ПРОГРАММА
Круглого стола «Новые тренды в кибербезопасности»

Дата: 26 октября 2026 года, понедельник
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 новым трендам в кибербезопасности. Развитие ключевых сквозных информационных технологий, в том числе, квантовых технологий и технологий искусственного интеллекта меняет ландшафт кибербезопасности: от появления новых классов угроз до применения перспективных квантово-устойчивых решений на основе упомянутых технологий. В рамках круглого стола ведущие учёные и представители RnD подразделений бизнеса обсудят, какие фундаментальные и поисковые научные исследования в области кибербезопасности необходимо проводить сегодня, чтобы обеспечить технологический суверенитет страны в условиях роста киберугроз, повышения требований ИБ к объектам КИИ РФ и уже недостаточности известных технологий кибербезопасности. Дискуссия сосредоточена на формировании долгосрочной научно-исследовательской повестки и определении приоритетных направлений развития кибербезопасности.

МОДЕРАТОР

Петренко Сергей Анатольевич - доктор технических наук, профессор, руководитель группы, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Федеральная территория «Сириус», Россия.

Области научных интересов: информационная безопасность и киберустойчивость объектов КИИ РФ, квантовая и постквантовая кибербезопасность, раннее обнаружение, нейтрализация и предупреждение компьютерных атак, проактивная безопасность киберфизических систем, разработка иммунных систем защиты информации, технологии ИИ, технологии самовосстановления объектов КИИ РФ.

УЧАСТНИКИ ДИСКУССИИ

Игорь Борисович Саенко (СПб ФИЦ РАН) – доктор технических наук, профессор, ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук. Основные работы опубликованы в области исследования теоретических и практических проблем использования информационных и телекоммуникационных технологий, в том числе защиты информации в компьютерных сетях, искусственного интеллекта, баз данных, поддержки принятия решений при проектировании и планировании использования информационных систем. Является автором более 400 научных работ, в том числе 10 учебников, учебных пособий и монографий.

Евгений Сергеевич Абрамов (ЮФУ) - кандидат технических наук, доцент, заведующий кафедрой безопасности информационных технологий им. О.Б. Макаревича (БИТ ИКТИБ ЮФУ). Области научных интересов: информационная безопасность, обнаружение аномалий и компьютерных атак, машинное обучение, анализ и визуализация данных безопасности, защита киберфизических систем.

Алексей Михайлович Вульфин (УУНиТ) - доктор технических наук, профессор, профессор кафедры вычислительной техники и защиты информации Уфимского университета науки и технологий. Области научных интересов: информационная безопасность, модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных, технологии обнаружение аномалий и компьютерных атак, архитектура и технологии построения центров мониторинга ИБ, технологии искусственного интеллекта, компьютерно-техническая экспертиза, микропроцессоры и микропроцессорные системы.

Илья Юрьевич Попов (ИТМО) - кандидат технических наук, доцент ИТМО. Область научных интересов: Методы и системы защиты информации, информационная безопасность, роевые системы и беспилотные технологии. Руководитель секции гонок дронов — университетской команды «Кронверкские Барсы», вице-президент федерации гонок дронов Ленинградской области. Руководитель ряда проектов ИТМО по разработке и тестированию беспилотных транспортных систем (совместно с НИИАС).

Александр Алексеевич Менщиков (ИТМО) - кандидат технических наук, доцент, декан ИТМО, директор учебно-практического центра — Киберполигон. Области научных интересов: формальная верификация нейросетевых систем технического зрения и управление доменным сдвигом синтетических данных в задачах кооперативного восприятия беспилотных транспортных средств, разработка алгоритмов для создания автоматических цепочек рассуждения большой языковой модели, создание систем обнаружения, нейтрализации и предупреждения компьютерных атак на объекты КИИ РФ, разработка математических моделей противодействия компьютерным атакам в учебных киберполигонах на основе принципов Attack-Defense CTF, создание технологий обеспечения целостности информации в системах кооперативного восприятия V2X для мультиагентных автономных транспортных средств.

РЕГЛАМЕНТ ПРОВЕДЕНИЯ

16:30–16:45

Вступительное слово Сергея Петренко «Новые вызовы и угрозы кибербезопасности».

16:45–17:00

Блок 1. Современные тренды кибербезопасности.

17:00–17:15

Блок 2. Квантовая и постквантовая кибербезопасность.

17:15–17:30

Блок 3. Применение технологий ИИ в кибербезопасности

17:30-17:45

Блок 4. Развитие технологий мониторинга и операционного управления ИБ (SOC, MSSP, CERT и CIRT и др.)

17:45–18:00

Вопросы аудитории, подведение итогов.

ВОПРОСЫ ДЛЯ ОБСУЖДЕНИЯ

БЛОК 1. Современные тренды кибербезопасности.

16:45–17:00

1. Что из перечисленного по Вашему мнению наиболее актуально для развития периметровой защиты объектов КИИ РФ?

Распознавание технологий веб-сервера и развитие рекомендаций по защите? Виджет «здоровья» приложений в реальном масштабе времени? Развитие профилей информационной безопасности? Быстрое создание исключений прямо из журнала атак? Автоматизация через Ansible (IaC)? Расширенная защита JSON и XML? Свои варианты ответов?

