DOI: 10.26583/bit.2025.3.15

УЧАСТИЕ В 34-ОЙ КОНФЕРЕНЦИИ «МЕТОДЫ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ 2025» (МИТСОБИ 2025)

с докладом

«Подход к формированию модели угроз доверенных интегральных микросхем для доверенных ПАК» (Кессаринский Л.Н., Сидорин Ю.Ю., Никифоров А.Ю., Дураковский А.П.)

23–26 июня 2025 в Репино (Ленинградская обл.) автор принимал участие в работе одной из старейших конференций по вопросам информационной безопасности – «Методы и технические средства обеспечения безопасности информации» имени Петра Дмитриевича Зегжды «МиТСОБИ 2025».

Данная заметка частично использует материал с официального сайта конференции, с которым полностью можно ознакомиться **https://mitsobi.ru/.**

В этом году основными темами для обсуждения в рамках конференции стали вопросы цифровой криминалистики и эволюции методов защиты критической информационной инфраструктуры. Мероприятие собрало экспертов в сфере информационной безопасности со всей России.

Конференция «Методы и технические средства обеспечения безопасности информации» (МиТСОБИ) – одна из старейших и наиболее авторитетных экспертных площадок в сфере защиты информации, сохраняющая свою значимость как на Северо-Западе, так и в масштабах всей страны. Организуемая под эгидой Санкт-Петербургского политехнического университета Петра Великого, конференция традиционно объединяет фундаментальную науку и прикладные решения, предлагая профессиональному сообществу обсудить самые острые вопросы отрасли. Особенность конференции – диалог между учеными, разработчиками и отраслевыми экспертами, позволяющий находить решения для самых сложных вызовов современной кибербезопасности. Каждый год в работе конференции участвуют также регуляторы отрасли, обеспечивая площадку для прямой коммуникации.

Ключевыми темами круглых столов и дискуссий на «МиТСОБИ 2025» стали информационные войны (противодействие кибератакам, дезинформации и цифровым угрозам национальной безопасности), технологический суверенитет, искусственный интеллект, цифровая криминалистика и новые квантовые угрозы безопасности.

Приветствуя участников конференции, председатель Организационного комитета Конференции, чл.-корр. РАН, директор Института компьютерных наук и кибербезопасности Санкт-Петербургского политехнического университета Петра Великого *Дмитрий Петрович Зегжда* подчеркнул возрастающую преемственность среди участников МиТСОБИ: *«В зале я вижу множество знакомых лиц. Некоторые из вас участвуют в нашей конференции десятилетиями, буквально с первых ее дней. Среди спикеров всё больше ученых, некогда приезжавших на секцию для молодых специалистов – сегодня эти исследователи стали полноценными участниками профессионального диалога и выступают здесь теперь в качестве лидеров отрасли. Такая преданность профессиональному диалогу не может не вдохновлять. Мы вместе создаем по-настоящему значимую площадку для решения ключевых вопросов информационной безопасности».* Конференция МиТСОБИ проводится с 1991 г. В ее специальной секции участвуют молодые ученые.

Конференцию поддерживает Правительство Санкт-Петербурга, Министерство обороны РФ, ФСБ, ФСО и другие государственные структуры. В этом году в рамках конференции впервые прошел Ночной турнир соревнования по кибербезопасности NeoQUEST. Финалисты CTF прошлых лет сразились друг с другом, решая задания по веб, реверсу, ИИ и осинту. Победителем Ночного турнира стал Владимир Ситнов (Новосибирск). Второе и третье место заняли Роман Лебедев (Новосибирск) и Эридан Доморацкий (Санкт-Петербург).

Автор представил доклад в научной секции 4 «Современные технологии кибербезопасности», которую вели Жуков И.Ю. (д.т.н., профессор, НИЯУ МИФИ, Руководитель Департамента разработок ООО «Группа компаний «Инфотактика») и Овасапян Т.Д. (к.т.н., доцент, Санкт-Петербургский политехнический университет Петра Великого), посвященный текущему состоянию разработки модели угроз для доверенных интегральных микросхем на основе подходов, традиционно применяемых для формирования специальных требований к средствам защиты информации – на основе модели нарушителя и модели эксплуатации.

