения нейронных сетей»

1. В каком случае многослойные сети не могут привести к увеличению вычислительной мощности по сравнению с однослойной сетью?
2. Сетью без обратных связей называется сеть
3. Активационная функция называется "сжимающей", если
4. Слоем нейронной сети называется множество нейронов
5. Какие сети характеризуются отсутствием памяти?
6. Чем характеризуется геометрический метод обучения нейронных сетей?
7. В чем состоит основная идея геометрического метода обучения?
8. Какие инструменты и концепции используются в геометрическом методе обучения нейронных сетей?
9. Как геометрический метод обучения отличается от других методов обучения, например, градиентного спуска?
10. Какие преимущества и ограничения имеет геометрический метод обучения нейронных сетей?

Практическая работа № 3 «Правило Хебба обучения нейронных сетей»

1. Что в наибольшей степени влияет на результат работы нейронной сети?
2. Что является главным результатом Розенблатта?
3. Какую парадигму искусственного интеллекта реализуют нейронные сети?

4. К чему приводит отказ компонента (нейрона или синаптической связи) сети?

5. Что такое Правило Хебба в контексте обучения нейронных сетей?

6. Как сформулировано Правило Хебба?

7. Какое предположение лежит в основе Правила Хебба?

8. Каким образом Правило Хебба модифицирует веса связей между нейронами?

9. В каких случаях и при каких условиях применяется Правило Хебба?

10. Какие преимущества и ограничения имеет Правило Хебба в контексте обучения нейронных сетей?

Практическая работа № 4 «Правило Розеблатта. Псевдо обратные матрицы»

1. Что необходимо сначала выполнить для регрессионной идентификации линейных непрерывных систем управления?

2. В каком случае матрица входа дискретной модели управления будет рассчитываться более просто?

3. Что будет представлять собой матрица регрессоров при регрессионной идентификации непрерывной системы управления?

4. Из какого уравнения определяются оценки матриц дискретной системы управления?

5. Какой тип модуляции обычно применяется при дискретизации непрерывной системы управления?

6. Что такое Правило Розеблатта в контексте обучения нейронных сетей?

7. Как формулируется Правило Розеблатта?

8. В чем отличие Правила Розеблатта от Правила Хебба?

9. Что такое псевдообратная матрица?

10. Каким образом псевдообратные матрицы используются в контексте обучения нейронных сетей?

Практическая работа № 5 «Алгоритм Видроу-Хоффа»

1. Теория обучения Хэбба подразумевает:

2. В алгоритме обучения Хэбба предполагается обучение

3. В алгоритме Хэбба величина изменения синоптической связи между двумя нейронами зависит от?

4. Каков принцип работы алгоритма Видроу-Хоффа?

5. Какой тип задач решает алгоритм Видроу-Хоффа?

6. Какие шаги включает в себя процесс обучения с использованием алгоритма Видроу-Хоффа?

7. Какие преимущества имеет алгоритм Видроу-Хоффа по сравнению с другими методами обучения нейронных сетей?

8. Какие могут быть проблемы или ограничения при использовании алгоритма Видроу-Хоффа?

9. Каким образом происходит коррекция весовых коэффициентов в алгоритме Видроу-Хоффа?

10. В каких областях применяется алгоритм Видроу-Хоффа?

Практическая работа № 6 «Обучение ассоциативной памяти»

1. Какая память наиболее точно удерживает информацию:
2. Какая память является самой сильной и преобладающей:
3. Осмысленное запоминание достигается за счет?
4. Что такое ассоциативная память в контексте нейронных сетей?
5. Каким образом происходит обучение ассоциативной памяти?
6. Какие методы используются для установления ассоциативных связей в нейронной сети?
7. Какая роль синаптических весов в обучении ассоциативной памяти?
8. Каковы преимущества использования ассоциативной памяти в решении задач машинного обучения?
9. Существуют ли ограничения или проблемы при использовании ассоциативной памяти?
10. В каких областях применяется обучение ассоциативной памяти?

Практическая работа № 7«Алгоритм обратного распространения ошибок»

1. Что самое главное должно продумать руководство при классификации данных?
2. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
3. Что такое политики безопасности?
4. Что такое алгоритм обратного распространения ошибок и как он работает?
5. Какие компоненты включает в себя нейронная сеть при применении алгоритма обратного распространения ошибок?
6. Как вычисляются градиенты ошибки в алгоритме обратного распространения ошибок?
7. Каким образом корректируются весовые коэффициенты нейронов в алгоритме обратного распространения ошибок?
8. Какие факторы могут повлиять на эффективность алгоритма обратного распространения ошибок?
9. Какие проблемы могут возникнуть при использовании алгоритма обратного распространения ошибок?
10. Какие возможности и ограничения имеет алгоритм обратного распространения ошибок?

Практическая работа № 8«Нейросети в прогнозировании временных рядов»

1. Составляющие временного ряда следующие

2. Процедура выравнивания временного ряда включает в себя следующие этапы

3. В качестве показателей точности модели используют следующие

4. Какие особенности временных рядов делают прогнозирование сложной задачей?

5. Какие типы нейронных сетей широко используются для прогнозирования временных рядов?

6. Каким образом нейронные сети обрабатывают последовательность значений временного ряда?

7. Каковы шаги процесса обучения нейронной сети для прогнозирования временных рядов?

8. Как оценивается качество прогнозов, полученных с помощью нейросетей для временных рядов?

9. Какие факторы могут повлиять на точность прогнозирования временных рядов с использованием нейросетей?

10. В каких областях применяются нейронные сети для прогнозирования временных рядов?

Критерии оценки:

12-24 баллов (или оценка «отлично») 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.

2-11 баллов (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

1 балл (или оценка «удовлетворительно») 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 (или оценка «неудовлетворительно») 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.

1.3 ПРОИЗВОДСТВЕННЫЕ ЗАДАЧИ

1. Оценка стойкости пароля: Ваша компания хочет улучшить систему управления паролями для обеспечения безопасности доступа к информационным системам. Ваша задача состоит в разработке математической модели, которая будет оценивать стойкость паролей, основываясь на их длине, использовании различных символов, уникальности и других параметрах. Эта модель поможет определить слабые пароли и рекомендовать пользователям создавать более надежные пароли.

2. Моделирование атаки методом перебора: Ваша компания хочет оценить стойкость своей системы шифрования путем моделирования атаки методом перебора. Ваша задача состоит в разработке математической модели, которая будет оценивать время, необходимое для взлома шифра при различных сценариях атаки, учитывая мощность вычислительных ресурсов и сложность алгоритма шифрования. Это позволит компании оценить уровень стойкости своей системы и принять соответствующие меры по усилению безопасности.

