АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки (специальность)	09.04.01 «Информатика и вычислительная техника»
Направленность (профиль) подготовки	Инженерия искусственного интеллекта
Цель освоения дисциплины	Целью дисциплины «Искусственный интеллект для информационной безопасности» является изучение возможных путей использования искусственного интеллекта в области обеспечения информационной безопасности. Формирование умений по использованию технологий искусственного интеллекта для предотвращения несанкционированного доступа к информации, а также уменьшения последствий при нарушении информационной безопасности.
Общая трудоемкость дисциплины	3 зачетных единицы, 108 часов
Форма промежуточной аттестации	зачет
Краткое содержание дисциплины:	Типы атак в информационной безопасности. Криптография. Хэш-функции. Безопасность компьютерных сетей и сетевых протоколов. Безопасность в ОС Linux. Инъекции. Бинарные уязвимости. 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. 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 использование.

Аннотацию рабочей программы составил: зав. каф. ВТиСУ К.В. Куликов