Приложение 6

к основной профессиональной образовательной программе

по направлению подготовки 09.03.03 «Прикладная информатика»

направленность (профиль) программы «Прикладная информатика в экономике*»*

**Министерство науки и высшего образования Российской Федерации**

**федеральное государственное бюджетное образовательное учреждение**

**высшего образования**

**«Российский экономический университет имени Г.В. Плеханова»**

**Краснодарский филиал РЭУ им. Г. В. Плеханова**

Факультет экономики, менеджмента и торговли

Кафедра бухгалтерского учета и анализа

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ**

**по дисциплине Информационная безопасность**

**Направление подготовки 09.03.03 Прикладная информатика**

**Направленность (профиль) программы Прикладная информатика в экономике**

**Уровень высшего образования Бакалавриат**

**Год начала подготовки 2022**

**Краснодар – 2021 г.**

Составитель: к.п.н., доцент кафедры бухгалтерского учета и анализа В.В. Салий

Оценочные материалы одобрены на заседании кафедры бухгалтерского учета и анализа Краснодарского филиала РЭУ им. Г.В. Плеханова протокол № 1 от 30 августа 2021 г.

Оценочные материалы составлены на основе рабочей программы по дисциплине «Информационная безопасность», утвержденной на заседании базовой кафедры Прикладной информатики и информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Российский экономический университета имени Г.В. Плеханова» протокол № 10 от 28 апреля 2021 г., разработанной авторами:

Козыревым П.А., ассистент, базовой кафедры Прикладной информатики и информационной безопасности

Креопаловым В.В., к.т.н, доцент кафедры прикладной информатики и информационной безопасности

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ**

**по дисциплинеИнформационная безопасность**

**ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ С УКАЗАНИЕМ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ И ЭТАПОВ ИХ ФОРМИРОВАНИЯ ПО ДИСЦИПЛИНЕ**

|  |  |  |  |
| --- | --- | --- | --- |
| **Формируемые компетенции** **(*код и наименование компетенции*)**  | **Индикаторы достижения компетенций****(*код и наименование индикатора*)** | **Результаты обучения** ***(знания, умения)*** | **Наименование контролируемых разделов и тем** |
| УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений | УК-2.1. Понимает базовые принципы постановки задач и выработки решений | УК-2.1. З-1. Знает основные принципы и концепции в области целеполагания и принятия решенийУК-2.1. З-2. Знает методы генерирования альтернатив решений и приведения их к сопоставимому виду для выбора оптимального решения УК-2.1. З-3. Знает природу данных, необходимых для решения поставленных задач | **Тема 1.** Стандарты и нормативно-правовые акты в области информационной безопасности.**Тема 2.** Анализ рисков и угроз информационной безопасности.**Тема 3.** Проектирование, разработка и внедрение автоматизированных систем в защищенном исполнении. |
| УК-2.1. У-1. Умеет системно анализировать поставленные цели, формулировать задачи и предлагать обоснованные решенияУК-2.1. У-2. Умеет критически оценивать информацию о предметной области принятия решенийУК-2.1. У-3. Умеет использовать инструментальные средства для разработки и принятия решений |
| УК-2.2. Выбирает оптимальные способы решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений | УК-2.2. З-1. Знает основные методы принятия решений, в том числе в условиях риска и неопределенностиУК-2.2. З-2. Знает виды и источники возникновения рисков принятия решений, методы управления имиУК-2.2. З-3. Знает основные нормативно-правовые документы, регламентирующие процесс принятия решений в конкретной предметной области | **Тема 1.** Стандарты и нормативно-правовые акты в области информационной безопасности.**Тема 2.** Анализ рисков и угроз информационной безопасности.**Тема 3.** Проектирование, разработка и внедрение автоматизированных систем в защищенном исполнении. |
| УК-2.2. У-1. Умеет проводить многофакторный анализ элементов предметной области для выявления ограничений при принятии решенийУК-2.2. У-2. Умеет разрабатывать и оценивать альтернативные решения с учетом рисковУК-2.2. У-3. Умеет выбирать оптимальные решения исходя из действующих правовых норм, имеющихся ресурсов и ограничений |
| 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-3.2. Решает задачи профессиональной деятельности с учетом основных требований информационной безопасности | ОПК-3.2. З-1. Знает методологические и технологические основы комплексного обеспечения безопасности автоматизированных информационных системОПК-3.2. З-2. Знает методы и средства, современные подходы к построению систем защиты информации, критерии оценки защищенности ИС, принципы формирования политики информационной безопасности в автоматизированных системахОПК-3.2. З-3. Знает нормативно-правовые документы по обеспечению информационной безопасности, стандарты построения систем информационной безопасности и оценки степени защиты систем информационной безопасности объектов ОПК-3.2. З-4. Знает основные методы контроля эффективности обеспечения информационной безопасности информационных систем | **Тема 1.** Стандарты и нормативно-правовые акты в области информационной безопасности.**Тема 2.** Анализ рисков и угроз информационной безопасности.**Тема 3.** Проектирование, разработка и внедрение автоматизированных систем в защищенном исполнении. |
| ОПК-3.2. У-1. Умеет разрабатывать модели угроз и нарушителей информационной безопасности ИС, выявлять угрозы информационной безопасности и обосновывать организационно-технические мероприятия по защите информации в ИСОПК-3.2. У-2. Умеет выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и проводить мониторинг угроз безопасности ИСОПК-3.2. У-3. Умеет анализировать риски информационных систем, осуществлять оценку защищенности и обеспечения информационной безопасности информационных системОПК-3.2. У-4. Умеет выполнять работы на стадиях и этапах создания ИС в защищенном исполненииОПК-3.2. У-5. Умеет составлять аналитические обзоры по вопросам обеспечения информационной безопасности ИС и разрабатывать частные политики информационной безопасности ИС |

**КОМПЛЕКТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ**

**Компетенция – УК-2**

 **Индикатор компетенции УК-2.1, УК-2.2**

**Тестовые задания закрытого типа**

1. Какой из ниже перечисленных методов является наиболее безопасным для создания пароля?
а. Использование простого слова или фразы

б. Использование комбинации заглавных и строчных букв, цифр и специальных символов
в. Использование повторяющихся символов или последовательностей

г. Использование одного и того же пароля для разных аккаунтов

верный ответ: б

2. Что такое двухфакторная аутентификация?
а. Процесс проверки подлинности пользователя, который осуществляется на основе двух разных факторов: что-то, что знает пользователь и что-то, что имеет пользователь

б. Хакерская атака, при которой злоумышленник получает доступ к аккаунту пользователя

в. Метод шифрования данных для обеспечения их безопасности

г. Программа, используемая для защиты компьютера от вредоносных программ

верный ответ: а

3. Средствами воздействия на сеть офиса нельзя считать:

а. Слабый трафик, информационный обман, вирусы в интернет

б. Вирусы в сети, логические мины (закладки), информационный перехват

г. Компьютерные сбои, изменение админстрирования, топологии

*(укажите не менее двух правильных ответов)*

верный ответ: а, г

4. Какая категория является наименее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

а. Сотрудники

б. Хакеры

в. Покупатели

г. Поставщики

*(укажите не менее двух правильных ответов)*

верный ответ: б, в, г

5. По какой формуле нельзя рассчитать остаточный риск?

а. Угрозы х Риски х Ценность актива

б. (Угрозы х Ценность актива х Уязвимости) х Риски

в. SLE x Частоту = ALE

г. (Угрозы х Уязвимости х Ценность актива) x Недостаток контроля

*(укажите не менее двух правильных ответов)*

верный ответ: а, б, в

6. Что такое DDoS-атака?

а. Атака, при которой злоумышленник получает доступ к аккаунту пользователя и контролирует его

б. Атака, при которой злоумышленник блокирует доступ к определенному веб-сайту или онлайн-сервису, перегрузив его трафиком

в. Программа-вымогатель, которая блокирует доступ к файлам на компьютере пользователя и требует выкуп за их разблокировку.

г. Метод шифрования данных для защиты их конфиденциальности

верный ответ: б

7. Что такое шифрование данных?

а. Процесс преобразования данных в зашифрованный формат для обеспечения их конфиденциальности и безопасности

б. Метод защиты компьютера от вредоносного программного обеспечения

в. Техника, используемая злоумышленниками для получения доступа к компьютеру или сети

г. Атака, при которой злоумышленник получает доступ к аккаунту пользователя и контролирует его

верный ответ: а

8. Основными рисками информационной безопасности являются:

а. Искажение, уменьшение объема, перекодировка информации

б. Техническое вмешательство, выведение из строя оборудования сети

в. Потеря, искажение, утечка информации

верный ответ: в

9. Из каких четырех доменов состоит CobiT?

а. Планирование и организация

б. Приобретение и внедрение

в. Поддержка и внедрение

г. Эксплуатация и сопровождение

д. Мониторинг и оценка

*(укажите не менее двух правильных ответов)*

верный ответ: а, б, г, д

10. Процесс управления ключами включает в себя реализацию трех основных функций:

а. Генерацию ключей

б. Использование ключей

в. Хранение ключей

г. Распределение ключей

*(укажите не менее двух правильных ответов)*

верный ответ: а, в, г

**Вопросы открытого типа**

11. Интернетизированная сеть, в которой соединения между информационными ресурсами устанавливаются только между доверенными (и многократно проверенными) IP адресами, с использованием специфицированных протоколов и портов называется … Web.