3. Анализ времени выполнения алгоритмов шифрования: Ваша компания хочет оптимизировать процесс шифрования и дешифрования данных, чтобы обеспечить более эффективную работу информационной системы. Ваша задача состоит в математическом анализе времени выполнения различных алгоритмов шифрования в зависимости от объема данных и вычислительных ресурсов. На основе этого анализа вы можете рекомендовать использование наиболее эффективных алгоритмов для обеспечения быстрой и безопасной обработки данных.

4. Анализ ресурсов системы: Вам предстоит проанализировать ресурсы информационной системы производственного объекта, такие как процессорное время, память, пропускная способность сети и дисковое пространство. Задача состоит в математическом моделировании и определении оптимального распределения этих ресурсов для обеспечения безопасной работы системы при сохранении производительности.

5. Определение оптимального размера ключа: Ваша компания использует криптографические алгоритмы для защиты данных. Задача состоит в математическом анализе стойкости алгоритмов в зависимости от размера ключа и определении оптимального размера ключа для обеспечения требуемого уровня безопасности при минимальных вычислительных ресурсах.

6. Разработка и оптимизация алгоритмов хэширования: Вам предстоит разработать и оптимизировать алгоритмы хэширования для

обеспечения целостности данных в производственной системе. Задача включает математическое моделирование, анализ коллизий, определение оптимальной длины хэш-значения и разработку алгоритмов, устойчивых к атакам.

7. Оценка стойкости системы контроля доступа: Вам необходимо оценить стойкость системы контроля доступа к производственному объекту. Задача состоит в математическом анализе алгоритмов аутентификации и авторизации, определении вероятности несанкционированного доступа и предложении улучшений для повышения безопасности системы.

8. Разработка системы мониторинга инцидентов: Ваша задача - разработать систему мониторинга и анализа инцидентов информационной безопасности в производственной среде. Задача включает математическое моделирование, анализ данных, обнаружение аномалий и разработку алгоритмов для предотвращения и быстрого реагирования на инциденты безопасности.

9. Разработка системы аутентификации на основе односторонних функций: Вам предстоит разработать систему аутентификации, которая будет использовать математические односторонние функции, такие как хэш-функции или криптографические преобразования. Задача состоит в выборе подходящих функций, создании протокола аутентификации и математическом анализе его безопасности.

10. Реализация системы разделения секрета: Ваша задача - реализовать систему разделения секрета, которая будет использовать математические алгоритмы, такие как схемы Шамира. Задача включает в себя разделение секрета на несколько частей, распределение этих частей разным участникам и восстановление секрета только при наличии определенного количества частей.

Критерии оценки:

3-4 балла (или оценка «отлично») 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.

2 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

1 балл (или оценка «удовлетворительно») 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 (или оценка «неудовлетворительно») 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.

1.4 КЕЙС-ЗАДАЧИ

Кейс 1. Компания А занимается разработкой информационных систем и вам был поручен проект по разработке криптографического протокола для безопасной передачи данных между клиентским приложением и сервером. Ваша задача - создать математический алгоритм и протокол, который обеспечит конфиденциальность, целостность и аутентификацию данных.

Необходимо выполнить следующие задачи:

1) Выбор алгоритмов шифрования: Проанализируйте различные алгоритмы шифрования, такие как AES, RSA или ECC, и определите подходящие алгоритмы для защиты передаваемых данных. Рассмотрите их стойкость, эффективность и требования к вычислительным ресурсам.

2) Разработка ключевого обмена: Разработайте алгоритм и протокол для безопасного обмена ключами между клиентом и сервером. Обеспечьте конфиденциальность и аутентификацию ключей, используя асимметричное шифрование или другие методы.

3) Защита целостности данных: Разработайте методы для обеспечения целостности передаваемых данных. Используйте хэш-функции, цифровые подписи или другие криптографические методы для обнаружения возможных изменений данных в процессе передачи.

4) Реализация протокола: Опишите последовательность шагов протокола для безопасной передачи данных. Разработайте математические вычисления и операции, которые должны быть выполнены на каждом этапе протокола.

5) Тестирование и анализ протокола: Проведите тестирование разработанного протокола для оценки его безопасности и эффективности. Используйте различные тестовые сценарии и атаки, чтобы проверить устойчивость протокола к возможным угрозам.

6) Оценка стойкости: Проведите математическую оценку стойкости разработанного протокола. Анализируйте его уязвимости и возможности взлома с использованием различных атак. Предложите улучшения или модификации для повышения безопасности протокола.

Кейс 2. Компания Б использует облачное хранилище для хранения и обработки большого объема персональных данных своих клиентов. В связи с усилением требований к безопасности данных, вам необходимо разработать и реализовать математические методы и алгоритмы для защиты информации и обеспечения конфиденциальности данных в облачном хранилище.

Необходимо:

1) Разработка криптографического протокола: Разработайте криптографический протокол для обеспечения конфиденциальности и целостности данных, передаваемых между клиентом и облачным хранилищем. Используйте математические алгоритмы шифрования, хэширования и аутентификации для защиты данных.

2) Реализация схемы шифрования на стороне клиента: Разработайте математическую схему шифрования на стороне клиента, которая позволит зашифровать данные перед их передачей в облачное хранилище. Используйте асимметричные алгоритмы шифрования, такие как RSA или ECC, для обеспечения безопасности данных.

3) Распределение ключей: Разработайте метод распределения ключей между клиентом и облачным хранилищем. Используйте алгоритмы асимметричной и симметричной криптографии для обмена и установки общего секретного ключа.

4) Защита от атак на стороне облачного хранилища: Разработайте математические методы для защиты данных от возможных атак на стороне облачного хранилища, таких как атаки на основе словарей, перебора паролей или атаки с извлечением информации. Используйте алгоритмы хэширования, соли и другие методы для защиты от таких атак.

5) Оценка стойкости системы: Проведите оценку стойкости разработанных математических методов и алгоритмов. Используйте криптоанализ и другие методы для определения возможных уязвимостей системы и предложите улучшения для повышения ее безопасности.

Кейс 3. Компания В разрабатывает систему цифровой подписи для обеспечения безопасности электронных документов и транзакций. Однако, недавно были обнаружены попытки атаки подбором на цифровую подпись. Ваша задача - разработать и реализовать математические методы и

технологии, которые устойчивы к таким атакам и обеспечивают безопасность цифровой подписи.

Необходимо выполнить следующие задачи:

1) Анализ уязвимостей: Изучите существующие методы атаки подбором на цифровую подпись и их уязвимости. Оцените вероятность успешной атаки и потенциальные последствия для безопасности системы.

2) Разработка защищенной системы: Разработайте математические методы и технологии, которые устойчивы к атакам подбором на цифровую подпись. Включите в свою систему использование криптографически стойких хэш-функций, ключей достаточной длины и других математических механизмов, которые обеспечат безопасность подписи.

3) Реализация алгоритма: Реализуйте разработанный алгоритм и интегрируйте его в систему цифровой подписи. Проверьте его работоспособность и соответствие требованиям безопасности.

