Учебно-методические материалы:

- ГОСТ Р 71539-2024. Системы искусственного интеллекта. Процессы жизненного цикла;
- ГОСТ Р 59276-2020. Системы искусственного интеллекта. Способы обеспечения доверия;
- Методические рекомендации ФСТЭК России по обеспечению безопасности ИИ-систем;
- Объяснение и использование адверсариальных примеров. Ян Дж. Гудфеллоу, Джонатан Шленс, Кристиан Сегеди и другие, // ICLR, 2015;
- К вопросу об оценке устойчивости нейронных сетей. Николас Карлини, Дэвид Вагнер и другие, IEEE S&P, 2017;
- Николенко С. Глубокое обучение. Погружение в мир нейронных сетей / С. Николенко, А. Кадурин, Е. Архангельская. – Питер, 2020;
- Распознавание образов и машинное обучение. Бишоп Кристофер М. ; Переводчик: Клюшин Дмитрий Анатольевич ; Издательство: Вильямс; Год выпуска: 2020;
- Модель угроз для ИИ-систем (внутренний документ Банка)