**Перечень вопросов для итогового контроля студентов 4 курса по предмету "Политика кибербезопасности".**

**Осенний семестр 2023/2024 учебного года**

1. Понятие кибербезопасности и ее задачи
2. Виды национальной безопасности и ее роль в политике кибербезопасности
3. Основные задачи в обеспечении информационной безопасности
4. Какие шаги следует предпринять для определения политики кибербезопасности?
5. Каков жизненный цикл политики безопасности?
6. Привести пример из шаблонов политики безопасности, разработанных SANS (system Administration Networking and security).
7. Роль стратегии и архитектуры кибербезопасности в архитектуре предприятия.
8. Перечислите основные термины кибербезопасности.
9. Каковы области знаний о кибербезопасности?
10. Какова роль человеческого фактора в политике кибербезопасности?
11. Что подразумевается под конфиденциальностью в кибербезопасности?
12. Почему необходимо думать как атакующий?
13. Предоставить информацию о методах предотвращения киберпреступлений и киберзаконах.
14. Что вы понимаете под иерархией политики кибербезопасности?
15. Какая политика безопасности используется на предприятиях в сфере информационных технологий?
16. Опишите 4 категории политики использования Интернета?
17. Что вы подразумеваете под логическим управлением использованием?
18. Что такое метод контроля использования DAC и его особенности?
19. Что такое модель Белла-Ла Падула и ее роль в политике кибербезопасности?
20. Предоставить информацию о международных стандартах в области кибербезопасности.
21. Объясните классификацию компьютерных вирусов по среде обитания.
22. Какова роль межсетевых экранов в защите информации в политике кибербезопасности?
23. Какая конфигурация межсетевого экрана соответствует политике безопасности?
24. Роль антивирусных средств в защите операционных систем
25. Определите эти слова :

* Авторизация
* Авторские права
* Аудит безопасности
* Bot
* Несанкционированное использование информации

1. Дайте определение этим терминам безопасности:

* Удобство использования
* Организационная защита информации
* Идентификатор использования
* Социальная инженерия
* Инсайдер

1. Что такое технологии аутентификации?
2. Облачная антивирусная технология. Предпосылки для создания «Антивирусных облаков».
3. В чем разница между кибербезопасностью и информационной безопасностью?
4. Процедуры найма и увольнения для организации информационных систем?
5. Защита корпоративных систем от воздействия вредоносных программ и вирусов.
6. Защита учетных записей пользователей с помощью Google Authenticator
7. Обеспечение защиты от кибератак с помощью брандмауэра
8. Использование инструментов управления паролями пользователей
9. Резервное копирование пользовательских данных с помощью облачных сервисов
10. Инструменты обеспечения конфиденциальности данных пользователей в сети Интернет
11. Инструменты обеспечения конфиденциальности данных пользователей в сети Интернет
12. Какова роль отдельных лиц в предотвращении кибербезопасности?
13. Что такое средства кибербезопасности?
14. Какова важность обучения сотрудников безопасности в политике кибербезопасности?
15. Понимание управления данными?
16. Каковы методы внедрения и разработки политики кибербезопасности?
17. Какова роль геополитики в политике кибербезопасности?
18. Что такое биометрическая аутентификация пользователя?
19. Определить концепции аутентификации, авторизации и управления поведением пользователей?
20. Что вы понимаете под методами аутентификации на основе пароля?
21. Электронная цифровая подпись. Объясните основные процедуры цифровой подписи.
22. Что вы подразумеваете под мониторингом и аудитом безопасности корпоративных информационных систем?
23. Дайте определение цифровой криминалистике?
24. Виды киберпреступлений и их определение?
25. Каков подход России к политике кибербезопасности?
26. Меры против риска кибермошенничества.
27. Услуги по защите от кибератак в России.
28. История кибератак.
29. Воздействие кибератак на организации.
30. Каков подход США к политике кибербезопасности?
31. Перечислите основные виды кибератак.
32. Последствия кибератак в глобальном масштабе.
33. Современные решения для защиты от кибератак.
34. Роль правоохранительных органов в предотвращении кибератак.
35. Предоставить информацию о рейтинге организаций кибербезопасности Узбекистана за 2022 год.
36. Каков подход Узбекистана к политике кибербезопасности?
37. Показатели Республики Узбекистан в индексе NCSI в 2021 году.
38. Объясните разницу между кибербезопасностью и информационной безопасностью.
39. Перечислите этапы разработки политики безопасности.
40. Что следует учитывать при разработке политики информационной безопасности?
41. Узнайте об инструментах кибербезопасности.
42. Узнайте об инструментах сетевой безопасности для кибербезопасности.
43. Каковы основные цели кибербезопасности?
44. Дайте информацию о типах кибератак.
45. Кратко охарактеризуйте состояние кибербезопасности в США на сегодняшний день.
46. Какова роль кибербезопасности в современном мире?
47. Классификация рисков в кибербезопасности.
48. Показатели кибербезопасности России в 2021 году.
49. Необходимость политики безопасности в организациях.
50. Инструменты проверки паролей и сканирования пакетов в кибербезопасности.
51. Инструменты сетевой безопасности в кибербезопасности.
52. Инструменты обнаружения веб-уязвимостей в кибербезопасности.
53. Инструменты мониторинга сетевой безопасности в кибербезопасности.
54. Средства обнаружения сетевых вторжений в кибербезопасности.
55. Дайте информацию о Законе Республики Узбекистан о кибербезопасности.
56. Перечислите показатели Республики Узбекистан в индексе NCSI?
57. Какие человеческие риски связаны с кибербезопасностью?
58. Объясните функции обучения, SSL-сертификаты, брандмауэры, средства защиты от вредоносных программ(Antimalware) ?
59. Кратко опишите киберугрозы в России?
60. Общие понятия фишинговых атак.
61. Общие понятия DDoS-атак.
62. Объясните вредоносное ПО Ransomware?
63. GAFA - Насколько сильна «большая четверка» США?
64. На каком этапе концепция кибербезопасности развивалась в Азии?
65. Объясните эволюцию кибербезопасности в современную эпоху и угрозы, с которыми она сталкивается.
66. Перечислите многочисленные последствия наличия сильной системы кибербезопасности и кибератак на организации?
67. Что такое профессиональные вредности?
68. Какие услуги предоставляет Центр кибербезопасности?
69. ТОП-5: Перечислите организации, обеспечивающие кибербезопасность в Узбекистане.
70. Кто определяет единую государственную политику в сфере кибербезопасности и какие полномочия им предоставлены?
71. Когда был принят Закон Республики Узбекистан «О кибербезопасности» и перечислите цели этого закона.
72. Объясните основные понятия кибербезопасности и информационной безопасности.
73. Перечислите этапы и цели разработки политики.
74. Какие существуют категории политик безопасности?