4) Тестирование и оценка производительности: Проведите тестирование разработанного алгоритма на тестовых данных и оцените его производительность. Измерьте время выполнения операций подписи и проверки подписи, а также ресурсоемкость алгоритма.

5) Анализ безопасности: Проведите анализ безопасности разработанного алгоритма и системы цифровой подписи в целом. Оцените стойкость системы относительно атак подбора и предложите улучшения, если необходимо.

6) Документирование результатов: Создайте документацию, в которой подробно описываются разработанный алгоритм, его реализация и результаты тестирования. Объясните принципы работы системы цифровой подписи и обеспечение безопасности от атак подбора.

Кейс 4. Компания Г занимается разработкой информационной безопасности и получила заказ от клиента на разработку криптографической системы для безопасной передачи конфиденциальной информации. Клиент работает с чувствительными данными, которые требуют высокого уровня защиты от несанкционированного доступа. Ваша задача - разработать и реализовать криптографическую систему, которая будет обеспечивать конфиденциальность и целостность передаваемых данных.

Необходимо выполнить следующие задачи:

1) Выбор криптографических алгоритмов: Проанализируйте различные криптографические алгоритмы, такие как блочные шифры, поточные шифры, асимметричные шифры и хэш-функции. Выберите

подходящие алгоритмы, которые обеспечат необходимый уровень безопасности для передаваемой информации.

2) Разработка протокола обмена ключами: Разработайте протокол обмена ключами, который будет использовать математические методы, такие как диффи-хеллмановский обмен ключами или эллиптическая криптография. Протокол должен обеспечивать безопасность передаваемых ключей и защиту от атак по перехвату.

3) Реализация шифрования данных: Разработайте алгоритм шифрования данных с использованием выбранных криптографических алгоритмов. Обеспечьте конфиденциальность и целостность данных при передаче и хранении. Учтите требования клиента относительно скорости и эффективности шифрования.

4) Разработка системы цифровой подписи: Разработайте систему цифровой подписи, которая позволит клиенту подтверждать подлинность и целостность передаваемых данных. Используйте асимметричные криптографические методы, такие как RSA или эллиптическая криптография, для создания и проверки цифровых подписей.

5) Тестирование и анализ безопасности: Проведите тестирование разработанной криптографической системы на наличие уязвимостей и атак.

Кейс 5. Компания Д была нанята, чтобы разработать систему электронного голосования для государственных выборов. Однако, важно обеспечить безопасность системы и предотвратить возможные атаки на процесс голосования и подмену результатов. Необходимо выполнить следующие задачи:

1) Разработка криптографического протокола: Разработайте протокол, который будет обеспечивать безопасную передачу данных между избирателями и системой электронного голосования. Используйте математические методы для защиты конфиденциальности и целостности данных, а также для обеспечения аутентификации участников.

2) Гарантирование анонимности голосования: Разработайте систему, которая будет гарантировать анонимность голосования, сохраняя одновременно возможность проверки правильности подсчета голосов. Используйте методы криптографии, такие как криптографические протоколы смешивания или протоколы доказательства знания для достижения этой цели.

3) Обеспечение безопасности системы: Разработайте математический алгоритм для обнаружения и предотвращения атак на систему электронного голосования. Включите в алгоритм методы

мониторинга и регистрации необычной активности, анализа целостности данных и обнаружения попыток взлома.

4) Оценка стойкости системы: Проведите математическую оценку стойкости разработанной системы электронного голосования. Используйте методы формального анализа, такие как вероятностные модели или методы анализа уязвимостей, для определения уровня безопасности системы и возможных уязвимостей.

5) Проведение пилотного проекта: Организуйте пилотный проект системы электронного голосования для оценки ее эффективности и безопасности. Включите в проект тестирование системы на отказоустойчивость, проверку аутентичности голосов и анонимность голосующих.

Критерии оценки:

5-8 баллов (или оценка «отлично») 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.

2-4 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

1 балл (или оценка «удовлетворительно») 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 (или оценка «неудовлетворительно») 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.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1.Какие операции применяются в шифре, определяемом ГОСТ 28147-89?

(1) нахождение остатка от деления на большое простое число

(2) циклический сдвиг

(3) сложение по модулю 2

(4) возведение в степень

(5) замена бит по таблице замен

2.Какова длина ключа в алгоритме, определяемом ГОСТ 28147-89?

(1) 48 бит

(2) 48 байт

(3) 56 бит

(4) 56 байт

(5) 64 бита

(6) 64 байта

(7) 256 бит

(8) Длина ключа может быть переменной в зависимости от используемого количества раундов

3.Какие шифры из перечисленных ниже относятся к композиционным шифрам?

(1) ГОСТ 28147-89

(2) DES

(3) шифр Вижинера

(4) шифр Цезаря

4.Алгоритм, определяемый стандартом ГОСТ 28147-89, является

(1) алгоритмом вычисления функции хеширования

(2) алгоритмом формирования электронной цифровой подписи

(3) блочным алгоритмом асимметричного шифрования

(4) блочным алгоритмом симметричного шифрования

5.Для решения задачи обнаружения искажений в зашифрованном массиве данных предусмотрен режим

(1) гаммирования

(2) операции сложения по модулю 2

(3) простой замены

(4) подстановки

(5) выработки имитовставки

6.Как называется комбинация бит, получаемая в одном из режимов использования ГОСТ 28147-89 и служащая для контроля изменений в зашифрованном сообщении?

(1) имитовставка

(2) гамма

(3) цифровая подпись

(4) подстановка

7.В каких режимах использования алгоритма ГОСТ 28147-89 возможно шифрование неполных блоков исходного текста?

(1) в режиме простой поблочной замены

(2) в режиме гаммирования

(3) в режиме гаммирования с обратной связью

(4) в режиме создания хеш-кода

8.Как называется режим использования блочного шифра, определяемого стандартом ГОСТ 28147-89, в котором каждый блок исходных данных шифруется независимо от остальных блоков с применением одного и того же ключа шифрования?

(1) режим простой замены

(2) режим гаммирования

(3) режим гаммирования с обратной связью

(4) режим создания хеш-кода

9.Что является особенностью использования режима простой замены блочного шифра, определяемого ГОСТ 28147-89?

(1) одинаковые блоки исходного текста преобразуются в одинаковый шифротекст

(2) одинаковые сообщения, состоящие из нескольких блоков, преобразуются в разный шифротекст

(3) сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока

(4) сообщение, зашифрованное в данном режиме, можно расшифровать, выбирая блоки шифротекста в произвольном порядке

(5) этот режим рекомендуется использовать для шифрования данных с размером, не кратным размеру блока (64 битам)

10.Что является особенностью использования режима гаммирования блочного шифра, определяемого ГОСТ 28147-89?