*(Ответ записать словом с большой буквы в именительном падеже на английском языке)*

верный ответ: Deep

12. …. – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных.

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: кибербезопасность

13. … – это незаконное проникновение или угроза вредоносного проникновения в виртуальное пространство для достижения политических, социальных или иных, целей.

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: киберугроза

14. Посылка обманных сообщений с целью обмануть пользователей и получить их личные данные носит название ….

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: фишинг

15. Устройство или программное обеспечение, которое фильтрует и контролирует сетевой трафик, позволяя разрешить или блокировать доступ в зависимости от заданных правил – это ….

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: файрвол

16. Форма мошенничества, при которой злоумышленник получает доступ к финансовым данным пользователя, используя специальное устройство для чтения информации с магнитных полос карты носит название …

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: скимминг

17. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы носит название …

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: детектор

18. Антивирус 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 носит название …

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: ревизор

19. Программа, осуществляющая несанкционированные действия по сбору, и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию носит название …

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: троян

20. Процесс преобразования информации, хранящейся в файле к виду, при котором уменьшается избыточность в ее представлении и соответственно требуется меньший объем памяти для ее хранения называется … файла

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: архивация

21. Устройство хранения криптографических ключей, аппаратный ключ носит название ...

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: токен

22. … — создание различных копий вируса путем замены блоков команд на эквивалентные, перестановки местами кусков кода, вставки между значащими кусками кода «мусорных» команд, которые практически ничего не делают.

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: метаморфизм

23. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?

*(Ответ записать словом на английском языке, все буквы заглавные)*

верный ответ: OECD

24. ….. – это вычислительная инфраструктура (серверы, хранилища данных, сети, операционные системы), которая предоставляется клиентам для разворачивания и запуска собственных программных решений

*(Ответ записать словом в именительном падеже на английском языке, первая буква заглавная)*

верный ответ: Iaas

25. FLOAT содержит ….. байта информации.

*(Ответ записать в виде целого числа)*

верный ответ: 4

26. Сколько Петабайт в Зеттабайте?

*(Ответ записать в виде целого числа)*

верный ответ: 1024

27. Набор утилит, и программный каркас для выполнения распределённых программ, работающих на кластерах – это ….

*(Ответ записать словом с маленькой буквы в именительном падеже на английском языке)*

верный ответ: hadoop

28. … - это метод, при котором символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности.

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: гаммирование

29. Спам, который имеет своей целью опорочить ту или иную организацию носит название черный …..

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: пиар

30. …. – это антивирус, который представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов.

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: сторож

**Ответы (ключи) на тестовые задания для Индикатора компетенции УК-2**

|  |  |
| --- | --- |
| № задания | Ответ |
| 1 | б |
| 2 | а |
| 3 | а, г |
| 4 | б, в, г |
| 5 | а, б, в |
| 6 | б |
| 7 | а |
| 8 | в |
| 9 | а, б, г, д |
| 10 | а, в, г |
| 11 | Deep  |
| 12 | кибербезопасность |
| 13 | киберугроза |
| 14 | фишинг |
| 15 | файрвол |
| 16 | скимминг |
| 17 | детектор |
| 18 | ревизор |
| 19 | троян |
| 20 | архивация  |
| 21 | токен |
| 22 | метаморфизм |
| 23 | OECD |
| 24 | Iaas |
| 25 | 4 |
| 26 | 1024 |
| 27 | hadoop |
| 28 | гаммирование |
| 29 | пиар |
| 30 | сторож |

**Компетенция – ОПК-3**

 **Индикатор компетенции ОПК-3.2**

**Тестовые задания закрытого типа**

1. Кто является основным ответственным за определение уровня классификации информации?

а) Руководитель среднего звена

б) Высшее руководство

в) Владелец

г) Пользователь

верный ответ: в

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

а) Сотрудники

б) Хакеры

в) Атакующие

г) Контрагенты (лица, работающие по договору)

верный ответ: а

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

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

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

в) улучшить контроль за безопасностью этой информации

г) снизить уровень классификации этой информации

верный ответ: в

4. Что самое главное должно продумать руководство при классификации данных?

а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

б) Необходимый уровень доступности, целостности и конфиденциальности

в) Оценить уровень риска и отменить контрмеры

г) Управление доступом, которое должно защищать данные

верный ответ: б

5. Кто несет основную ответственность за гарантии того, что данные классифицированы и защищены?

а) Владельцы данных

б) Пользователи

в) Администраторы

г) Руководство

верный ответ: г

6. Что такое процедура?

