федеральное государственное бюджетное образовательное учреждение
высшего образования
"Красноярский государственный медицинский университет
имени профессора В.Ф. Войно-Ясенецкого"
Министерства здравоохранения Российской Федерации

Кафедра управления и экономики здравоохранения ИПО

УТВЕРЖДАЮ
Проректор по учебной работе
д.м.н., доцент
И.А. Соловьева
«20» октября 2021 г.

Информационная безопасность

Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации по специальности
38.04.02 Менеджмент направленность (профиль) «Управление в здравоохранении на основе интеллектуального анализа данных» (очная форма обучения)

Красноярск
2021

Коды компетенций, проверяемых с помощью оценочных средств: ПК-2.2,УК-7.1,УК-7.2,УК-7.6,ОПК-12.2.

Вопросы

Критерии оценки для оценочного средства: Вопросы

Показатель оценки результатов обучения	Уровень сформированности компетенции	Шкала оценивания
Обучающийся показывает всесторонние и глубокие знания программного материала, знание основной и дополнительной литературы; последовательно и четко отвечает на вопросы и дополнительные вопросы; уверенно ориентируется в проблемных ситуациях; демонстрирует способность применять теоретические знания для анализа практических ситуаций, делать правильные выводы, проявляет творческие способности в понимании, изложении и использовании программного материала; подтверждает полное освоение компетенций, предусмотренных программой	Повышенный	5 - "отлично"
Обучающийся показывает полное знание программного материала, основной и дополнительной литературы; дает полные ответы на теоретические вопросы и дополнительные вопросы, допуская некоторые неточности; правильно применяет теоретические положения к оценке практических ситуаций; демонстрирует хороший уровень освоения материала и в целом подтверждает освоение компетенций, предусмотренных программой	Базовый	4 - "хорошо"
Обучающийся показывает знание основного материала в объеме, необходимом для предстоящей профессиональной деятельности; при ответе на вопросы и дополнительные вопросы не допускает грубых ошибок, но испытывает затруднения в последовательности их изложения; не в полной мере демонстрирует способность применять теоретические знания для анализа практических ситуаций, подтверждает освоение компетенций, предусмотренных программой на минимально допустимом уровне	Пороговый	3 - "удовлетворительно"
Обучающийся имеет существенные пробелы в знаниях основного учебного материала по дисциплине; не способен аргументированно и последовательно его излагать, допускает грубые ошибки в ответах, неправильно отвечает на дополнительные вопросы или затрудняется с ответом; не подтверждает освоение компетенций, предусмотренных программой - Оценка «2» (неудовлетворительно)	-/-	2 - "неудовлетворительно"

1. **Классификация компьютерных преступлений**

1) Несмотря на многообразие компьютерных преступлений, их можно классифицировать по отдельным общим группам. В начале 90-х гг. XX века рабочая группа в рамках Интерпола разработала специальный классификатор. В соответствии с ним все компьютерные преступления классифицированы следующим образом. 1. QA — несанкционированный доступ и перехват: QAH — компьютерный абордаж (несанкционированный доступ); QAI — перехват с помощью специальных технических средств; QAT — кража времени (уклонение от платы за пользование); QAZ — иные виды несанкционированного доступа и перехвата. 2. QD — изменение компьютерных данных: QDL — логическая бомба; GDT — троянский конь; QDV — компьютерный вирус; QDW — компьютерный червь; QDZ — прочие виды данных. 3. QF — компьютерное мошенничество: QFC — мошенничество с банкоматами; QFF — компьютерная подделка; QFG — мошенничество с игровыми автоматами; QFM — манипуляции с программами ввода-вывода; QFP — мошенничество с платежными средствами; QFT — телефонное мошенничество; QFZ — прочие

компьютерные мошенничества. В соответствии с УК РФ выделяют следующие преступления в сфере компьютерной информации: Неправомерный доступ к компьютерной информации; Создание, использование и распространение вредоносных компьютерных программ; Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

ПК-2.2 , УК-7.6 , УК-7.1 , УК-7.2 , ОПК-12.2

2. **Симметричные методы криптографии**

1) Криптография сегодня по праву считается одним из разделов математики, который занимается разработкой методов и алгоритмов шифрования данных. Преобразование текста из открытого сообщения в шифротекст называется зашифровыванием (шифрацией). Обратное преобразование шифротекста в исходное сообщение назовем расшифровыванием (дешифрацией). Зашифровывание и расшифровывание должно производиться по определенному методу, называемому алгоритмом зашифровывания. Любой конкретный алгоритм содержит некоторый набор параметров, позволяющих всякий раз использовать его для шифрации. Таким образом, для понятий метода и ключа шифрования введем следующие определения. Метод шифрования - это формальный алгоритм, описывающий порядок преобразования исходного сообщения в шифрованное. Ключ шифрования - это набор параметров (данных), необходимых для применения метода. Если при зашифровывании и расшифровывании применялся один и тот же ключ, то такой метод называется симметричным. Существует достаточно много методов симметричного шифрования. Как известно, Юлий Цезарь для связи со своими военачальниками использовал метод подстановки с ключом, равным 3. В исходном сообщении каждый символ заменялся другим символом, от-стоящим от него в алфавите на 3 позиции вправо.