(1) одинаковые блоки исходного текста преобразуются в одинаковый шифротекст

(2) одинаковые сообщения при использовании разных векторов инициализации преобразуются в одинаковый шифротекст

(3) сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока

(4) этот режим можно использовать для шифрования данных с размером, не кратным размеру блока (64 битам)

(5) этот режим работает очень медленно, что практически не позволяет использовать его для обработки больших (> 1 Кбайт) исходных сообщений

11.Что является особенностью использования режима простой замены блочного шифра, определяемого ГОСТ 28147-89?

(1) этот режим позволяет создать комбинацию бит, служащую для контроля изменений в зашифрованном сообщении

(2) одинаковые сообщения, даже состоящие из нескольких блоков, преобразуются в одинаковый шифротекст

(3) сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока

(4) сообщение, зашифрованное в данном режиме, можно расшифровать, выбирая блоки шифротекста в произвольном порядке

(5) этот режим рекомендуется использовать для шифрования данных с размером, не кратным размеру блока (64 битам)

12.Какая операция наиболее быстро выполняется при программной реализации алгоритмов шифрования?

(1) сложения по модулю 2

(2) возведения в степень

(3) вычисления дискретных логарифмов

(4) нахождения остатка от деления на большое простое число

(5) умножения по модулю 232

(6) перестановки бит

13.Какой способ реализации криптографических методов обладает максимальной скоростью обработки данных?

(1) программный

(2) ручной

(3) аппаратный

14.Какие факторы влияют на стойкость блочного алгоритма шифрования?

(1) используемые операции

(2) длина ключа

(3) количество раундов

(4) год разработки

15.Что является основным недостатком программной реализации криптографических методов?

(1) небольшое быстродействие

(2) высокая стоимость разработки

(3) небольшая разрядность

(4) невозможность использования в современных беспроводных сетях

16.Каков российский стандарт на блочный алгоритм симметричного шифрования?

(1) ГОСТ 28147-89

(2) ГОСТ Р3410-94

(3) ГОСТ 3411-94

(4) DES

(5) AES

17.Что общего имеют все методы шифрования с закрытым ключом?

(1) в них для шифрования информации используется один ключ, а для расшифрования – другой ключ

(2) в них для шифрования и расшифрования информации используется один и тот же ключ

(3) в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов

(4) в них производится сложение символов исходного текста и ключа по модулю, равному числу букв в алфавите

18 .При каком алгоритме обучения обучающее множество состоит как из входных, так и из выходных векторов?

(1) "обучение с учителем"

(2) "обучение без учителя"

19.Как происходит обучение нейронной сети?

(1) эксперты настраивают нейронную сеть

(2) сеть запускается на обучающем множестве, и незадействованные нейроны выкидываются

(3) сеть запускается на обучающем множестве, и подстраиваются весовые значения

(4) сеть запускается на обучающем множестве, и добавляются или убираются соединения между нейронами

20."Обучение с учителем" это:

(1) использование знаний эксперта

(2) использование сравнения с идеальными ответами

(3) подстройка входных данных для получения нужных выходов

(4) подстройка матрицы весов для получения нужных ответов

21.Синапсами называются:

(1) точки соединения нейронов, через которые передаются нейронные сигналы

(2) "усики" нейронов, по которым проходят электрохимические сигналы

(3) тело нейрона, в котором происходит обработка электрохимического сигнала

22.Дендритами называются:
(1) точки соединения нейронов, через которые передаются нейронные сигналы

(2) "усики" нейронов, по которым проходят электрохимические сигналы

(3) тело нейрона, в котором происходит обработка электрохимического сигнала

23.Искусственный нейрон

(1) является моделью биологического нейрона

(2) имитирует основные функции биологического нейрона

(3) по своей функциональности превосходит биологический нейрон

24. В чем заключается обучение нейронной сети?
(1) в построении точного алгоритма решения задачи

(2) в минимизации штрафа, как неявной функции связей

25.На какие классы нейронные сети делятся по структуре?

(1) однослойные

(2) односвязные

(3) многослойные

(4) многосвязные

26.Каковы типичные приложения нейронных сетей?

(1) классификация образов

(2) обработка символьных строк

(3) ассоциативная память

27.Какие из перечисленных ниже свойств характерны для нейронных сетей?

(1) массовый параллелизм обработки информации

(2) функционирование по заданному алгоритму

(3) устойчивость к шумам и искажениям сигналов

(4) обобщение результатов обучения

(5) чувствительность к искажениям данных и повреждениям аппаратуры

28.Какую функцию реализует ассоциативная память?

(1) классифицирует входной объект

(2) восстанавливает полный образ по частичным данным

(3) задает соответствие между нейронами и входными объектами

29.Какие из нижеперечисленных особенностей присущи традиционным вычислительным системам?

(1) необходимо точное описание алгоритма

(2) искажения данных не влияют существенно на результат

(3) каждый обрабатываемый объект явно указан в памяти

30.Что представляет собой задачник при обучении нейронных сетей?

(1) набор примеров с заданными ответами

(2) набор нерешенных задач

31.Как нейрон МакКаллока-Питса определяет свое состояние?

(1) сравнивает взвешенную сумму входных сигналов с порогом

(2) вычисляет значение непрерывной функции от взвешенной суммы входных сигналов

32.В каких областях применяются нейрокомпьютеры?

(1) для решения задач искусственного интеллекта

(2) в системах управления и технического контроля

(3) для создания спецвычислителей параллельного действия

(4) как инструмент изучения человеческого мозга

(5) для построения компиляторов программ

33.Какие состояния имеют нейроны МакКаллока-Питса?
(1) любое значение из интервала (0,1)

(2) 0 и 1

34.Как должен изменяться вес входа нейрона по правилу Хебба?
(1) вес входа должен уменьшаться при корреляции между входом и выходом нейрона

(2) вес входа должен увеличиваться при корреляции между входом и выходом нейрона

35.Какое изменение управляющего воздействия в пределах одного такта квантования обычно применяется при дискретизации непрерывной системы?
(1) управление меняется по квадратичному закону

(2) управление меняется по линейному закону

(3) управление меняется по нелинейному закону

(4) управление остается постоянным

36.Что необходимо предпринять в случае неполного ранга матрицы регрессоров при регрессионной идентификации дискретной системы управления?
(1) необходимо из матрицы регрессоров удалить линейно зависимые столбцы

(2) необходимо из матрицы регрессоров удалить линейно зависимые строки

(3) необходимо использовать псевдообратную матрицу

(4) необходимо использовать матрицу Мура - Пенроуза

37.Сколько специальных свойств имеет матрица Мура - Пенроуза?
(1) одно

(2) два

(3) три

(4) четыре

(5) пять

38.Какими уравнениями описывается модель дискретной во времени системы управления?
(1) обыкновенными дифференциальными

(2) дифференциальными уравнениями в частных производных

(3) разностными

(4) конечными

39.Какой будет размерность матрицы коэффициентов дискретной системы управления, если размерность вектора состояний непрерывной системы управления равна $n \times 1$, а размерность вектора управления $r \times 1$?
(1) $n \times r$

