Аннотация к рабочей программе дисциплины
Искусственный интеллект для информационной безопасности

Направление подготовки: 09.04.01 Информатика и вычислительная техника
Направленность (профиль*):* Инженерия искусственного интеллекта
Квалификация выпускника: магистр
Целью освоения дисциплины является: изучение способов использования искусственного интеллекта в области обеспечения информационной безопасности. В рамках курса студенты сделают выводы о потенциале использования технологий искусственного интеллекта для предотвращения несанкционированного доступа к информации, а также уменьшения последствий при нарушении информационной безопасности
Объем дисциплины: 3 зачетные единицы – 108 часов
Семестр: 3
Краткое содержание основных разделов дисциплины:

№ п/п раздела	Основные разделы дисциплины	Краткое содержание разделов дисциплины
1	**Основы компьютерной безопасности**	Типы атак в информационной безопасности Криптография. Хэш-функции. Безопасность компьютерных сетей и сетевых протоколов. Безопасность в ОС Linux. Инъекции. Бинарные уязвимости
2	**Применение машинного обучения для задач информационной безопасности**	Определение спама. Классификация сетевых атак. Определение распределенной сетевой атаки “отказ в обслуживании” Определение злонамеренных (malicious) сайтов Определение инъекций Поиск злонамеренного программного обеспечения (malware) Анализ аномалий в активности пользователей
3	**Проекты искусственного интеллекта в области информационной безопасности**	Жизненный цикл проекта создания приложений искусственного интеллекта для информационной безопасности. Подготовка набора данных в информационной безопасности Выбор модели и ее обучение. Оценка качества модели Разработка приложения, использующего модель. Внедрение приложения в практическое

Форма промежуточной аттестации: зачет