Перечень вопросов
по оценке сформированности компетенций образовательной программы
09.03.02 «Информационные системы и технологии»
по дисциплине «Основы компьютерной безопасности»

УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

1. Почему внутренние угрозы безопасности могут нанести организации еще больший ущерб, чем внешние?
2. Какие три способа можно использовать для обеспечения конфиденциальности информации?
3. Какой способ используется для проверки целостности данных?
4. Назовите мотивацию белого хакера.
5. Какие элементы являются компонентами тройки CIA?
6. Что такое кибервойна?
7. Как еще называют конфиденциальность информации?
8. Что является примером «хактивизма»?
9. Какой инструмент используется для получения списка открытых портов на сетевых устройствах?
10. Каким образом в атаках используются «зомби»?
11. Для чего предназначен руткит?
12. Назовите основную цель отравления SEO (поисковой оптимизации).
13. Какой тип атаки позволяет злоумышленнику воспользоваться методом подбора пароля (brute-force)?

ПК-7 Способность выполнять работы по обслуживанию программно-аппаратными средствами сетей и инфокоммуникаций

1. В чем заключается основная цель атак типа «отказ в обслуживании» (DoS-атак)?
2. Какие характеристики описывают программу-червь?
3. Каким образом можно скрыть вредоносное ПО?
4. Пользователь просматривает сайты в Интернете на ноутбуке через публичный Wi-Fi в кафе. Что пользователь должен проверить прежде всего, подключаясь к публичной сети?
5. Пользователю трудно запоминать пароли для разных учетных записей в Интернете. Как пользователю лучше всего поступить, чтобы решить эту проблему?
6. Каким образом надежнее всего можно предотвратить использование уязвимости в Bluetooth?
7. Каким образом пользователям, работающим на общем компьютере, скрыть личную историю просмотров в браузере от остальных сотрудников, которые могут пользоваться этим компьютером?
8. Какая конфигурация беспроводного маршрутизатора считается неадекватной защитой для беспроводной сети?
9. Если данные хранятся на локальном жестком диске, как лучше всего защитить их от неавторизованного доступа?

10. Как пользователю обезопасить себя от «подслушивания» сетевого трафика, когда он пользуется публичной точкой доступа Wi-Fi на своем ПК?
11. Сетевой администратор проводит тренинг для персонала о том, как создавать надежный и эффективный пароль. Какой пароль будет труднее всего взломать злоумышленнику?
12. Потребитель хотел бы распечатать фотографии, хранящиеся в облачном хранилище, используя онлайн-сервис печати третьей стороны. После успешного входа в облачную учетную запись пользователю автоматически предоставляется доступ к онлайн-сервису печати третьей стороны. Почему стала возможной такая автоматическая аутентификация?
13. Технология какого типа может предотвратить слежение вредоносным ПО за активностью пользователей, сбор персональной информации и выдачу нежелательной всплывающей рекламы на компьютере пользователя?
14. Почему устройства IoT представляют больше риска, чем другие вычислительные устройства в сети?
15. Какой инструмент может выявлять вредоносный трафик, сравнивая содержимое пакета с известными сигнатурами атак?
16. Какой протокол используется решением по кибербезопасности Cisco Cyberthreat Defense для сбора информации о трафике, проходящем по сети?
17. Назовите последний этап структуры убийственной цепочки.
18. Любое устройство, которое выполняет управление трафиком, входящим или выходящим из сети, или его фильтрацию — это ... (2 слова через пробел)
19. Какой тип атаки способен прерывать оказание услуг, переполняя сетевые устройства поддельным трафиком?