ПК-2.2 , УК-7.1 , УК-7.2 , УК-7.6 , ОПК-12.2

3. **Персональные данные**

1) Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» определяет 6 категорий конфиденциальных сведений. Это: Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях. Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна). Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее). Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна). Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них. Иными словами, конфиденциальная информация – это информация с ограниченным доступом, не содержащая государственную тайну. Абсолютное большинство информационных ресурсов медицинских учреждений содержат те или иные сведения конфиденциального характера (служебная, коммерческая, врачебная тайна) и в соответствии с частью 4 ст. 9 Закона «Об информации,

информационных технологиях и о защите информации» доступ к ней должен быть ограничен. При этом наибольшее внимание современное законодательство уделяет защите персональных данных. Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных» устанавливает, что «персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)». Под обработкой персональных данных следует понимать «любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных». Важно, что под обработкой понимаются любые действия, как с использованием средств автоматизации (т.е. средств вычислительной техники), так и без этих средств. Иными словами, если персональные данные собираются, накапливаются и хранятся (т.е. обрабатываются) на бумажных носителях, в виде, например, традиционной бумажной медицинской документации, то на любые действия с этой документацией распространяется действие данного Федерального закона. Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств. Таким образом, если в медицинской информационной системе обрабатываются персональные данные (а именно это и происходит в абсолютном большинстве медицинских информационных систем), то эта система является информационной системой персональных данных. Первейшим условием обработки персональных данных является согласие субъекта персональных данных на обработку этих данных. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Согласие должно включать в себя, в частности: 1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе; 2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных); 3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных; 4) цель обработки персональных данных; 5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных; 6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу; 7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных; 8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом; 9) подпись субъекта персональных данных. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных только при наличии оснований, перечисленных в Законе.

ПК-2.2 , УК-7.1 , УК-7.2 , УК-7.6 , ОПК-12.2

4. **Межсетевые экраны**

1) Межсетевой экран (firewall) - это устройство контроля доступа в сеть, предназначенное для

блокировки всего трафика, за исключением разрешенных данных. Этим оно отличается от маршрутизатора, функцией которого является доставка трафика в пункт назначения в максимально короткие сроки. Межсетевые экраны, как правило, обладают большим набором настроек. Прохождение трафика на межсетевом экране можно настраивать по службам, IP-адресам отправителя и получателя, по идентификаторам пользователей, запрашивающих службу. Межсетевые экраны позволяют осуществлять централизованное управление безопасностью. В одной конфигурации администратор может настроить разрешенный входящий трафик для всех внутренних систем организации. Это не устраняет потребность в обновлении и настройке систем, но позволяет снизить вероятность неправильного конфигурирования одной или нескольких систем, в результате которого эти системы могут подвергнуться атакам на некорректно настроенную службу. Существуют два основных типа межсетевых экранов: межсетевые экраны прикладного уровня и межсетевые экраны с пакетной фильтрацией. В их основе лежат различные принципы работы, но при правильной настройке оба типа устройств обеспечивают правильное выполнение функций безопасности, заключающихся в блокировке запрещенного трафика.

5. **Что такое информационная война?**

6. **Что такое электронный ключ?**

7. **Что такое вирус?**

8. **Что такое криптография?**

9. **Что такое "защита информации"?**

10. **Что такое "модель управления доступом"?**

1. **Что такое «информационный шум»?**

ПК-2.2 , УК-7.6 , УК-7.1 , УК-7.2 , ОПК-12.2

2. **Каковы предпосылки начала информационной войны?**

ПК-2.2 , УК-7.1 , УК-7.2 , УК-7.6 , ОПК-12.2

3. **Что такое открытый ключ электронной подписи?**

1) Открытый ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и его сертификатом, подтверждающим принадлежность ключа проверки электронной подписи его владельцу.

