***Программа итогового контроля по дисциплине***

***«*Безопасность и конфиденциальность данных*»***

***на 2023/2024 учебный год***

*осенний семестр*

**Факультет** *ИТ*

**Кафедра** *ИИ и BD*

**Шифр и наименование образовательной программы**

**«5B06101 –** *Инженерия Данных***»**

**Отделение**: *полигруппа*

**Уровень образования** *бакалавр*

**Курс***: 2*

**Преподаватель**: *Шортанбаева А.Т.*

**Форма и платформа проведения итогового контроля** –

Стандартно - устно (офлайн)

**Формат экзамена** - *офлайн*

**Темы экзаменационных вопросов (программа)**

1. Правила безопасности при работе с компьютером.
2. Перечислить и охарактеризуйте меры защиты информации в компьютере?
3. Что такое вирус? Дать классификацию вирусов.
4. Что такое антивирусная программа? Дать классификацию антивирусных программ. Привести примеры.
5. Перечислите услуги, обеспеченные SSL или TLS.
6. Объясните, как в SSL создается из *предварительного главного секретного кода* *главный секретный код*.
7. Объясните, как в TLS создается из *предварительного главного секретного кода* *главный секретный код*.
8. Объясните, как в SSL создается из *главного секретного кода* *материал для ключей*.
9. Объясните, как в TLS создается из *главного секретного кода* *материал для ключей*.
10. Покажите различия между сеансом и соединением.
11. Перечислите цель четырех протоколов, определенных в SSL или TLS.
12. Определите цель каждой фазы в *протоколе установления соединения*.
13. Сравните и противопоставьте *протоколы установления соединения* в SSL и TLS.
14. Сравните и противопоставьте *протоколы передачи записей* в SSL и TLS.
15. Покажите, как SSL или TLS реагируют на атаку воспроизведения. То есть покажите, как SSL или TLS отвечает нападавшему, который пытается имитировать одно или более сообщений установления соединения (предварительно записав сообщение).
16. Покажите, как SSL или TLS реагируют на атаку грубой силы. Может ли злоумышленник использовать исчерпывающий компьютерный поиск и найти ключ шифрования в SSL или TLS? Какой протокол более безопасен в этом отношении - SSL или TLS?
17. Каков риск использования ключей короткой длины в SSL или TLS? Какую атаку злоумышленник может применить, если ключи коротки?
18. Действительно ли SSL или TLS относительно безопасны к атаке "посредника"? Может ли злоумышленник создать *материал для ключей* между клиентом и самим собой и между собой и сервером?
19. SSL-архитектура и роль
20. Построение системы защиты персональных данных
21. Рассмотри каждый *класс* ИСПД в отдельности, и перечисли все категории
22. Уязвимость информационной системы персональных данных
23. Что такое информационная безопасность, принципы защиты информации
24. Целостность информационной безопасности
25. Хэш для сообщения Finished в TLS
26. Как обеспечить безопасность данных при использовании общественных Wi-Fi-сетей?
27. Что такое защита от вредоносного программного обеспечения и как она работает?
28. Какие меры предосторожности следует принимать при отправке чувствительных данных по электронной почте?
29. Какой роль играют физические меры безопасности в защите данных?
30. Что такое управление рисками в области безопасности данных?