Далее приведены тезисы доклада – **«Подход к формированию модели угроз доверенных интегральных микросхем для доверенных программно-аппаратных комплексов» (Кессаринский Л.Н., Сидорин Ю.Ю., Никифоров А.Ю., Дураковский А.П.)**

В основе формирования модели эксплуатации и модели нарушителя лежит информация о комплектуемом доверенном программно-аппаратном комплексе (ДПАК) – либо уже определенном на этапе утверждения технического задания на разработку микросхемы, либо предполагаемом в качестве потенциальной целевой аппаратуры для нее. ДПАК в свою очередь «наследуют» требования от объекта критической информационной (и не только информационной) инфраструктуры (ОКИИ), которые представляют собой в системе терминологии радиоэлектронщиков – системы (автоматизированного управления [технологическим процессом], информационно-телекоммуникационную или информационную). ОКИИ могут быть 4 категорий значимости (1, 2, 3 и без категории), для которых формируется модель нарушителя на основе возможного ущерба от отказа/сбоя. Перечни типовых значимых (т.е. 1–3 категорий) ОКИИ в 2024 г. опубликовали практически все федеральные органы исполнительной власти (ФОИВ) и госкорпорации (ГК), ответственные за переход на ДПАК в своих сферах КИИ.

Возможны два алгоритма формирования исходной информации для модели эксплуатации и модели угроз доверенных микросхем:

а) «сверху вниз»: (1) для категорированного ОКИИ проводится декомпозиция на ДПАК, из которых он состоит, с требованием обеспечения мер защиты от типовой модели нарушителя и эксплуатации; (2) требования ДПАК разбиваются на те, которые реализуются на уровне самого ДПАК (например, на уровне системного или прикладного ПО) и на те, которые необходимо обеспечить на уровне электронной компонентной базы (ЭКБ); (3) требования к ЭКБ переносятся в ТЗ на доверенную микросхему, предназначенную для комплектования такого рода ДПАК, который в свою очередь реализует функционал такой категории систем ЗОКИИ.

б) «снизу вверх»: (1) при формировании ТЗ (внешнего или внутреннего) предполагается для какого типа ДПАК возможно применять разрабатываемую микросхему, в т.ч. на основе маркетингового анализа регулируемого рынка электроники,

оценки собственных возможностей разработчика по реализации требований, возможности переноса ряда требований от реализации с уровня ДПАК на уровень ЭКБ; (2) применение разработанных доверенных микросхем в ДПАК с экономией усилий на реализации ряда требований, поскольку они уже обеспечиваются характеристиками ЭКБ; (3) сертификация ДПАК для применения в составе систем ОКИИ определенной категории.

Понятно, что на практике чаще всего реализуется смешанный алгоритм на основе тесного взаимодействия разработчиков ЭКБ, ДПАК, интеграторов ОКИИ и регуляторов своей сферы КИИ.

Набор требований к доверенным микросхемам определяется совокупностью документов: (1) Общие технические условия на доверенные интегральные микросхемы (стандарт в стадии разработки в ТК 167) + (2) дополнительные специфические требования класса интегральных микросхем (для микропроцессоров, для памяти, для АЦП/ЦАП и т.д.) + (3) специальные требования регулятора сферы КИИ (автомобильной электроники, АСУ ТП для нефтегазовой отрасли, требования РЖД и т.д.) + (4) частное техническое задание или технические условия на конкретную микросхему.

В докладе приведен пример реализации описанного алгоритма для формирования модели угроз для микросхемы, предназначенной для модуля аналогового ввода/вывода программируемого логического контроллера автоматизированной системы управления установкой атмосферной перегонки нефти.

Подводя итог участию в конференции «МиТСОБИ 2025» хочется отметить удачный формат мероприятия, особенно в программной части: разнообразие секций по разным аспектам обеспечения безопасности информации – от организационных до психологических, от кибербезопасности с применением технологии искусственного интеллекта до разбора надежности автоматизированных систем банковских транзакций.

Автор выражает благодарность за приглашение на конференцию оргкомитету МиТСОБИ и лично Д.П. Зегжде.

Леонид Н. Кессаринский, к.т.н.,
руководитель Рабочей группы «Доверенные интегральные схемы» ТК 167
и Экспертно-аналитической группы по вопросам обеспечения доверенности электроники,
доцент НИЯУМИФИ
Каширское ш., 31, Москва, 115409, Россия
e-mail: LNKessarinskiy@mephi.ru, https://orcid.org/0000-0001-7756-6166