ПК-2.2 , УК-7.1 , УК-7.2 , УК-7.6 , ОПК-12.2

4. **Каковы характерные черты информационной войны?**

5. **Какова деятельность Аллена Даллеса по отношению к России?**

6. **Что такое закрытый ключ электронной подписи?**

7. **Что такое сертификат открытого ключа электронной подписи?**

8. **Что такое неквалифицированная электронная подпись?**

9. **Что такое антивирус?**

10. **Перечислите способы защиты информации от вирусов?**

11. **Как распространяются вирусы?**

12. **Перечислите виды антивирусов?**

13. **Что такое шифротекст?**

14. **Что такое метод шифрования?**

15. **Что такое ключ шифрования?**

16. **В чем заключается суть процедуры зашифровывания?**

17. **Что такое конфиденциальность?**

18. **Что такое целостность?**

19. **Что такое доступность?**

20. **Какова цель защиты информации?**

21. **Что такое EFS?**

22. **Как работает EFS?**

23. **Что такое "прозрачное шифрование"?**

24. **Какой интерфейс используется для работы с EFS?**

25. **Какие протоколы защиты данных необходимо использовать для защиты передаваемых данных?**

26. **В чем заключается суть дискреционного управления доступом?**

27. **В чем заключается суть ролевого управления доступом?**

28. **В чем заключается суть мандатного управления доступом?**

29. **Что такое "метка критичности"?**

Практические навыки

Критерии оценки для оценочного средства: Практические навыки

Показатель оценки результатов обучения	Уровень сформированности компетенции	Шкала оценивания
Показатель рассчитывается в процентном соотношении верных ответов к общему числу выполненных параметров 100% -90%	Повышенный	5 - "отлично"
Показатель рассчитывается в процентном соотношении верных ответов к общему числу выполненных параметров 89% -80%	Базовый	4 - "хорошо"
Показатель рассчитывается в процентном соотношении верных ответов к общему числу выполненных параметров 79% -70%	Пороговый	3 - "удовлетворительно"
Показатель рассчитывается в процентном соотношении верных ответов к общему числу выполненных параметров - менее 70%	-/-	2 - "неудовлетворительно"

1. **Создать sfx-архив файла с помощью программы 7-zip**

1) Запустить программу «Пуск - Программы - «7-Zip»; указать путь к папке, где находится файл; выделить указателем мыши файл, подлежащий архивации и нажать кнопку Добавить; в открывшемся окне необходимо уточнить, если нужно, имя архивного файла и поставить галочку "Создать SFX-архив"; нажать кнопку "ОК".

ПК-2.2 , УК-7.2 , УК-7.6 , УК-7.1 , ОПК-12.2

2. **Создать электронную подпись заданного текстового фрагмента с помощью**

программы PGP

1) Выделить фрагмент текста; скопировать его в буфер обмена; щелкнуть правой кнопкой мыши на значке PGP на панели задач; выбрать пункт "ClipBoardSign"; выбрать владельца электронной подписи; вставить из буфера обмена сформированную электронную подпись после исходного текстового фрагмента.

ПК-2.2 , УК-7.1 , УК-7.2 , УК-7.6 , ОПК-12.2

3. **Определить IP-адрес компьютера**

1) Нажать сочетание клавиш "Win R"; в появившемся окне "Выполнить" написать "cmd"; нажать кнопку "ОК"; в появившейся командой строке написать "ipconfig /all".

ПК-2.2 , УК-7.1 , УК-7.2 , УК-7.6 , ОПК-12.2

№ п/п	Практические умения/Навыки	Компетенции
1	Применять правовые нормы и стандарты в области искусственного интеллекта при создании систем искусственного интеллекта.	УК-7.1
2	Применять этические нормы и стандарты в области искусственного интеллекта при создании систем искусственного интеллекта.	УК-7.1
3	Использовать нормативно-правовые документы в сфере информационных технологий, искусственного интеллекта и информационной безопасности при разработке стандартов, норм и правил.	УК-7.1
4	Нормативно-правовой базой, правовыми, этическими правилами, стандартами при решении задач искусственного интеллекта.	УК-7.1
5	Использовать международные и российские стандарты и методологии разработки автоматизированных систем программного обеспечения, стандартов в области информационной безопасности, принципы развития и использования технологий искусственного интеллекта при разработке стандартов, норм и правил в сфере искусственного интеллекта.	УК-7.2
6	Навыками разработки стандартов, правил в сфере искусственного интеллекта и смежных областях.	УК-7.2
7	Осуществлять лицензирование и защиту авторских прав при создании инновационных продуктов в области профессиональной деятельности.	УК-7.6
8	Методами лицензирования и защиты авторских прав при создании инновационных продуктов в области профессиональной деятельности.	УК-7.6
9	Модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач.	ОПК-12.2
10	Навыками модернизации программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач.	ОПК-12.2
11	Ставить задачи и участвовать в проведении тестовых и экспериментальных испытаний работоспособности систем, основанных на знаниях, анализировать результаты и вносить изменения.	ПК-2.2
12	Навыками проведении тестовых и экспериментальных испытаний работоспособности систем, основанных на знаниях, анализа результатов и внесения изменения.	ПК-2.2