(2) $n \times n$

(3) $r \times n$

(4) $r \times r$

39.Какова размерность информационной матрицы в задаче регрессионной идентификации непрерывной системы управления при размерности век-тора состояния $n \times 1$ и размерности вектора управления $r \times 1$?
(1) $n \times n$

(2) $(n + r) \times r$

(3) $(n + r) \times (r + n)$

(4) $(r + r) \times (r + r)$

(5) $(n + n) \times (n + n)$

(6) $(n + r) \times (n + r)$

40.Какая матрица системы MATLAB может быть использования для формирования матрицы коэффициентов дискретной системы управления?
(1) expfit

(2) expm

(3) exp

(4) expinv

41.В каком случае детерминант информационной матрицы равен нулю при регрессионной идентификации непрерывной системы управления?
(1) когда она хорошо обусловленная

(2) когда она плохо обусловленная

(3) когда она является неособенной

(4) когда она является особенной

41.В каком случае приходиться применять операцию интегрирования при модельном расчете матрицы входа дискретной системы управления?
(1) когда информационная матрица вырожденная

(2) когда матрица коэффициентов непрерывной системы вырожденная

(3) когда матрица коэффициентов непрерывной системы управления несингулярная

(4) когда матрица коэффициентов непрерывной системы сингулярная

(5) когда матрица коэффициентов непрерывной системы управления имеет свою обратную матрицу

42.Что понимается под верификацией в задаче регрессионной идентификации непрерывной системы управления?
(1) проверка величины детерминанта информационной матрицы

(2) проверка ранга информационной матрицы

(3) проверка реакций идентифицированной системы и реальной системы при различных управляющих воздействиях

(4) проверка собственных чисел матрицы коэффициентов идентифицированной системы и реальной системы

43.С помощью какой функции системы MATLAB можно определить полюса модели дискретной системы управления?
(1) edit

(2) eig

(3) pole

(4) poly

(5) такой функции нет

44.Какая матричная операция используется при формировании информационной матрицы при регрессионной идентификации непрерывной системы управления?
(1) операция псевдообращения

(2) операция транспонирования

(3) операция триангуляции

(4) операция приведения к нижней треугольной матрице

(5) операция приведения к верхней треугольной матрице

45.Какая функция системы MATLAB применяется для модельного определения матрицы входа в случае особенной матрицы коэффициентов непрерывной системы управления?
(1) inf

(2) inline

(3) int

(4) imag

(5) interpn

46.Какая функция системы MATLAB применяется для построения переходной функции дискретной системы управления?
(1) stem

(2) impulse

(3) step

(4) plot

47.Чему будет равняться размерность матрицы регрессоров в задаче регрессионной идентификации непрерывной системы n-го порядка с одним управляющим воздействием при наличии выходного сигнала на протяжении k отсчетов времени?

(1) $(n+k) \times (n+k)$

(2) $k \times n$

(3) $k \times (n+k)$

(4) $(n+1) \times (n+1)$

(5) $k \times (n+1)$

48.Сколько k отсчетов времени необходимо для регрессионной идентификации дискретной системы управления размерности n с m входными управляющими воздействиями?

(1) k < (n + m)

(2) k > (n + m)

(3) k = n

(4) k = m

49.В каких случаях необходима параметрическая идентификация систем управления?

(1) когда необходимо определить входные сигналы по известным выходным

(2) когда необходимо определить статический коэффициент передачи системы

(3) когда необходимо определить постоянные матрицы коэффициентов и входа по известным входным и выходным сигналам

(4) когда для известной модели системы управления необходимо определить ее постоянные коэффициенты соответствующих дифференциальных уравнений по входным и выходным сигналам

50.С помощью какой функции системы MATLAB осуществляется переход от матрицы коэффициентов дискретной системы управления к матрице коэффициентов непрерывной системы?
(1) lcm

(2) log

(3) loglog

(4) logm

51.Каким образом осуществляется переход от матрицы входа дискретной системы управления к матрице входа непрерывной системы при малом шаге квантования?
(1) матрицу входа дискретной системы логарифмируют

(2) матрицу входа дискретной системы потенцируют

(3) матрицу входа дискретной системы делят на шаг квантования

(4) матрицу входа дискретной системы умножают на шаг квантования

(5) матрицу входа дискретной системы умножают на ее транспонированную матрицу

52. Что относится к виду запоминания:
а) объем памяти
б) воспроизведение
в) осмысление
53. Информация, которая хранится в генотипе:
а) внутренняя память
б) моторная память
в) образная память
54. Запоминание может быть:
а) непреднамеренное
б) многократное
в) случайное
55. Факторы, влияющие на воспроизведение:
а) настроение
б) общее состояние
в) забывчивость
56. К видам памяти относятся:
а) произвольная и непроизвольная
б) распределенная и устойчивая
в) преактивная и ретроактивная

57. Зрительная память относится к следующему типу:
а) логическая память
б) образная память
в) кратковременная память
58. Сколько в среднем слов за раз может запомнить человек:
а) 5 – 9
б) 3 – 4
в) 17 – 20
59. Что такое мнемотехнические приемы:
а) перевод информации в образы, картинки
б) длительное сохранение информации
в) специальные приемы для облегчения запоминания

Задания в открытой форме

1. В алгоритме обучения Хэбба предполагается обучение…
2. В алгоритме Хэбба величина изменения синоптической связи между двумя нейронами зависит…
3. В алгоритме сигнального обучения Хэбба величина синоптической связи между двумя нейронами зависит…
4. Метод дифференциального обучения Хэбба заключается в том, что в нем для изменения синоптических связей учитываются…
5. Входная звезда Гроссберга используется для…
6. Выходом входной звезды Гроссберга является…
7. Выходом выходной звезды Гроссберга является…
8. Хорошо обученная входная звезда Гроссберга способна реагировать…
9. В алгоритме обучения выходной звезды Гроссберга величина синоптической связи между двумя нейронами зависит…
10. Алгоритм обучения персептрона является…
11. В алгоритме обучения персептрона величина изменения синоптической связи между двумя нейронами зависит…
12. При обучении персептрона предполагается обучение…
13. Обучение персептрона считается законченным, когда…
14. Метод обучения Уидроу-Хоффа отличается от метода обучения персептрона…
15. В статистических алгоритмах обучения величина изменения синоптической связи между двумя нейронами зависит…
16. Статистические методы обучения являются…
17. В статистических алгоритмах обучения искусственная температура используется для…
18. Самоорганизующиеся сети используются для…
19. В алгоритме обучения Кохонена обучению подвергаются…
20. Алгоритм обучения Кохонена является…

Задания на установление соответствия

1. Установить соответствие:

1) Криптосистема	a) Раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства анализа криптосистемы или её входных и выходных сигналов с целью извлечения конфиденциальных параметров, включая открытый текст;
2) Криптоанализ	b) Система, реализованная программно, аппаратно или программно - аппаратно и осуществляющая криптографическое преобразование информации;
3) Криптография	c) Раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства преобразования информации (шифрования) в целях сокрытия её содержания, предотвращения или несанкционированного использования.

