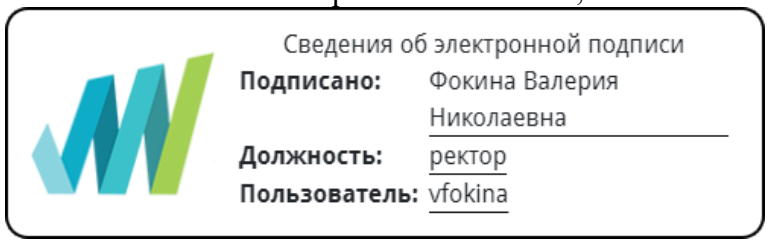
Автономная некоммерческая организация высшего образования
«Открытый университет экономики, управления и права»
(АНО ВО ОУЭП)

УТВЕРЖДАЮ:
Ректор АНО ВО ОУЭП, Фокина В.Н.



19 апреля 2023 г.

Решение Ученого совета АНО ВО ОУЭП,
Протокол N 9 от 19.04.2023 г.

09.03.01 «Информатика и вычислительная техника»

Направленность (профиль): Информатика и вычислительная техника

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ (МАТЕРИАЛОВ)
приложение 1

по компетенциям
Оценочные материалы для проверки сформированности компетенции
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Москва 2021

Оценочные материалы для проверки сформированности компетенции

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.1. Знает: общие характеристики технических средств, применяемых в информационных и автоматизированных системах, методы работы с информацией и общие требования к составлению библиографического описания документов, основные положения правовой базы в области защиты информационных систем и ресурсов организаций

ОПК-3.2. Умеет: использовать средства информационно-коммуникационных технологий в профессиональной деятельности с учетом основных требований к информационной безопасности

ОПК-3.3. Владеет: навыками работы с компьютерными технологиями в рамках профессиональной деятельности с учетом основных требований к информационной безопасности, навыками эффективного мониторинга обеспечения информационной безопасности в профессиональной деятельности

Компетенция формируется дисциплинами:

Защита информации	7 семестр
Основы автоматизированных информационных систем	5 семестр

Вопросы и задания для проверки сформированности компетенции

Дисциплина «Защита информации»

Разъясните основные понятия:

№	Понятие	Определение
1.	Методы и средства защиты информации	Методы и средства защиты информации – это организационно-технические и организационно-правовые мероприятия, проводимые в процессе создания и

		эксплуатации компьютерной системы для обеспечения защиты информации.
2.	Политика безопасности	Политика безопасности — это набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа.
3.	Угроза безопасности информации	Угроза безопасности информации в компьютерной системе – это событие или действие, которое может вызвать изменение функционирования компьютерной системы, связанное с нарушением защищенности обрабатываемой в ней информации.
4.	Утечка	Утечка – это неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками.
5.	Уязвимость информации	Уязвимость информации – это возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.
6.	Целостность информации	Целостность информации – неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения.
7.	Собственник информационных ресурсов, систем и технологий	Собственник информационных ресурсов, систем и технологий – это субъект с полномочиями владения, пользования и распоряжения указанными объектами.
8.	Разглашение	Разглашение – это доведение защищаемой информации до неконтролируемого количества получателей информации (например, публикация информации на открытом сайте в сети Интернет или в открытой печати).
9.	Непреднамеренное воздействие	Непреднамеренное воздействие на защищаемую информацию - воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств,

		природных явлений, иных нецеленаправленных воздействий (например, уничтожение документов в результате отказа накопителя на жестком магнитном диске компьютера).
10.	Конфиденциальность информации	Конфиденциальность информации – это известность ее содержания только имеющим соответствующие полномочия субъектам.
11.	Информационная безопасность	Область, которая занимается защитой информации и данных от несанкционированного доступа, использования, раскрытия, изменения или уничтожения. Она представляет собой комплекс мер и политик, направленных на обеспечение конфиденциальности, целостности и доступности информации.
12.	Мониторинг обеспечения информационной безопасности	Процесс постоянного контроля и наблюдения за системами, сетями или приложениями с целью обнаружения и предотвращения угроз безопасности, а также реагирования на инциденты информационной безопасности.