Ситуационные задачи

Критерии оценки для оценочного средства: Ситуационные задачи

Показатель оценки результатов обучения	Уровень сформированности компетенции	Шкала оценивания
Полно раскрыто содержание материала; материал изложен грамотно, в определенной логической последовательности; продемонстрировано системное и глубокое знание программного материала; точно используется терминология; показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации; продемонстрировано усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость компетенций, умений и навыков; продемонстрирована способность творчески применять знание теории к решению профессиональных задач; продемонстрировано знание современной учебной и научной литературы	Повышенный	5 - "отлично"
Вопросы излагаются систематизированно и последовательно; продемонстрировано умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер; продемонстрировано усвоение основной литературы; в изложении допущены небольшие пробелы, не исказившие содержание; допущены один - два недочета при освещении основного содержания, исправленные по замечанию преподавателя	Базовый	4 - "хорошо"
Неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала; усвоены основные категории по рассматриваемому вопросу; имелись затруднения или допущены ошибки в определении понятий, использовании терминологии; при неполном знании теоретического материала выявлена недостаточная сформированность компетенций, умений и навыков, студент не может применить теорию в новой ситуации; продемонстрировано усвоение основной литературы	Пороговый	3 - "удовлетворительно"
Не раскрыто основное содержание учебного материала; обнаружено незнание или непонимание большей или наиболее важной части учебного материала; допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов; не сформированы компетенции, умения и навыки	-/-	2 - "неудовлетворительно"

1. **Ситуационная задача №1:** Вы - руководитель отдела информационной безопасности организации. Вы подозреваете, что один из пользователей корпоративной информационной системы создает и распространяет вредоносные программы внутри сети.

1) Какая статья уголовного кодекса была нарушена?

2) Какое наказание должен понести нарушитель?

Ответ 1: Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

Ответ 2: Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

УК-7.1 , УК-7.2

2. **Ситуационная задача №2:** Вы готовите доклад по методам и концепции информационных войн.

1) Перечислите способы поражения и разрушения сознания информационными войнами.

2) Какова концепция информационной войны?

Ответ 1: Можно выделить пять основных способов поражения и разрушения сознания: 1) Поражение нейромозгового субстрата, снижающее уровень функционирования сознания, может происходить на основе действия химических веществ, длительного отравления воздуха, пищи, направленных радиационных воздействий. 2) Понижение уровня организации информационно—коммуникативной среды на основе ее дезинтеграции и примитивизации, в которой функционирует и живет сознание. 3) Оккультное воздействие на организацию сознания на основе направленной передачи мыслеформ субъекту поражения. 4) Специальная организация и распространение по каналам коммуникации образов и текстов, которые разрушают работу сознания (условно может быть обозначено как психотропное оружие). 5) Разрушение способов и форм идентификации личности по отношению к фиксированным общностям, приводящее к смене форм самоопределения и к деперсонализации.

Ответ 2: Концепция информационной войны: 1) подавление элементов инфраструктуры государственного, военного управления; 2) радиоэлектронная борьба (электронно-магнитное воздействие); 3) радиоэлектронная разведка; 4) хакерная война; 5) формирование и массовое распространение по информационным каналам противника или глобальным сетям дезинформации.

УК-7.2 , УК-7.6

3. **Ситуационная задача №3:** Вы владеете сертификатом ключа подписи.

1) Каковы обязательства владельца сертификата ключа подписи?

2) Как происходит приостановление действия сертификата ключа подписи?

Ответ 1: Владелец сертификата ключа подписи обязан: не использовать для электронной цифровой подписи открытые и закрытые ключи электронной цифровой подписи, если ему известно, что эти ключи используются или использовались ранее; хранить в тайне закрытый ключ электронной цифровой подписи; немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа электронной цифровой подписи нарушена.

Ответ 2: 1. Действие сертификата ключа подписи может быть приостановлено удостоверяющим центром на основании указания лиц или органов, имеющих такое право в силу закона или договора, а в корпоративной информационной системе также в силу установленных для нее правил пользования. 2. Период от поступления в удостоверяющий центр указания о приостановлении действия сертификата ключа подписи до внесения соответствующей информации в реестр сертификатов ключей подписей должен устанавливаться в соответствии с общим для всех владельцев сертификатов ключей подписей правилом. По договоренности между удостоверяющим центром и владельцем сертификата ключа подписи этот период может быть сокращен. 3. Действие сертификата ключа подписи по указанию полномочного лица (органа) приостанавливается на исчисляемый в днях срок, если иное не установлено нормативными правовыми актами или договором. Удостоверяющий центр возобновляет действие сертификата ключа подписи по указанию полномочного лица (органа). В случае, если по истечении указанного срока не поступает указание о возобновлении действия сертификата ключа подписи, он подлежит аннулированию. 4. В соответствии с указанием полномочного лица (органа) о приостановлении действия сертификата ключа подписи удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты, времени и срока

приостановления действия сертификата ключа подписи, а также извещает об этом владельца сертификата ключа подписи и полномочное лицо (орган), от которого получено указание о приостановлении действия сертификата ключа подписи.