2. Установить соответствие длины ключа:

1) AES	a) 256 бит
2) DES	b) Переменная
3) ГОСТ 28147-89	c) 56 бит

3. Установить соответствие:

1) Чему равен результат выполнения побитовой операции «сумма по модулю 2» для двоичных чисел 10101100 и 11001010?	a) 01000101
2) Чему равен результат выполнения побитовой операции «сумма по модулю 2» для десятичных чисел 250 и 191?	b) 10100011
3) Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 9E и	c) 00111101

0A3?	

4. Установить соответствие:

1) Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 0B5 и 37?	a) 10000010
2) Чему равна сумма по модулю 28 двоичных чисел 10101100 и 11001010?	b) 01110110
3) Чему равна сумма по модулю 28 двоичных чисел 01011001 и 11111010?	c) 01010011

5. Установить соответствие:

1) Чему равна сумма по модулю 28 десятичных чисел 250 и 191?	a) 10111001
2) Чему равна сумма по модулю 28 шестнадцатеричных чисел 9E и 0A3?	b) 01000001
3) Чему равна сумма по модулю 28 шестнадцатеричных чисел 0B5 и 37?	c) 11101100

6. Установить соответствие:

1) Чему равен результат выполнения операции циклического сдвига влево на 5 разрядов для двоичного числа 10101100?	a) 10010101
2) Чему равен результат выполнения операции циклического сдвига вправо на 5 разрядов для двоичного числа 01011001?	b) 11001010
3) Чему равен результат выполнения операции циклического сдвига влево на 5 разрядов для шестнадцатеричного числа 0B5?	c) 10110110

7. Установить соответствие:

1) Чему равен результат выполнения операции циклического сдвига	a) 10011011

влево на 7 разрядов для одного байта, хранящего шестнадцатеричное значение 37?	
2) Чему равен результат выполнения операции циклического сдвига вправо на 2 разряда для одного байта, хранящего шестнадцатеричное значение 55?	b) 01010101
3) 11) Чему равна сумма по модулю 28 шестнадцатеричных чисел 9E и 0A3?	c) 01000001

8. Установить соответствие:

1) Угроза безопасности	a) Это некая неудачная характеристика системы, которая делает возможным возникновение угрозы.
2) Уязвимость	b) Это угроза раскрытия информации.
3) Атака	c) Это потенциально возможное происшествие, которое может оказать воздействие на информацию в системе.
4) Угроза конфиденциальности	d) Это действие по использованию уязвимости; реализация угрозы.

9. Установить соответствие:

1) Линейная структура процесса вычислений	a) Предполагает, что для получения результата некоторые действия необходимо выполнить несколько раз.
2) Разветвленная структура процесса вычислений	b) Предполагает, что конкретная последовательность операций зависит от значений одной или нескольких переменных.
3) Циклическая структура процесса вычислений	c) Предполагает, что для получения результата необходимо выполнить некоторые операции в определенной последовательности.

10. Установить соответствие:

1) Правильность	a) Возможность проверки получаемых результатов;
2) Универсальность	b) Обеспечение полной повторяемости результатов, т. Е. Обеспечение их правильности при наличии различного рода сбоев;
3) Надежность	c) Обеспечение правильной работы при любых допустимых данных и защиты от неправильных данных;
4) Проверяемость	d) Функционирование в соответствии с техническим заданием;

10.Установить соответствие между элементами и функциями

1	Идентификация рисков	А	Сравнение уровней рисков с критериями сравнения рисков и критериями принятия рисков
2	Оценка опасности рисков	Б	Формируется и утверждается руководством список принимаемых рисков
3	Принятие рисков	В	выявление последствий реализации угроз нарушения конфиденциальности / целостности / доступности ИТ-активов
4	Поддержка и улучшение процесса управления рисками ИБ	Г	Контекст, оценка и план обработки рисков должны оставаться релевантными текущей ситуации и обстоятельствам

11. Установить соответствие угроз безопасности информации в локальных размерах

1	Компьютерные вирусы	А	нарушающие информационную безопасность. Они оказывают воздействие на информационную систему одного компьютера или сети ПК после попадания в программу и самостоятельного размножения. Вирусы способны остановить действие системы, но в

			основном они действуют локально;
2	«Черви»	Б	модификация вирусных программ, приводящая информационную систему в состояние блокировки и перегрузки. ПО активируется и размножается самостоятельно, во время каждой загрузки компьютера. Происходит перегрузка каналов памяти и связи
3	«Троянские кони»	В	программы, которые внедряются на компьютер под видом полезного обеспечения. Но на самом деле они копируют персональные файлы, передают их злоумышленнику, разрушают полезную информацию

12.Установить соответствие

1	Информация как предмет труда	А	это первичные исходные данные, сведения в конкретной сфере деятельности и смежных с нею областях
2	Информация как средство труда	Б	это совокупность знаний, данных и приемов, при помощи которых исходная информация (предмет труда) может быть наиболее эффективным образом обработана в целях получения запланированного результата
3	Информация как результат	В	должна обладать потребительскими свойствами, то есть снижать неопределенность ситуации или риск, в которой оказался субъект
4	Продукция индустрии информации	Г	в укрупненном виде может быть подразделена на продукты (вычислительная техника, офисное оборудование, коммуникационное оборудование, программное обеспечение, информационный продукт) и услуги (техническое обслуживание, сопровождение программного обеспечения,

			обучение и консультации, услуги связи, услуги по обработке данных).

13. Установить соответствие между

1	Перехват паролей	А	мошенничество возможно с участием специальных программ, которые имитируют на экране монитора окошко для ввода имени и пароля. Введенные данные попадают в руки злоумышленника, и далее на дисплее появляется сообщение о неправильной работе системы.
2	«Маскарад»	Б	действия в информационной системе от лица другого человека в сети компании. Существуют такие возможности реализации планов злоумышленников в системе -передача ложных данных в системе от имени другого человека
3	Незаконное использование привилегий	В	название разновидности хищения информации и подрыва безопасности информационной системы говорит само за себя

14.Установить соответствие между процедурами управления оперрисками

1	Идентификация риска	А	Информирование СУОР о реализации событий , Регистрацию событий ОР
2	Операционный риск	Б	систематическое использование информации для установления опасностей относительно аспекта риска или для описания проблемы
3	Сбор и регистрация событий и потерь	В	риск, связанный с выполнением компанией бизнес-функций, включая риски мошенничества и внешних событий