Вопросы открытого типа:

№	Вопрос	Ответ
1.	Что такое умышленная угроза информационной безопасности?	К умышленным угрозам относятся: − несанкционированные действия обслуживающего персонала КС (например, ослабление политики безопасности администратором, отвечающим за безопасность КС); − несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями.
2.	Что относится к непреднамеренным угрозам	К непреднамеренным угрозам относятся: − ошибки в проектировании КС;

	компьютерных систем?	– ошибки в разработке программных средств КС; – случайные сбои в работе аппаратных средств КС, линий связи, энергоснабжения; – ошибки пользователей КС; – воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др.
3.	Какие существуют непосредственные каналы утечки информации?	Непосредственными каналами утечки информации являются: – хищение носителей информации; – сбор производственных отходов с информацией (бумажных и магнитных носителей); – копирование носителей информации; – намеренное использование для несанкционированного доступа к информации незаблокированных терминалов других пользователей КС; – маскировка под других пользователей путем похищения их идентифицирующей информации (паролей, карт и т. п.); – обход средств разграничения доступа к информационным ресурсам вследствие недостатков в их программном обеспечении и др.
4.	Какие существуют косвенные каналы утечки информации?	Косвенными каналами утечки называют каналы, не связанные с физическим доступом к элементам КС: – использование подслушивающих (радио закладных) устройств; – дистанционное видеонаблюдение; – перехват побочных электромагнитных излучений и наводок (ПЭМИН).
5.	Что включают в себя организационные методы	Методы и средства организационной защиты информации включают в себя:

	защиты информации?	− ограничение физического доступа к объектам КС и реализация режимных мер; − ограничение возможности перехвата ПЭМИН (перехват побочных электромагнитных излучений и наводок); − разграничение доступа к информационным ресурсам и процессам КС (установка правил разграничения доступа, шифрование информации при ее хранении и передаче, обнаружение и уничтожение аппаратных и программных закладок); − резервное копирование наиболее важных с точки зрения утраты массивов документов; − профилактику заражения компьютерными вирусами.
6.	Какие существуют уровни правового обеспечения информационной безопасности?	Можно выделить четыре уровня правового обеспечения информационной безопасности. Первый уровень образуют международные договоры, к которым присоединилась Российская Федерация, и федеральные законы России. Второй уровень составляют подзаконные акты, к которым относятся указы Президента РФ и постановления Правительства РФ, а также письма Высшего Арбитражного Суда РФ и постановления пленумов Верховного Суда РФ. Третий уровень составляют государственные стандарты (ГОСТы) в области защиты информации, руководящие документы, нормы, методики и классификаторы, разработанные соответствующими государственными органами. Четвертый уровень образуют локальные нормативные акты, положения, инструкции, методические рекомендации и другие документы по комплексной защите информации в КС конкретной организации.

7.	Какая информация является конфиденциальной?	В соответствии с российским законодательством к конфиденциальной относится следующая информация: − служебная тайна (врачебная, адвокатская, тайна суда и следствия и т.п.); − коммерческая тайна; − персональные данные (сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность).
8.	Что является опосредованной угрозой безопасности информации в КС?	Опосредованной угрозой безопасности информации в КС является угроза раскрытия параметров подсистемы защиты информации, входящей в состав КС. Реализация этой угрозы дает возможность реализации перечисленных ранее непосредственных угроз безопасности информации.
9.	Что представляет собой системно-концептуальный подход решении задачи защиты информации в КС?	При решении задачи защиты информации в КС необходимо применять так называемый системно-концептуальный подход. В соответствии с ним решение задачи должно подразумевать: − системность целевую, при которой защищенность информации рассматривается как составная неотъемлемая часть ее качества; − системность пространственную, предполагающую взаимосвязанность защиты информации во всех элементах КС; − системность временную, предполагающую непрерывность защиты информации; − . системность организационную, предполагающую единство организации всех работ по защите информации в КС и управления ими.
10.	Какие существуют методы и средства защиты информации?	Существующие методы и средства защиты информации можно подразделить на четыре основные группы: − методы и средства организационно-правовой защиты информации; − методы и средства инженерно-технической защиты информации;

		− криптографические методы и средства защиты информации; − программно-аппаратные методы и средства защиты информации.