УК-7.1 , УК-7.2

4. **Ситуационная задача №4:** И.И. Иванов, сотрудник одной из поликлиник, внедрил в компьютерную медицинскую систему вирус, уничтоживший исполняемые файлы (файлы с расширением .exe). В результате внедрения этого вируса было уничтожено 60% информации.

1) Как можно квалифицировать действия И.И. Иванова?

2) Полагается ли за такие действия наказание?

Ответ 1: Действия И.И. Иванова квалифицируются как противоправные на основании ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», п. 3 УК РФ, т. к. налицо распространение вредоносных программ для ЭВМ, которое привело к тяжким последствиям.

Ответ 2: Такие деяния наказываются лишением свободы на срок до семи лет.

Тесты

Критерии оценки для оценочного средства: Тесты

Показатель оценки результатов обучения	Уровень сформированности компетенции	Шкала оценивания
Показатель рассчитывается в процентном соотношении верных ответов к общему числу тестовых заданий 100% -90%	Повышенный	5 - "отлично"
Показатель рассчитывается в процентном соотношении верных ответов к общему числу тестовых заданий 89% -80%	Базовый	4 - "хорошо"
Показатель рассчитывается в процентном соотношении верных ответов к общему числу тестовых заданий 79% -70%	Пороговый	3 - "удовлетворительно"
Показатель рассчитывается в процентном соотношении верных ответов к общему числу тестовых заданий - менее 70%	-/-	2 - "неудовлетворительно"

1. **ИНФОРМАЦИЯ В ЭЛЕКТРОННОЙ ФОРМЕ, КОТОРАЯ ПРИСОЕДИНЕНА К ДРУГОЙ ИНФОРМАЦИИ В ЭЛЕКТРОННОЙ ФОРМЕ (ПОДПИСЫВАЕМОЙ ИНФОРМАЦИИ) И КОТОРАЯ ИСПОЛЬЗУЕТСЯ ДЛЯ ОПРЕДЕЛЕНИЯ ЛИЦА, ПОДПИСЫВАЮЩЕГО ИНФОРМАЦИЮ - ЭТО**

1) электронная подпись

2) ключ электронной подписи

3) открытый ключ проверки электронной подписи

4) сертификат открытого ключа электронной подписи

5) закрытый ключ электронной подписи

Правильный ответ: 1

ОПК-12.2

2. **НАИБОЛЕЕ РИСКОВАННОЙ ДЛЯ МЕДИЦИНСКОГО УЧРЕЖДЕНИЯ С ТОЧКИ ЗРЕНИЯ ВЕРОЯТНОГО МОШЕННИЧЕСТВА И НАРУШЕНИЯ БЕЗОПАСНОСТИ ЯВЛЯЕТСЯ КАТЕГОРИЯ**

1) сотрудники

2) хакеры

3) атакующие

4) контрагенты (лица, работающие по договору)

5) руководство компании

Правильный ответ: 1

ОПК-12.2

3. **НЕКАЯ УНИКАЛЬНАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ СИМВОЛОВ, ЗАПИСАННАЯ НА ЭЛЕКТРОННЫЙ НОСИТЕЛЬ (ФЛЭШ-КАРТУ ИЛИ СМАРТ-КАРТУ) - ЭТО**

1) ключ электронной подписи

2) электронная подпись

3) сертификат открытого ключа электронной подписи

4) открытый ключ проверки электронной подписи

5) закрытый ключ электронной подписи

Правильный ответ: 1

ОПК-12.2

4. **ПРИ КЛАССИФИКАЦИИ ДАННЫХ РУКОВОДСТВО ДОЛЖНО**

1) продумать типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

2) продумать необходимый уровень доступности, целостности и конфиденциальности

3) оценить уровень риска и отменить контрмеры

4) продумать управление доступом, которое должно защищать данные

5) снизить уровень классификации информации, чтобы она была всем доступна

Правильный ответ: 2

ОПК-12.2

5. **В КОНЕЧНОМ СЧЕТЕ НЕСЕТ ОТВЕТСТВЕННОСТЬ ЗА ГАРАНТИИ ТОГО, ЧТО ДАННЫЕ КЛАССИФИЦИРОВАНЫ И ЗАЩИЩЕНЫ**

1) владелец данных

2) пользователь

3) администратор

4) руководство

5) сотрудник

Правильный ответ: 4

ОПК-12.2

6. **СОТРУДНИК УЧРЕЖДЕНИЯ МОЖЕТ БЫТЬ ПРИВЛЕЧЕН К ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЛУЧАЕ**

1) выхода в интернет без разрешения администратора

2) при установке компьютерных игр

3) установки нелицензионного ПО

4) не выхода из информационной системы

5) в любом случае неправомочного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности

Правильный ответ: 5

ОПК-12.2

7. **ИНФОРМАЦИОННАЯ ВОЙНА - ЭТО**

1) атака против информационной функции, зависимая от применяемых средств

2) атака против информационной функции, независимо от применяемых средств

3) любая атака против информационной функции

4) любая атака против информационной функции, независимо от применяемых средств

5) любая атака против информационной функции, зависимая от применяемых средств

Правильный ответ: 4

ОПК-12.2

8. **БОМБАРДИРОВКА АТС - ЭТО**

1) средство информационной войны

2) метод информационной войны

3) операция информационной войны

4) оружие информационной войны

5) информационная война

Правильный ответ: 1

ОПК-12.2

9. **АНТИВИРУС, КОТОРЫЙ ЗАПОМИНАЕТ ИСХОДНОЕ СОСТОЯНИЕ ПРОГРАММ, КАТАЛОГОВ И СИСТЕМНЫХ ОБЛАСТЕЙ ДИСКА КОГДА КОМПЬЮТЕР НЕ ЗАРАЖЕН ВИРУСОМ, А ЗАТЕМ ПЕРИОДИЧЕСКИ ИЛИ ПО КОМАНДЕ ПОЛЬЗОВАТЕЛЯ СРАВНИВАЕТ ТЕКУЩЕЕ СОСТОЯНИЕ С ИСХОДНЫМ, НАЗЫВАЕТСЯ**

1) детектор

2) доктор

3) сканер

4) ревизор

5) сторож

Правильный ответ: 4

ОПК-12.2

10. **ФУНКЦИИ СОЗДАНИЯ И ВЫДАЧИ СЕРТИФИКАТОВ ВОЗЛОЖЕНЫ НА ЮРИДИЧЕСКОЕ ЛИЦО (ИЛИ НА ИНДИВИДУАЛЬНОГО ПРЕДПРИНИМАТЕЛЯ), КРОМЕ ТОГО ВЕДУЩЕЕ РЕЕСТР ВЫДАННЫХ И АННУЛИРОВАННЫХ СЕРТИФИКАТОВ, А ИМЕННО**

1) удостоверяющий центр

2) многофункциональный центр

3) министерство внутренних дел

4) центр выдачи сертификатов

5) паспортную службу

Правильный ответ: 1

11. **ВЫВОД ИЗ СТРОЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРА АТС - ЭТО**

1) средство информационной войны

2) операция информационной войны

3) метод информационной войны

4) оружие информационной войны

5) информационная война

Правильный ответ: 2

12. **ЯВНЫЕ И СКРЫТЫЕ ЦЕЛЕНАПРАВЛЕННЫЕ ИНФОРМАЦИОННЫЕ ВОЗДЕЙСТВИЯ СИСТЕМ ДРУГ НА ДРУГА С ЦЕЛЬЮ ПОЛУЧЕНИЯ ОПРЕДЕЛЕННОГО ВЫИГРЫША В МАТЕРИАЛЬНОЙ СФЕРЕ - ЭТО**

1) информационная война

2) методы информационной войны

3) оружие информационной войны

4) средства информационной войны

5) часть информационной войны

Правильный ответ: 1

13. **АНТИВИРУС, КОТОРЫЙ ОБЕСПЕЧИВАЕТ ПОИСК ВИРУСОВ В ОПЕРАТИВНОЙ ПАМЯТИ, НА ВНЕШНИХ НОСИТЕЛЯХ ПУТЕМ ПОДСЧЕТА И СРАВНЕНИЯ С ЭТАЛОНОМ КОНТРОЛЬНОЙ СУММЫ, НАЗЫВАЕТСЯ**

1) детектор

2) доктор

3) сканер

4) ревизор

5) сторож

Правильный ответ: 1

14. **АНТИВИРУС, КОТОРЫЙ НЕ ТОЛЬКО НАХОДИТ ЗАРАЖЕННЫЕ ВИРУСАМИ ФАЙЛЫ, НО И "ЛЕЧИТ" ИХ, Т.Е. УДАЛЯЕТ ИЗ ФАЙЛА ТЕЛО ПРОГРАММЫ ВИРУСА, ВОЗВРАЩАЯ ФАЙЛЫ В ИСХОДНОЕ СОСТОЯНИЕ, НАЗЫВАЕТСЯ**

1) детектор

2) доктор

3) сканер

4) ревизор

5) сторож

Правильный ответ: 2

15. **АНТИВИРУС, КОТОРЫЙ ПРЕДСТАВЛЯЕТ СОБОЙ НЕБОЛЬШУЮ РЕЗИДЕНТНУЮ ПРОГРАММУ, ПРЕДНАЗНАЧЕННУЮ ДЛЯ ОБНАРУЖЕНИЯ ПОДОЗРИТЕЛЬНЫХ ДЕЙСТВИЙ ПРИ РАБОТЕ КОМПЬЮТЕРА, ХАРАКТЕРНЫХ ДЛЯ ВИРУСОВ, НАЗЫВАЕТСЯ**

