КОЛОНКА ГЛАВНОГО РЕДАКТОРА

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

Пишу эти строки погожим летним днем, а читать их вы будете уже прохладной осенью!

Этот летне-отпускной период не порадовал нас новыми нормативными документами по тематике журнала.

Вместе с тем, опубликован для обсуждения проект «Стратегии развития отрасли связи Российской Федерации на период до 2035 года», разработанной Минцифры России (далее – Стратегия). С этим документом я ознакомился с большим интересом и вам рекомендую, хотя перед глазами так и стоит другая подобная стратегия – развития электронной промышленности РФ на период до 2030 года (распоряжение от 17.01.2020 №20-р) – первый документ, подписанный главой правительства после его назначения на должность. Вот уже полтора года как события пошли по траектории, мягко говоря, ничего общего не имеющей со стратегией, но документ действует без изменений. Тем не менее, представленная Стратегия представляет большой интерес, как минимум, для расширения кругозора.

Почти шестидесятистраничный документ содержит многочисленные статистические данные и описания состояния отрасли связи в России и в мире, анализ тенденций развития связи и вызовов, которые стоят перед Россией. Описаны задачи отрасли и основные индикаторы, которые планируется достичь. Далее представлен не претендующий на системность и полноту реферат некоторых тезисов, имеющих прямое отношение к тематике журнала.

Необходимость повышения уровня технологического суверенитета в отрасли связи с одновременным поддержанием функционирования инфраструктуры связи и высокого уровня качества и доступности предоставляемых услуг связи – требуют пересмотра подходов к использованию телекоммуникационного оборудования (ТКО) зарубежного производства вне зависимости от оказываемого извне санкционного давления и на основе следующего:

– введение в законодательство Российской Федерации категории «**доверенного ТКО**» – ТКО, соответствующее установленным уполномоченными органами требованиям по безопасности информации, работающее в строгом соответствии с декларированным функционалом и исключающее выполнение недекларированных возможностей, свойства которого подтверждены в соответствии с требованиями Федерального закона от 27.12.2002 № 184-ФЗ «О техническом регулировании»;

– утверждение критериев и методики отнесения ТКО к категории «доверенного ТКО», которые позволят дифференцированно использовать различные классы/категории ТКО для решения различных задач в сетях связи;

– определение органов или организаций, уполномоченных осуществлять отнесение ТКО к категории «доверенного ТКО»;

– допустимость использования в Единой сети электросвязи Российской Федерации ТКО зарубежного производства, отнесённого к категории доверенного ТКО;

– переход на использование в сетях связи ТКО только отечественного производства возможен в случаях, когда на российском рынке представлена отечественная

конкурентоспособная продукция, способная заменить ТКО зарубежного производства без ухудшения качества предоставляемых услуг связи;

– необходимость категоризации объектов инфраструктуры связи в части отнесения их к объектам критической информационной инфраструктуры в соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Разработка и утверждение планов перехода операторов связи на использование доверенного ТКО на объектах критической информационной инфраструктуры. Установленные такими планами сроки перехода должны учитывать объективное наличие на российском рынке доверенного ТКО, а также планы производителей ТКО по созданию и выводу на рынок соответствующих решений.

В области развития технологического обеспечения в отрасли связи в Российской Федерации существуют следующие основные вызовы:

– высокая степень зависимости отечественных сетей связи от иностранного телекоммуникационного оборудования и программного обеспечения, поставленного в том числе из недружественных стран,

– в ситуации объективного отставания отечественной научно-технологической и производственной базы в данной сфере;

– введение недружественными государствами ограничений на доступ к современным технологиям с целью подрыва технологических возможностей Российской Федерации;

– ограниченность финансовых и кадровых ресурсов, а также технологических компетенций, необходимых для реализации масштабных инфраструктурных и научно-исследовательских проектов импортозамещения.

Рост производительности и пропускной способности ТКО приводит к усложнению алгоритмов обработки данных и миграции их реализации **из программной в аппаратную часть**.

