КОЛОНКА ГЛАВНОГО РЕДАКТОРА

Здравствуйте, уважаемые читатели и авторы журнала «Безопасность информационных технологий»!

Не успели мы встретить Новый 2024 год – а уже и весна пришла, а с ней и первый номер журнала в год его тридцатилетия! Поздравляю читателей, авторов, редакционный совет и редакционную коллегию журнала БИТ с этой юбилейной датой, думаю, никто не станет утверждать, что в нашем динамичном мире 30 лет для узкоспециализированного научно-технического журнала – это не срок 😊.

На отечественном нормативном фронте по тематике журнала в этот период наблюдалось затишье и интенсивная работа ФОИВ и госкорпораций по инвентаризации и категорированию принадлежащих им значимых объектов КИИ. Так, госорганы, госкорпорации и ЦБ, перечисленные в Постановлении Правительства № 1912 ответственными в своих сферах за переход субъектов КИИ на доверенные ПАК (ДПАК), должны по согласованию со ФСТЭК России сформировать перечни типовых отраслевых объектов КИИ, включающих в себя типы систем и выполняемых ими функций. По принятым ранее решениям и дорожным картам сроки составления календарных планов перехода на ДПАК приближаются, поэтому от наблюдения за ситуацией ведомства втягиваются в практическое исполнение принятых решений.

Частным на фоне глобальных событий в стране и в мире, но важным для аудитории нашего журнала итогом прошлого 2023 года явилось утверждение Росстандартом трех предварительных национальных стандартов (ПНСТ), разработанных ТК 167. Мне особенно близок один из этих стандартов: **ПНСТ 911-2024 «Критическая информационная инфраструктура. Доверенные интегральные схемы и электронные модули. Общие положения»**, разработанный рабочей группой «Доверенные интегральные схемы» (РГ «ДИС») ТК 167 и утвержденный приказом от 21 февраля 2024 г. № 9-пнст с датой введения в действие 1 апреля 😊 2024 г. и сроком действия до 1 апреля 2027 г. Искренне поздравляю с почином руководителя РГ «ДИС», постоянного автора и члена редколлегии нашего журнала – Кессаринского Л.Н., всех наших коллег – членов РГ «ДИС» и экспертно-аналитической группы в ее составе. Основные предпосылки, идеи и положения ПНСТ представлены в материале «ПНСТ 911-2024 «Инфраструктура критическая информационная. Доверенные интегральные микросхемы и электронные модули. Общие положения» в вопросах и ответах» в рубрике «СОБЫТИЯ И МНЕНИЯ» данного номера БИТ. Важно отметить, что в течение указанного трехлетнего срока апробации и применения ПНСТ необходимо преобразовать в ГОСТ Р.

В планах РГ «ДИС» ТК167 на 2024 год разработка четырех ПНСТ (названия могут быть уточнены):

– «Критическая информационная инфраструктура. Доверенные интегральные схемы. Общие технические условия»;

– «Критическая информационная инфраструктура. Доверенные интегральные схемы. Угрозы процессам стадий жизненного цикла»;

– «Критическая информационная инфраструктура. Доверенные интегральные схемы. Требования к проектированию и разработке»;

– «Критическая информационная инфраструктура. Доверенные интегральные схемы. Требования к производству».

Наиболее серьезным и сложным вызовом является задача разработки ОТУ на ДИС, которые по сути являются основным законом, регулирующим порядок взаимоотношений между участниками жизненного цикла ДИС (в том числе наиболее важное – между

производителями и потребителями). В настоящее время действуют два варианта ОТУ на ИС:

- ОСТ В 11.0998-98 – на микросхемы для оборонной продукции;
- ГОСТ 18725-83 – на микросхемы для гражданской продукции.

Оба стандарта в настоящее время устарели, ориентированы на объединение всех стадий жизненного цикла ИС от проектирования до поставки в рамках единого юридического лица (что не характерно для современных ИС, создаваемых в условиях контрактных разработки и изготовления) и вообще не учитывают требования безопасности (информационной, функциональной, технологической).

Современная проблемная ситуация убедительно свидетельствует, что в настоящее время мы существуем и в ближайшее обозримое время будем существовать в условиях «гибридной войны» (или «гибридного мира», как угодно), а развитые государства запустили и активно расширяют программы «приземления» микроэлектронной промышленности, снижения зависимости от мировой кооперации критических технологий и обеспечения технологического суверенитета КИИ. Причём именно цифровая инфраструктура во всех областях нашей жизнедеятельности является наиболее уязвимой для поражения разными видами дестабилизирующих воздействий – внешних и внутренних, природных и антропогенных.