1) детектор

2) доктор

3) сканер

4) ревизор

5) сторож

Правильный ответ: 5

16. **АКТИВНЫЙ ПЕРЕХВАТ ИНФОРМАЦИИ - ЭТО ПЕРЕХВАТ, КОТОРЫЙ**

1) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации

2) основан на фиксации электромагнитных излучений, возникающих при функционировании

средств компьютерной техники и коммуникаций

3) неправомерно использует технологические отходы информационного процесса

4) осуществляется путем использования оптической техники

5) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера

Правильный ответ: 5

17. **ОТВЕТСТВЕННЫМ ЗА ОПРЕДЕЛЕНИЕ УРОВНЯ КЛАССИФИКАЦИИ ИНФОРМАЦИИ ЯВЛЯЕТСЯ**

1) руководитель среднего звена

2) высшее руководство

3) владелец

4) пользователь

5) начальник

Правильный ответ: 3

18. **ЕСЛИ РАЗЛИЧНЫМ ГРУППАМ ПОЛЬЗОВАТЕЛЕЙ С РАЗЛИЧНЫМ УРОВНЕМ ДОСТУПА ТРЕБУЕТСЯ ДОСТУП К ОДНОЙ И ТОЙ ЖЕ ИНФОРМАЦИИ, ТО РУКОВОДСТВУ СЛЕДУЕТ**

1) снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования

2) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

3) улучшить контроль за безопасностью этой информации

4) снизить уровень классификации этой информации

5) разрешить к ней свободный доступ

Правильный ответ: 3

19. **ПЕРСОНАЛЬНЫЕ ДАННЫЕ - ЭТО**

1) любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу

2) фамилия, имя, отчество физического лица

3) год, месяц, дата и место рождения, адрес физического лица

4) адрес проживания физического лица

5) сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»

Правильный ответ: 1

20. **ОСНОВНОЕ СРЕДСТВО, ОБЕСПЕЧИВАЮЩЕЕ КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ, ПОСЫЛАЕМОЙ ПО ОТКРЫТЫМ КАНАЛАМ ПЕРЕДАЧИ ДАННЫХ, В ТОМ ЧИСЛЕ ПО СЕТИ ИНТЕРНЕТ, НОСИТ НАЗВАНИЕ**

1) шифрование

2) аутентификация

3) авторизация

4) идентификация

5) дискретизация

Правильный ответ: 1

21. **СИМВОЛЫ ШИФРУЕМОГО ТЕКСТА ПЕРЕМЕЩАЮТСЯ ПО ОПРЕДЕЛЕННЫМ ПРАВИЛАМ ВНУТРИ ШИФРУЕМОГО БЛОКА ЭТОГО ТЕКСТА, ЭТО МЕТОД**

1) гаммирования

2) подстановки

3) кодирования

4) перестановки

5) аналитических преобразований

Правильный ответ: 4

22. **СИМВОЛЫ ШИФРУЕМОГО ТЕКСТА ЗАМЕНЯЮТСЯ ДРУГИМИ СИМВОЛАМИ, ВЗЯТЫМИ ИЗ ОДНОГО ИЛИ НЕСКОЛЬКИХ АЛФАВИТОВ, ЭТО МЕТОД**

1) гаммирования

2) подстановки

3) кодирования

4) перестановки

5) аналитических преобразований

Правильный ответ: 2

23. **СИМВОЛЫ ШИФРУЕМОГО ТЕКСТА ПОСЛЕДОВАТЕЛЬНО СКЛАДЫВАЮТСЯ С СИМВОЛАМИ НЕКОТОРОЙ СПЕЦИАЛЬНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ, ЭТО МЕТОД**

1) гаммирования

2) подстановки

3) кодирования

4) перестановки

5) аналитических преобразований

Правильный ответ: 1

24. **ЗАЩИТА ИНФОРМАЦИИ - ЭТО**

1) процесс сбора, накопления, обработки, хранения, распределения и поиска информации

2) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа

3) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств

4) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям

5) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё

Правильный ответ: 5

25. **УНИКАЛЬНАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ СИМВОЛОВ, ОДНОЗНАЧНО СВЯЗАННАЯ С КЛЮЧОМ ЭЛЕКТРОННОЙ ПОДПИСИ И ЕГО СЕРТИФИКАТОМ - ЭТО**

1) открытый ключ проверки электронной подписи

2) ключ электронной подписи

3) электронная подпись

4) сертификат открытого ключа электронной подписи

5) закрытый ключ электронной подписи

Правильный ответ: 1

26. **ДЛЯ ПОДПИСАНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТА С ПОМОЩЬЮ ЭЛЕКТРОННОЙ ПОДПИСИ НЕОБХОДИМО ИМЕТЬ**

1) закрытый ключ электронной подписи, открытый ключ электронной подписи, сертификат открытого ключа электронной подписи

