ПРОГРАММА
Круглого стола «Искусственный интеллект и кибербезопасность»

Дата: 27 октября 2026 года, вторник
Время: 16:30–18:00 (90 минут)
Место проведения: Университет ИТМО, Санкт-Петербург, Песочная набережная, д. 14, лит. А.

О КРУГЛОМ СТОЛЕ

Круглый стол посвящен современным тенденциям применения искусственного интеллекта в информационной безопасности, новым возможностям и угрозам, связанным с развитием интеллектуальных технологий, а также вопросам их практического внедрения и подготовки специалистов. Представители науки, бизнеса и образования обсудят, как искусственный интеллект меняет противостояние атакующих и защитников, какие технологии уже доказали свою эффективность, насколько безопасно применение автономных интеллектуальных систем и как изменятся требования к специалистам по информационной безопасности в ближайшие годы. Особое внимание будет уделено взаимодействию научных организаций, университетов и индустрии, перспективным направлениям исследований и проблемам внедрения научных результатов в практику.

МОДЕРАТОРЫ

Чечулин Андрей Алексеевич - кандидат технических наук, доцент, ведущий научный сотрудник, руководитель Международного центра цифровой криминалистики Санкт-Петербургского федерального исследовательского центра Российской академии наук (СПб ФИЦ РАН).

Области научных интересов: информационная безопасность, цифровая криминалистика, обнаружение компьютерных атак, исследование киберинцидентов, безопасность киберфизических систем и применение искусственного интеллекта в информационной безопасности.

Забежайло Михаил Иванович - доктор физико-математических наук, профессор, Федеральный исследовательский центр «Информатика и управление» Российской академии наук (ФИЦ ИУ РАН).

Области научных интересов: искусственный интеллект, интеллектуальный анализ данных, машинное обучение, формализация рассуждений, индуктивный вывод и поддержка принятия решений.

УЧАСТНИКИ ДИСКУССИИ

Новикова Евгения Сергеевна - кандидат технических наук, доцент, заведующая кафедрой информационных систем Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина).

Области научных интересов: информационная безопасность, обнаружение аномалий и компьютерных атак, машинное обучение, анализ и визуализация данных безопасности, защита киберфизических систем.

Окунева Дарина Владимировна - кандидат технических наук, доцент, руководитель Аналитического центра кибербезопасности (АЦК) компании «Газинформсервис».

Направления профессиональной деятельности: информационная безопасность, разработка и применение технологий киберзащиты, анализ киберугроз, развитие

компетенций специалистов по информационной безопасности, внедрение отечественных решений в области кибербезопасности.

Бучаев Абдулхамид Яхьяевич - старший эксперт по защите искусственного интеллекта, Альфа-Банк, Университет ИТМО.

Профессиональная деятельность сосредоточена на актуальном и активно развивающемся направлении — MLSecOps (Machine Learning Security Operations), то есть на обеспечении безопасности жизненного цикла моделей машинного обучения и искусственного интеллекта.

РЕГЛАМЕНТ ПРОВЕДЕНИЯ

16:30–16:45

Вступительное выступление Андрея Чечулина «ИИ в кибербезопасности: инструмент защиты, средство атаки и объект исследования».

16:45–17:10

Блок 1. Технологии и угрозы.

17:10–17:30

Блок 2. Практика и внедрение.

17:30–17:50

Блок 3. Специалисты и будущее.

17:50–18:00

Вопросы аудитории, подведение итогов.

ВОПРОСЫ ДЛЯ ОБСУЖДЕНИЯ

БЛОК 1. ТЕХНОЛОГИИ И УГРОЗЫ

16:45–17:10

1. Кто сегодня быстрее осваивает ИИ: атакующие или защитники?

Какие изменения в кибератаках и средствах защиты уже произошли благодаря ИИ? Получают ли злоумышленники преимущество за счет доступности генеративных моделей и автоматизации?

2. Какие технологии ИИ действительно меняют кибербезопасность, а какие пока остаются маркетингом?

Большие языковые модели, автономные интеллектуальные агенты, машинное обучение для обнаружения атак, интеллектуальная автоматизация SOC. Где уже есть измеримые результаты, а где ожидания опережают реальные возможности?

3. Кто и как должен защищать сами системы искусственного интеллекта?

Атаки на модели, отравление данных, внедрение вредоносных инструкций, манипулирование интеллектуальными агентами. Достаточно ли традиционных подходов к информационной безопасности или нужны принципиально новые методы защиты?

БЛОК 2. ПРАКТИКА И ВНЕДРЕНИЕ

17:10–17:30

4. Можно ли доверить ИИ самостоятельное реагирование на кибератаки?

Где проходит граница между рекомендацией, автоматическим действием и решением человека? Какие задачи можно полностью автоматизировать и кто должен отвечать за ошибки интеллектуальных систем?

5. Почему перспективные научные разработки в области ИИ не всегда доходят до реального внедрения?

Чего не хватает для перехода от исследовательского прототипа к промышленному решению? Какие задачи бизнеса остаются нерешенными и на какие направления следует ориентировать научные исследования?

БЛОК 3. СПЕЦИАЛИСТЫ И БУДУЩЕЕ

17:30–17:50

6. Как ИИ меняет требования к специалистам по информационной безопасности?

Какие профессиональные задачи будут автоматизированы, какие компетенции станут наиболее востребованными и потребуется ли в будущем столько же специалистов по кибербезопасности?

7. Успевает ли система образования готовить специалистов к новым угрозам и технологиям?

Нужно ли пересматривать образовательные программы, чему обучать будущих специалистов по информационной безопасности и как обеспечить участие бизнеса и научных организаций в их подготовке?

8. Какой будет кибербезопасность через пять лет?

Станут ли автономные интеллектуальные агенты основными участниками противостояния атакующих и защитников? Какие проблемы сегодняшнего дня исчезнут, а какие новые угрозы появятся?

ФОРМАТ ПРОВЕДЕНИЯ

Круглый стол проводится в формате открытой модерируемой дискуссии.

После вступительного выступления участники последовательно обсудят вопросы, сгруппированные в три тематических блока. Модераторы направляют обсуждение, адресуют вопросы участникам с учетом их профессионального опыта и обеспечивают возможность обмена различными точками зрения.

В заключительной части предусмотрены вопросы аудитории и подведение итогов.

Продолжительность: 90 минут.

Язык проведения: русский.