Тестовые задания:

1	Упорядоченная совокупность документов и массивов документов и информационных технологий, реализующих информационные процессы, называется: **a) информационной системой;** b) политикой безопасности; c) информационной технологией; d) информационным процессором.
2	Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, называется **Защитой информации**
3	Получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней, называется **Несанкционированным доступом**
4	Набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа, называется: a) защитой информации; **b) политикой безопасности;** c) стратегией защиты информации; d) правилами поведения.
5	Информация, содержание которой может быть понятно любому субъекту, называется: a) сказкой;

	b) инструкцией хакера; c) криптосистемой; **d) открытым текстом.**
6	Доведение защищаемой информации до неконтролируемого количества получателей информации (например, публикация информации на открытом сайте в сети Интернет или в открытой печати): a) компьютерным шпионажем; **b) разглашением;** c) вредительством; d) предательством.
7	Субъект с полномочиями владения информационными ресурсами, их пользования и распоряжения, называется a) сетевым администратором; **b) собственником информационных ресурсов;** c) программистом; d) пользователем.
8	Неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками: a) расползанием информации; b) информационным предательством; c) вредительством; **d) утечкой.**
9	Возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации, называется**:** a) устареванием политики безопасности; b) сбоем системы защиты информации; **c) уязвимостью информации;**

	d) обходом защиты информации.
10	Воздействие на защищаемую информацию из-за ошибок пользователя, сбоя технических или программных средств, природных явлений, иных нецеленаправленных воздействий, называется: **а) непреднамеренным воздействием;** b) самоатакой; c) глюком.

Ключ к тестовым заданиям

1	**2**	**3**	**4**	**5**
a	зашитой информации;	несанкционированным доступом;	b	d
6	**7**	**8**	**9**	**10**
b	b	d	c	a

Дисциплина «Основы автоматизированных информационных систем»

Разъясните основные понятия:

№	Понятие	Определение
1.	Информация	Представление данных, организованных и структурированных таким образом, чтобы они имели смысл и могли быть использованы в различных целях.
2.	База данных	Организованная коллекция связанных данных, которая обычно хранится в централизованном хранилище.
3.	Системный анализ	Процесс исследования и изучения существующих систем с целью определения их

		требований, проблем и возможностей.
4.	Моделирование	Процесс создания абстрактных моделей, которые представляют реальные системы или процессы.
5.	Компьютерная безопасность	Область знаний и практик, направленных на защиту компьютерных систем, данных и информации от несанкционированного доступа, повреждения или уничтожения..
6.	Жизненный цикл информационной системы	Последовательность этапов, через которые проходит информационная система от ее концепции и разработки до эксплуатации, обслуживания и выхода из эксплуатации.
7.	Бизнес-процессы	Совокупность связанных операций и действий, которые выполняются внутри организации для достижения конкретных целей и обеспечения выполнения бизнес-задач.
8.	Интеграция систем	Процесс объединения различных компонентов и подсистем информационной системы в единую функциональную систему.
9.	Информационная безопасность	Защита информации от различных угроз и рисков, чтобы обеспечить ее конфиденциальность, целостность и доступность.
10.	Сеть	Взаимодействующие компьютеры и устройства, объединенные с использованием коммуникационных технологий для обмена информацией и ресурсами. Сети могут включать локальные сети (LAN), глобальные сети (WAN), Интернет и другие формы подключения и коммуникации.

Вопросы открытого типа:

№	Вопрос	Ответ
1.	Что такое автоматизированная информационная система?	Комплекс программного и аппаратного обеспечения, предназначенного для сбора, хранения, обработки и передачи информации с использованием компьютерных технологий.
2.	Какие основные компоненты	1. Аппаратное обеспечение (компьютерное оборудование, серверы, сети),