2) ключ электронной подписи

3) электронную подпись

4) открытый ключ проверки электронной подписи

5) закрытый ключ электронной подписи

Правильный ответ: 1

Рефераты

Критерии оценки для оценочного средства: Рефераты

Показатель оценки результатов обучения	Уровень сформированности компетенции	Шкала оценивания

Выполнены все требования к написанию и защите реферата. Содержание реферата соответствует заявленной в названии тематике, реферат имеет чёткую композицию и структуру, в тексте отсутствуют логические нарушения в представлении материала, обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция. Сформулированы выводы, тема раскрыта полностью, выдержан объём. Реферат представляет собой самостоятельное исследование, представлен качественный анализ найденного материала, отсутствуют факты плагиата. Корректно оформлены и в полном объёме представлены список использованной литературы и ссылки на использованную литературу в тексте реферата. Отсутствуют орфографические, пунктуационные, грамматические, лексические, стилистические и иные ошибки в авторском тексте. Соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы. Обучающийся подтверждает полное освоение компетенций, предусмотренных программой.	Повышенный	5 - "отлично"
Основные требования к реферату и его защите выполнены, но при этом допущены недочёты. Имеются неточности в изложении материала, отсутствует логическая последовательность в суждениях, не выдержан объём реферата. Содержание реферата соответствует заявленной в названии тематике, реферат оформлен в соответствии с общими требованиями написания реферата, но есть погрешности в техническом оформлении. Реферат представляет собой самостоятельное исследование, представлен качественный анализ найденного материала, отсутствуют факты плагиата. В полном объёме представлены список использованной литературы, но есть ошибки в оформлении, корректно оформлены и в полном объёме представлены ссылки на использованную литературу в тексте реферата. Отсутствуют орфографические, пунктуационные, грамматические, лексические, стилистические и иные ошибки в авторском тексте. На дополнительные вопросы при защите даны неполные ответы. В целом обучающийся подтверждает освоение компетенций, предусмотренных программой.	Базовый	4 - "хорошо"
Имеются существенные отступления от требований к реферированию. Тема освещена лишь частично, допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы. во время защиты отсутствует вывод. Есть погрешности в техническом оформлении. Не в полном объёме представлен список использованной литературы, есть ошибки в оформлении, некорректно оформлены или не в полном объёме представлены ссылки на использованную литературу в тексте реферата. Есть единичные орфографические, пунктуационные, грамматические, лексические, стилистические и иные ошибки в авторском тексте, отсутствуют факты плагиата. Обучающийся подтверждает освоение компетенций, предусмотренных программой, на минимально допустимом уровне.	Пороговый	3 - "удовлетворительно"
Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы, в тексте реферата есть логические нарушения в представлении материала. Есть погрешности в техническом оформлении. Допущены грубые ошибки в ответах. Не в полном объёме представлен список использованной литературы, есть ошибки в оформлении, некорректно оформлены или не в полном объёме представлены ссылки на использованную литературу в тексте реферата. Есть частые орфографические, пунктуационные, грамматические, лексические, стилистические и иные ошибки в авторском тексте, присутствуют факты плагиата. Обучающийся не подтверждает освоение компетенций, предусмотренных программой.	-/-	2 - "неудовлетворительно"

№ п/п	Темы рефератов	Компетенции
1	Искусственный интеллект в информационной безопасности.	ПК-2.2, УК-7.1, УК-7.2, УК-7.6, ОПК-12.2
2	Искусственный интеллект: возможности и угрозы.	ПК-2.2, УК-7.1, УК-7.2, УК-7.6, ОПК-12.2
3	Как технологии искусственного интеллекта могут противостоять кибератакам?	ПК-2.2, УК-7.1, УК-7.2, УК-7.6, ОПК-12.2
4	Искусственный интеллект и анализ данных.	ПК-2.2, УК-7.1, УК-7.2, УК-7.6, ОПК-12.2
5	Искусственный интеллект - прорывная технология в информационной безопасности.	ПК-2.2, УК-7.1, УК-7.2, УК-7.6, ОПК-12.2
6	Почему искусственный интеллект все чаще принимают на кибервооружение?	ПК-2.2, УК-7.1, УК-7.2, УК-7.6, ОПК-12.2
7	Нужна ли защита для искусственного интеллекта?	ПК-2.2, УК-7.1, УК-7.2, УК-7.6, ОПК-12.2
8	Робот-хакер.	ПК-2.2, УК-7.1, УК-7.2, УК-7.6, ОПК-12.2
9	Стоит ли бояться искусственного интеллекта?	ПК-2.2, УК-7.1, УК-7.2, УК-7.6, ОПК-12.2
10	Медицина и искусственный интеллект: возможно ли это?	ПК-2.2, УК-7.1, УК-7.2, УК-7.6, ОПК-12.2