15. Установить соответствие между основными принципы защиты информации

1	Принцип законности	А	необходимо нормативно- правовое регулирование этой области общественных отношений. Законодательно должны быть обозначены права различных субъектов в области защиты информации
2	Принцип защиты информации	Б	основополагающие идеи, важнейшие рекомендации по организации и осуществлению этой деятельности на различных этапах решения задач сохранения секретов
3	Принцип приоритета	В	объектом засекречивания не могут быть сведения, которые государство обнародует или сообщает согласно конвенциям или соглашениям
4	Принцип собственности и экономической целесообразности	Г	право собственникам информации принимать меры к защите этой информации, а также оценивать ее потребительские свойства

16.Установить соответствие между

1	Процедуры управления операционным риском	А	анализ базы событий самооценка анализ динамики количественных показателей (ключевых индикаторов риска) анализ результатов регуляторных проверок анализ результатов внешнего аудита анализ поступающих сигналов от сотрудников.
2	Сбор и регистрация информации о событиях операционного риска:	Б	автоматизированное (из информационных систем), неавтоматизированное (экспертным методом),

			алгоритмизированное выявление информации о рисках классификация рисковых событий оценка потерь, стоимости возмещения потерь регистрация рисковых событий в базе событий обновление информации, актуализация источников информации.
3	Мониторинг рисков:	В	анализ индикаторов риска и статистики контроль выполнения мероприятий мониторинг входящей информации.

17. Установить соответствие между элементами и функциями

1	Скрытие	А	метод защиты информации является в основе своей реализации на практике одним из основных организационных принципов защиты ин- формации - максимального ограничения числа лиц, допускаемых к секретам
2	Ранжирование	Б	метод защиты информации является частным случаем метода скрытия и включает в себя, во-первых, деление засекречиваемой ин- формации по степени секретности, и, во-вторых, регламентацию допуска и разграничение доступа к защищаемой информации
3	Дезинформация	В	распространении заведомо ложных сведений относительно истинного назначения каких-либо объектов и изделий, действительного состояния какой-то области

			государственной деятельности

18.Установить соответствие между элементами и функциями

1	В основные задачи управления ИБ входят	А	периметр безопасности сети
2	Компоненты архитектуры безопасности включают	Б	распределять административные роли по типам и группам устройств
3	Подсистемы управления обновлениями позволяют автоматизировать следующие задачи	В	управление доступом к базе данных
4	Использование централизованного управления рабочими станциями и серверами позволяет	Г	контроль времени обновления ПО

19. Установить соответствие между элементами и функциями

1	Дробление	А	знание какой-то одной части информации не позволяет восстановить всю технологию в целом
2	Кодирование	Б	метод защиты информации, преследующий цель скрыть от соперника содержание защищаемой информации и заключающийся в преобразовании с помощью кодов открытого текста в условный при передаче информации по каналам связи
3	Шифрование	В	метод защиты информации, используемый при передаче сообщений с помощью различной радиоаппаратуры, направлении письменных сообщений и в других случаях, когда есть опасность перехвата этих сообщений соперником
4	Страхование	Г	метод защиты информации сводится к тому, чтобы защитить права и интересы собственника информации или средства информации как от традиционных угроз

20.Установить соответствие между этапами алгоритма проведения экспертизы ИС предприятия и их описанием

1	Формулирование цели экспертизы и определение ее объектов	А	Проверка соответствия предъявляемым к ней требованиям безопасности
2	Формирование аналитической группы	Б	Подготовка экспертизы, оказание помощи в проведении оценки, обработке и анализе ее результатов
3	Утверждение состава экспертной группы	В	Определение области компетенций
4	Подготовка необходимой информации об объектах экспертизы	Г	Получение информации от персонала, изучение документации

Задания на установление правильной последовательности

1. Установить этапы построения программы обеспечения безопасности:
   1) Формирование политики безопасности организации
   2) Проведение разъяснительных мероприятий и обучения персонала для поддержки требуемых мер безопасности
   3) Регулярный контроль пошаговой реализации плана безопасности
   4) Установление уровня безопасности
   5) Определение ценности технологических и информационных активов организации

2. Выберите правильную последовательность этапов защиты информации:
   1) Анализ рисков для активов организации, включающий в себя выявление ценных активов и оценку возможных последствий реализации атак с использованием скрытых каналов
   2) Реализация защитных мер по противодействию скрытых каналов
   3) Организация контроля за противодействием скрытых каналов.
   4) Выявление скрытых каналов и оценка их опасности для активов организации

3. Выберите правильную последовательность этапов процесса управления рисками:
   1) Идентификация активов и ценности ресурсов, нуждающихся в защите;
   2) Анализ угроз и их последствий, определение слабостей в защите;

3) Классификация рисков, выбор методологии оценки рисков и проведение оценки;
4) Выбор, реализация и проверка защитных мер;
5) Оценка остаточного риска;
6) Выбор анализируемых объектов и степени детальности их рассмотрения;

4. Выберите последовательность проведения моделирования угроз:
   1) Определение негативных последствий от угроз безопасности информации.
   2) Определение объектов воздействия угроз безопасности информации.
   3) Оценка возможности реализации угроз и их актуальности.

5. Установите этапы процессной модели:
   1) Проверка.
   2) Планирование.
   3) Реализация
   4) Действие.

6. Установите последовательность этапов:
   1) Характеризуется внедрением электромеханических устройств в работу шифровальщиков. При этом продолжалось использование полиалфавитных шифров.
   2) Период перехода к математической криптографии.
   3) Характеризуется господством моноалфавитных шифров (основной принцип – замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами).
   4) Ознаменовался введением в обиход полиалфавитных шифров.
   5) Отличается зарождением и развитием нового направления – криптография с открытым ключом.

7. Установите последовательность этапов:
   1) Наивная криптография..
   2) Формальная криптография.
   3) Научная криптография.
   4) Компьютерная криптография.

8. Установите последовательность этапов шифрования текста методом «атбаш»:
   1) Выделить каждую букву исходного текста;
   2) Определить номер буквы, шифрующей каждую букву исходного текста, учитывая особенность метода;

3) Определить букву алфавита с номером;
4) Определить её номер в алфавите;

9. Установите последовательность этапов шифрования алгоритмом Цезаря:
   1) Выделить каждую букву исходного текста;
   2) Определить её номер в алфавите;
   3) Определить номер буквы, шифрующей каждую букву исходного текста, учитывая величину сдвига;
   4) Определить букву алфавита с номером, полученным на этапе..