	включает в себя автоматизированная информационная система?	2. Программное обеспечение (операционные системы, прикладные программы), 3. Базы данных. 4. Пользовательские интерфейсы. 5. Процессы обработки данных.
3.	Что такое информационная система?	Система, включающая в себя все компоненты, используемые для сбора, хранения, обработки, передачи и вывода информации.
4.	Какая роль моделирования в автоматизированных информационных системах?	Это процесс создания абстрактных моделей, которые представляют реальные компоненты и процессы в АИС. Моделирование позволяет анализировать, предсказывать и улучшать работу АИС, используя вычислительные и математические методы.
5.	Что такое компьютерная безопасность и почему она важна для автоматизированных информационных систем?	Это область знаний и практик, направленных на защиту компьютерных систем, данных и информации от несанкционированного доступа, повреждения или уничтожения. Компьютерная безопасность важна для обеспечения конфиденциальности, целостности и доступности информации в АИС и предотвращения возможных информационных угроз и инцидентов.
6.	Назначение математической модели –задачи Коши	Математическая модель задачи Коши служит основой для анализа и предсказания поведения системы на основе начального состояния. Она позволяет проводить структурный, статистический и численный анализ системы и имеет широкий спектр применений в различных областях науки и инженерии.
7.	Кратко определите понятие «моделирование на ЭВМ».	Моделирование на ЭВМ является процессом создания математической или физической модели с использованием программного обеспечения и аппаратных ресурсов компьютера.
8.	Перечислите основные возможности оценки результатов моделирования с	Оценка точности и достоверности результатов моделирования средствами OpenOffice.org Calc можно выполнить, используя различные функции и инструменты программы.

	помощью средств OpenOffice.org Calc.	1. Проверка формул. 2. Сравнение с экспериментальными данными. 3. Создание графиков. 4. Чувствительность к параметрам. 5. Статистический анализ. 6. Повторное моделирование.

Тестовые задания:

1.	Из перечисленных способов кодирования логических значений: 1) Л и И; 2) 0 и 1; 3) Т и Ф; 4) F и T – правильными являются
а)	**1, 2, 4**
б)	1, 2, 3
в)	2, 3, 4
г)	1, 3, 4

2.	Из следующих выражений: 1) $\neg$ 0 = 1; 2) 1 $\vee$ 0 = 1; 3) $\neg$ 1 = 1; 4) 0 $\wedge$ 1 = 1 правильными являются
а)	**1 и 2**
б)	2 и 3
в)	3 и 4
г)	1, 2, 3

3.	Из следующих выражений: 1) $\neg$ 0 = 0; 2) 1 $\vee$ 0 = 1; 3) $\neg$ 1 = 0; 4) 0 $\wedge$ 1 = 0 правильными являются
а)	**2, 3, 4**
б)	1, 2, 3

в)	2 и 3
г)	1 и 3

4.	Из перечисленного: 1) бинарный предикат; 2) предикат второго ранга; 3) двухместный предикат; 4) тернарный предикат – одинаковые значения имеют словосочетания
а)	**1, 2, 3**
б)	2, 3, 4
в)	1 и 4
г)	2 и 3

5.	Из перечисленных знаков: 1) $\in$; 2) &; 3) $\subseteq$ – в теории множеств используется
а)	**1 и 3**
б)	только 2
в)	2 и 3
г)	только 1

6.	Теория символьных конструкций является разделом теории _____
а)	**формальных языков**
б)	множеств
в)	кодирования
г)	булевых функций

7.	Даны алфавиты букв А = а 1 2 б в, В = а 2 1 г, тогда А $\cap$ В =
а)	**а 1 2**

б)	а 1 2 б в
в)	а 2 1 г
г)	а 1 г

8.	Даны алфавиты букв А = а 1 2 б в, В=а 2 1 г, тогда А ∪ В =
а)	**а 1 2 б в г**
б)	а 2 1 г б в
в)	а 2 1 г в б
г)	а 1 2 в б г

9.	Язык, уже нам известный, с помощью которого производится определение другого языка, называют
а)	**метаязыком**
б)	языком описания
в)	формальным языком
г)	конструктивным языком

10.	Определение: алгоритм – это предписание, ведущее от исходных данных к искомому результату и обладающее свойствами: определенности (общепонятности и точности, не оставляющей места для произвола); массовости; результативности – называют определением
а)	**по Маркову**
б)	неформальным
в)	по Мальцеву
г)	полуинтуитивным

11.	Сигнал в теории информации является
а)	**носителем информации**
б)	импульсом
в)	сообщением
г)	математической моделью

Ключ к тестовым заданиям

1	**2**	**3**	**4**	**5**
а	а	а	а	а
6	**7**	**8**	**9**	**10**
формальных языков	а	а	метаязыком	по Маркову
11	**12**	**13**	**14**	
Носителем информации				