а) Правила использования программного и аппаратного обеспечения в компании

б) Пошаговая инструкция по выполнению задачи

в) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

г) Обязательные действия

верный ответ: б

7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

а) Поддержка высшего руководства

б) Эффективные защитные меры и методы их внедрения

в) Актуальные и адекватные политики и процедуры безопасности

г) Проведение тренингов по безопасности для всех сотрудников

верный ответ: а

8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски

б) Когда риски не могут быть приняты во внимание по политическим соображениям

в) Когда необходимые защитные меры слишком сложны

г) Когда стоимость контрмер превышает ценность актива и потенциальные потери

верный ответ: г

9. Что такое политики безопасности?

а) Пошаговые инструкции по выполнению задач безопасности

б) Общие руководящие требования по достижению определенного уровня безопасности

в) Широкие, высокоуровневые заявления руководства

г) Детализированные документы по обработке инцидентов безопасности

верный ответ: в

10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

а) Анализ рисков

б) Анализ затрат / выгоды

в) Результаты ALE

г) Выявление уязвимостей и угроз, являющихся причиной риска

верный ответ: б.

**Вопросы открытого типа**

11. Интернетизированная сеть, в которой соединения между информационными ресурсами устанавливаются только между доверенными (и многократно проверенными) IP адресами, с использованием специфицированных протоколов и портов называется … Web.

*(Ответ записать словом с большой буквы в именительном падеже на английском языке)*

верный ответ: Deep

12. …. – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных.

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: кибербезопасность

13. … – это незаконное проникновение или угроза вредоносного проникновения в виртуальное пространство для достижения политических, социальных или иных, целей.

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: киберугроза

14. Посылка обманных сообщений с целью обмануть пользователей и получить их личные данные носит название ….

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: фишинг

15. Устройство или программное обеспечение, которое фильтрует и контролирует сетевой трафик, позволяя разрешить или блокировать доступ в зависимости от заданных правил – это ….

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: файрвол

16. Форма мошенничества, при которой злоумышленник получает доступ к финансовым данным пользователя, используя специальное устройство для чтения информации с магнитных полос карты носит название …

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: скимминг

17. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы носит название …

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: детектор

18. Антивирус 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 носит название …

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: ревизор

19. Программа, осуществляющая несанкционированные действия по сбору, и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию носит название …

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: троян

20. Процесс преобразования информации, хранящейся в файле к виду, при котором уменьшается избыточность в ее представлении и соответственно требуется меньший объем памяти для ее хранения называется … файла

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: архивация

21. Устройство хранения криптографических ключей, аппаратный ключ носит название ...

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: токен

22. … — создание различных копий вируса путем замены блоков команд на эквивалентные, перестановки местами кусков кода, вставки между значащими кусками кода «мусорных» команд, которые практически ничего не делают.

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: метаморфизм

23. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?

*(Ответ записать словом на английском языке, все буквы заглавные)*

верный ответ: OECD

24. ….. – это вычислительная инфраструктура (серверы, хранилища данных, сети, операционные системы), которая предоставляется клиентам для разворачивания и запуска собственных программных решений

*(Ответ записать словом в именительном падеже на английском языке, первая буква заглавная)*

верный ответ: Iaas

25. FLOAT содержит ….. байта информации.

*(Ответ записать в виде целого числа)*

верный ответ: 4

26. Сколько Петабайт в Зеттабайте?

*(Ответ записать в виде целого числа)*

верный ответ: 1024

27. Набор утилит, и программный каркас для выполнения распределённых программ, работающих на кластерах – это ….

*(Ответ записать словом с маленькой буквы в именительном падеже на английском языке)*

верный ответ: hadoop

28. … - это метод, при котором символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности.

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: гаммирование

29. Спам, который имеет своей целью опорочить ту или иную организацию носит название черный …..

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: пиар

30. …. – это антивирус, который представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов.

*(Ответ записать словом с маленькой буквы в именительном падеже)*

верный ответ: сторож

**Ответы (ключи) на тестовые задания для Индикатора компетенции ОПК-3**

|  |  |
| --- | --- |
| № задания | Ответ |
| 1 | в |
| 2 | а |
| 3 | в |
| 4 | б |
| 5 | г |
| 6 | б |
| 7 | а |
| 8 | г |
| 9 | в |
| 10 | б |
| 11 | Deep  |
| 12 | кибербезопасность |
| 13 | киберугроза |
| 14 | фишинг |
| 15 | файрвол |
| 16 | скимминг |
| 17 | детектор |
| 18 | ревизор |
| 19 | троян |
| 20 | архивация  |
| 21 | токен |
| 22 | метаморфизм |
| 23 | OECD |
| 24 | Iaas |
| 25 | 4 |
| 26 | 1024 |
| 27 | hadoop |
| 28 | гаммирование |
| 29 | пиар |
| 30 | сторож |

Критерии оценки освоения компетенций:

|  |  |
| --- | --- |
| Уровень освоения компетенции | Процент баллов максимального количества  |
| Компетенция сформирована | 50% и выше |
| Компетенция не сформирована | менее 50% |