10. Установите последовательность этапов шифрования алгоритмом Виженера:
   1) Выделить каждую букву исходного текста;
   2) Определить её номер в алфавите;
   3) Выделить каждую букву ключа шифрования;
   4) Сопоставить её соответствующей букве исходного текста;

11. Установите последовательность этапов шифрования алгоритмом Виженера:
   1) Определить номер каждой буквы ключа шифрования в алфавите;
   2) Определить номер буквы, шифрующей каждую букву исходного текста;
   3) Определить букву алфавита с номером, полученным на этапе…

12. Установить этапы реализации в ОС механизмов безопасности в порядке их внедрения:
1. Создание кольцевой системы защиты процессора
2. Реализация аутентификации пользователя
3. Реализация многозадачности
4. Создание виртуальных контейнеров для запуска приложений

13. Расположить параметры для группировки данных в журнале брандмауэра информации об атаке:
1. Дата, время
2. Протокол
3. Порт получателя
4. Номер агента
5. IP-адрес атакующего
6. Тип атаки

14. Расположить этапы процесса управления рисками информационной безопасности:

1. Описание методов YCL к ресурсам ОС
2. Формирование атрибутов безопасности и прав доступа субъектов
3. Выбор, реализация и проверка защитных мер
4. Анализ журналов безопасности ОС
5. Идентификация активов и ценности ресурсов, нуждающихся в защите

15. Выберите правильную последовательность этапов по созданию системы защиты персональных данных:
1. Опытная и промышленная эксплуатация
2. Проектный этап
3. Аттестация или декларирование
4. Предпроектный этап

16. Выберите правильную последовательность этапов разработки профиля защиты.
1. Анализ среды применения ИТ-продукта с точки зрения
2. безопасности.
3. Выбор профиля-прототипа.
4. Синтез требований.

17. Выберите правильную последовательность этапов защиты информации, информационных технологий и автоматизированных систем от атак:
1. Анализ рисков для активов организации, включающий в себя выявление ценных активов и оценку возможных последствий реализации атак с использованием скрытых каналов
2. Реализация защитных мер по противодействию скрытых каналов
3. Организация контроля за противодействием скрытых каналов.
4. Выявление скрытых каналов и оценка их опасности для активов организации

18. Выберите последовательность уровней защищенности персональных данных
1. специальные категории ПДн
2. биометрические ПДн
3. общедоступные ПДн
4. иные категории ПДн

19. Выберите последовательность уровней безопасности информации:
1. Административный уровень
2. Процедурный уровень
3. Программно-технический уровень
4. Законодательный уровень

20. Выберите правильную последовательность этапов построения политики безопасности:

1. Выбор и установка средств защиты;
2. Организация обслуживания по вопросам информационной безопасности;
3. Создание системы периодического контроля информационной безопасности
4. Обследование информационной системы на предмет установления организационной и информационной структуры и угроз безопасности информации;
5. Подготовка персонала работе со средствами защиты;

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

2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

1. Криптографический алгоритм: Ваша задача состоит в разработке и анализе криптографического алгоритма для защиты конфиденциальных данных. Используя математические принципы, разработайте алгоритм шифрования, который обеспечит высокую стойкость и безопасность передаваемой информации.

2. Анализ времени выполнения алгоритма: Вам нужно провести анализ времени выполнения алгоритма шифрования для оценки его эффективности и применимости в информационной безопасности. Используйте математические методы и модели для определения скорости и сложности алгоритма, а также для оптимизации его производительности.

3. Криптографический протокол: Ваша компания разрабатывает криптографический протокол для безопасной передачи данных между клиентами и сервером. Ваша задача состоит в математическом моделировании и анализе протокола для обеспечения его надежности, конфиденциальности и целостности данных.

4. Методы стеганографии: Вам предстоит разработать математические методы стеганографии для скрытой передачи информации в цифровых медиафайлах. Ваша задача состоит в разработке алгоритмов, которые позволят эффективно внедрять и извлекать скрытую информацию, используя математические принципы и модели.

5. Оценка стойкости криптосистемы: Вам предоставлена криптосистема, и ваша задача - провести математическую оценку ее стойкости. Используйте методы анализа сложности атак и математическую криптоанализ, чтобы определить уровень безопасности системы и рекомендовать необходимые улучшения или модификации.

6. Шифрование и дешифрование: Разработайте математическую модель для шифрования и дешифрования данных. Используйте различные алгоритмы, такие как шифр Цезаря, шифр Виженера или асимметричное шифрование RSA. Задача состоит в разработке и реализации математических операций, которые позволят надежно зашифровывать и расшифровывать данные.

7. Анализ уязвимостей: Примените математические методы для анализа уязвимостей в информационной системе. Разработайте модели угроз и уязвимостей, используя статистические данные и методы анализа. Задача состоит в определении наиболее вероятных уязвимостей и их потенциального влияния на систему, а также в разработке стратегий предотвращения и устранения уязвимостей.

8. Криптоанализ: Разработайте методы и алгоритмы криптоанализа для анализа и взлома шифров. Используйте математические методы, такие как статистический анализ, анализ частоты символов или методы линейного и дифференциального криптоанализа. Задача состоит в разработке методов атаки на шифры и восстановлении исходных данных из зашифрованных сообщений.

9. Моделирование атак: Разработайте математические модели для моделирования различных типов атак на информационную систему. Используйте теорию игр, стохастические процессы или методы оптимизации для анализа и определения оптимальных стратегий защиты. Задача состоит в определении наиболее вероятных атак и разработке превентивных мер, чтобы усилить безопасность системы.

10. Шифрование данных: Разработка и анализ математических алгоритмов шифрования для обеспечения конфиденциальности данных. Задача состоит в разработке новых криптографических алгоритмов или анализе существующих, чтобы обеспечить надежную защиту передаваемой информации.

11. Криптографические протоколы: Разработка и анализ математических моделей и протоколов для обеспечения безопасной передачи данных и аутентификации. Задача заключается в разработке протоколов, которые гарантируют конфиденциальность, целостность и аутентичность информации, используя математические методы и алгоритмы.

12. Анализ уязвимостей: Применение математических методов и моделей для анализа уязвимостей информационных систем и идентификации потенциальных угроз безопасности. Задача состоит в применении математических моделей и статистических методов для определения уязвимых мест в системе и разработке соответствующих мер безопасности.

13. Криптоанализ: Исследование и анализ криптографических алгоритмов с целью обнаружения слабостей и возможности взлома. Задача заключается в использовании математических методов и вычислительных алгоритмов для анализа криптографических алгоритмов и поиска уязвимостей, которые могут быть использованы злоумышленниками.

14. Распределенные системы безопасности: Разработка и анализ математических моделей и алгоритмов для обеспечения безопасности в распределенных информационных системах. Задача состоит в разработке моделей безопасности, которые учитывают особенности распределенных систем, таких как отказоустойчивость, масштабируемость и аутентификация.

15. Шифрование RSA: Вам предстоит разработать и реализовать алгоритм шифрования RSA для обеспечения безопасности передачи данных. Задача состоит в выборе простых чисел p и q, вычислении модуля n = p * q, выборе открытого ключа и закрытого ключа, а также разработке алгоритма шифрования и дешифрования данных с использованием этих ключей.

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):

6-5 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 (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.