2. Какие технологические тренды кибербезопасности действительно полезны на практике, а какие пока остаются в статусе многообещающих технологий ИБ?

- **Реализация принципа «Secure by Design» (безопасность по умолчанию),** подразумевающего проектирование и создание автоматизированных систем в защищенном исполнении, начиная с первых этапов жизненного цикла (анализ требований, техническое проектирование) такого создания.
- **Идентификация и контроль доступа (Identity Security): смещение фокуса** защиты с периметра системы на конкретные учетные записи, усиление многофакторной аутентификации (MFA) и контроль цифровых следов.
- **Адаптация к моделям MaaS (Malware-as-a-Service) и Attacker AI-as-a-Service (вредоносный ИИ по подписке), когда злоумышленники взяли на вооружение** «услуги»: фишинг, шифровальщики и использование стилеров на «черных» маркетплейсах по подписке.
- **Акцент на обеспечение ИБ цепочек поставок (Supply Chain Security), учет рисков** компрометации через уязвимости в сторонних ПО, слабости подрядных или партнерских организаций и их сервисах.
- **Переход от «реагирования на вызовы ИБ» к «обеспечению киберустойчивости»,** понимание, что 100% защиты не существует и риски ИБ остаются всегда, управление рисками ИБ, развитие метрик и мер ИБ.

БЛОК 2. Квантовая и постквантовая кибербезопасность.

17:00–17:15

3. Глобальный переход к постквантовой криптографии перестал быть исключительно исследовательской перспективой и трансформировался в инженерно-организационную задачу миграции, сроки и стоимость которой напрямую определяются параметрами базовых криптографических примитивов. Существующие стандартизированные семейства (решёточные, хеш-ориентированные, MQ-схемы) демонстрируют компромисс между уровнем стойкости и накладными расходами на

передачу, хранение и верификацию, что делает их применение в высоконагруженных распределённых системах сопряжённым с архитектурными ограничениями.

Какие методы конструирования постквантовых алгоритмов ЭЦП в настоящее время наиболее востребованы и почему? Как оценить стойкость криптопримитивов? Как реализовать на практике архитектуру программных средств построения постквантовых ЭЦП?

4. Переходный этап миграции объектов критической информационной инфраструктуры на постквантовую криптографию требует поддержки гибридных схем подписывания (например, КНАА-2-ЭЦП + ГОСТ Р 34.10-2018).

Как определить достаточные процедуры агрегации подписей, маршрутизации фолбэка и оценки накладных расходов на хранение двойных криптографических материалов в реестре транзакций? Как формализовать протокол гибридного режима и оценить влияние на пропускную способность и объём состояния промежуточных узлов или нод.

БЛОК 3. Развитие технологий ИИ в кибербезопасности

17:15–17:30

В 2026 году наблюдается бурное развитие и внедрение ИИ-агентов и развитие мультиагентных систем в целом. При этом на первый план вышла инженерная задача не создания ИИ-агентов, а их развертывания. В результате, стали востребованы так называемые, открытые инфраструктуры для быстрого развертывания Agent Stack. Использование протокола Agent2Agent (A2A) позволило агентам из разных фреймворков более продуктивно взаимодействовать друг с другом. Подобные технологии вывели агентный ИИ на новый уровень развития.

Помимо этого не потеряли актуальность и следующие вопросы.

5. Как обеспечить требуемую точность универсальных языковых моделей (LLM), обученных на больших массивах данных, на конкретные предметные области и инженерные задачи ИБ. Какова здесь роль предметно-специфических языковых моделей (Domain-Specific Language Models, DSLM)? Как обучать упомянутые на узкоспециализированных датасетах?

6. Какие возможности открывают технологии ИИ для широкого применения на практике программотехнических средств разработки ПО, Low-code и no-code.

БЛОК 4. Развитие технологий мониторинга и операционного управления ИБ: SOC, MSSP, CERT/CIRT.

17:30-17:45

7. Какие технологические новинки мониторинга и управления ИБ ожидаются на горизоте ближайших трех лет?

- **SIEM + Next-Gen SIEM (сбор и корреляция событий ИБ):** развитие поведенческого анализа пользователей и сущностей (**UEBA**) для выявления ранее неизвестных аномалий.
- **EDR / XDR (детализированное обнаружение, нейтрализация и реагирование):** развитие функционала кибербезопасности на конечных точках, применение облачных сред и расширенного анализа сетевого трафика (NTA)? Как это повлияет на развитие единой цепочки кибератак (Kill Chain) и совершенствование

известных методик моделирования угроз безопасности информации MITRE и ФСТЭК России в целом?

- **SOAR / IRP (оркестрация и автоматизация):** развитие роботизированных сценариев (**Playbooks**) для своевременного обнаружения и изоляции скомпрометированных хостов и пр.?
- **ASM (Attack Surface Management):** развитие технологий управления внешней поверхностью кибератак, как это отобразится на развитие SOC 2 и следующего поколения (возможности внешнего мониторинга, отслеживание забытых ИТ-активов, открытых портов и теневых облачных сервисов Darknet (Shadow IT) и пр.?

ФОРМАТ ПРОВЕДЕНИЯ

Круглый стол проводится в формате открытой модерируемой дискуссии.

После вступительного выступления участники последовательно обсудят вопросы, сгруппированные в четыре 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.