**Факультет Вычислительной математики и кибернетики**

**Межфакультетский курс**

**Технологические угрозы и системы обеспечения кибербезопасности**

Technological threats and cybersecurity systems

**Вопросы к зачету:**

1. Внешние и внутренние угрозы ИБ и уязвимости.
2. Понятие и основные подсистемы обеспечения сетевой информационной безопасности.
3. Понятие вредоносного программного обеспечения (ЗПО), его виды, основные техники и сценарии проникновения, эволюционное развитие.
4. Таргетированные атаки и сложные угрозы ИБ. Информация об угрозах (Cyber Threat Intelligence).
5. Понятие SIEM (security information event management) платформы как ключевой подсистемы в обеспечении ИБ крупной организации, базовая архитектура, основной функционал и сценарии использования..
6. Понятие и назначение SOC (Security Operation Center), ключевые процессы, шаги внедрения, архитектурные подходы.
7. Информационная безопасность индустриальной среды, особенности и применяемые подсистемы ИБ.