По оценкам до 90% всей ЭКБ обслуживает критическую гражданскую инфраструктуру нашей жизнедеятельности, для которой важными и критичными являются требования **доверенности – совокупности качества (включая надежность и стойкость в режимах и условиях эксплуатации) и безопасности (информационной, функциональной и технологической)**.

Значительная часть программно-аппаратных комплексов объектов критической гражданской инфраструктуры не относится ни к средствам защиты информации (СЗИ), ни к средствам криптографической защиты информации (СКЗИ), ни к значимым объектам КИИ и, таким образом, не подпадает под требования соответствующих регуляторов. Вместе с тем, задание и выполнение требований доверенности через прослеживаемость стадий жизненного цикла с регламентированной возможностью парирования рисков от использования априори недоверенных стадий (например, в условиях контрактного производства изделий на иностранной фабрике) по результатам дополнительных испытаний и входного контроля позволят обеспечить потребителя в ИС с приемлемым и документированным уровнем доверенности.

Создаётся ощущение, что с учётом растущей степени интеллекта всего спектра электронных систем современной гражданской инфраструктуры, доля изделий микроэлектроники без требований доверенности будет неуклонно снижаться, так как любой гаджет, игрушка, выключатель или бытовой прибор в системе интернета вещей потенциально обладает значимой уязвимостью и может нанести ущерб инфраструктуре жизнедеятельности.

Поэтому требования доверенности в ОТУ на ИС целесообразно вводить в качестве дополнительных практически для всей гражданской электроники за редким исключением. Возможно, что на этом пути придётся активно преодолевать инерцию и недопонимание со стороны всё тех же профильных ФОИВ и госкорпораций, если согласование требований доверенности к ИС в их кабинетах будет проходить в привычном для мирной жизни темпе.

Совершенно очевидно, что базовые требования ОТУ применительно к ДИС будут учитывать лишь унифицированные угрозы процессам и стадиям жизненного цикла, и могут потребоваться дополнительные нормативные документы, регламентирующие более конкретные требования, исходя из областей применения ИС. Например, уже сейчас

действуют нормативные документы на ИС для автоэлектроники, авионики, космической техники, оборонных систем, которые потенциально будут дополнять требования и положения будущих ОТУ на ДИС и действовать с ними в комплексе. Очевидно также, что это окажет непосредственное влияние и на отраслевые технологические процессы разработки, производства и испытаний ИС с заданными требованиями доверенности.

Новый стандарт по угрозам доверенности ставит задачу распространить очень эффективный и отлично зарекомендовавший себя нормативный подход ФСТЭК России не только на аспекты обеспечения информационной безопасности в ЭКБ (как состояния её защищённости к воздействию компьютерных атак), но и на все аспекты обеспечения качества и безопасности на стадиях жизненного цикла ИС.

Наконец, два стандарта по требованиям к проектированию и разработке (1) и производству (2) ДИС будут регламентировать основные пути противодействия типовым угрозам процессам на указанных стадиях жизненного цикла изделий, актуализируя и расширяя на аспекты безопасности действующие, но также устаревшие стандарты ОСТ 11 0999 «Микросхемы интегральные. Обеспечение качества в процессе разработки. Требования к системе качества разработки» и ОСТ 11 20.9926 «Микросхемы интегральные. Требования к элементам производства. Сертификация системы качества и производств».

Приглашаю всех заинтересованных читателей принять участие в разработке и обсуждении заявленных предварительных национальных стандартов на ДИС.

В рассматриваемый период состоялось две крупные конференции по вопросам информационной безопасности. В феврале в г. Москве традиционно прошёл Форум «Технологии безопасности» (ТБ Форум), в рамках которого на конференции «Актуальные вопросы защиты информации» представители ФСТЭК России традиционно анонсируют свою техническо-правовую политику на ближайшее время. Буквально следом в ТУСУР (г. Томск) состоялся Форум «Cyber V - 2024». Личные впечатления участника обоих мероприятий Кессаринского Л.Н. – в рубрике «СОБЫТИЯ И МНЕНИЯ».

Продолжаем движение! До скорой встречи на страницах журнала «БИТ»!

Искренне ваш,

Главный редактор Александр Ю. Никифоров
доктор технических наук, профессор
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия

Editor in chief Alexander Yu. Nikiforov
Doctor of Technical Sciences, Professor
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe sh., 31, Moscow, 115409, Russia
e-mail: aynik@spels.ru, https://orcid.org/0000-0002-2427-663X