Одним из способов обеспечения информационной безопасности в сетях электросвязи является применение криптографических методов защиты информации. Несмотря на достигнутые успехи в разработке отечественных криптографических механизмов, предназначенных для защиты информации в сетях электросвязи, а также на придание им официального статуса документов национальной системы стандартизации, их практическое внедрение зачастую ограничивается государственными информационными системами. Существенным фактором, препятствующим широкому внедрению российской криптографии, является то, что отечественные стандарты криптографии не представлены в международных стандартах телекоммуникационных протоколов.

В области обеспечения информационной безопасности в отрасли связи в Российской Федерации существуют следующие основные вызовы:

– неуклонный рост во всём мире значимости угроз информационной безопасности и ущерба от их реализации в сетях связи на фоне совершенствования методов, способов и технологий осуществления компьютерных атак;

– сохранение рычагов контроля над сетью «Интернет» в руках узкой группы государств в ущерб безопасности других стран.

КОЛОНКА ГЛАВНОГО РЕДАКТОРА

Обеспечение кибербезопасности инфраструктуры связи Российской Федерации включает в себя:

– поэтапный переход на доверенные решения (в том числе операционные системы), соответствующие национальным требованиям по информационной безопасности и сертифицированные ФСТЭК России и/или ФСБ России;

– введение норм использования в отрасли связи программного обеспечения, созданного в соответствии со стандартом безопасной разработки и соответствующего требованиям по информационной безопасности;

– установление требований по проведению непрерывной оценки защищенности предприятий и организаций отрасли связи;

– создание юридически значимых механизмов оценки последствий компьютерных инцидентов, вызванных компьютерными атаками, и проработка условий для развития системы страхования рисков информационной безопасности в отрасли связи, не ухудшающей уровень её информационной безопасности.

Первый этап Стратегии (2023–2030 гг.) включает:

– разработку и внедрение на сетях связи отечественного оборудования стандарта LTE;

– завершение использования технологии 3G с высвобождением радиочастотного спектра для современных технологий;

– разработку и опытную эксплуатацию отечественного оборудования стандартов 5G и 6G-Ready, а также внедрение практики совместного использования опорной инфраструктуры операторами мобильной связи для развёртывания сетей 5G, а к 2035 г. – и 6G;

– нормативное закрепление основных принципов дальнейшего развития сетей 4G и 5G в Российской Федерации: использование диапазона радиочастот 4800–4990 МГц (с потенциалом расширения до 4400–4990 МГц) в качестве основного для создания сетей мобильной связи 5G; использование отечественных СКЗИ для защиты сетей связи; использование российского ТКО, включённого в единый реестр российской радиоэлектронной продукции;

– создание отечественной низкоорбитальной спутниковой группировки, позволяющей обеспечить широкополосный доступ к Интернету в отдельных регионах России, а также передачу сообщений с мобильного телефона в адрес экстренных служб – на территориях с отсутствующим или недостаточным покрытием сетями сотовой связи;

– первую очередь обновления российской национальной группировки космических аппаратов связи и вещания на геостационарной орбите с применением отечественного оборудования;

– организация разработки и производства отечественной ЭКБ, требуемой для создания абонентских терминалов сетей мобильной связи 4G/LTE и 5G, а также налаживание серийного выпуска данных терминалов, в том числе с использованием опыта стран-партнеров Российской Федерации;

– разработка и внедрение сквозных систем и метрик оценки качества функционирования сетей связи и Рунета и их защищенности от реализации недопустимых событий;

– перевод всей отечественной критической информационной инфраструктуры на доверенные отечественные решения (в том числе, отечественные операционные системы);

– расширение взаимодействия научных организаций с участниками отрасли связи, разработчиками ТКО, программного обеспечения и средств защиты информации, в том числе криптографических;

– поэтапное замещение иностранных средств защиты информации, в том числе криптографических, на доверенные средства, сертифицированных в соответствии с законодательством Российской Федерации;

– внедрение систем фильтрации компьютерных атак в сетевом трафике при оказании услуг связи, в том числе использующих технологии искусственного интеллекта;

– развитие отраслевого центра государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая систему раннего предупреждения об угрозах информационной безопасности;

– внедрение технологии квантового распределения ключа на основе отечественного оборудования в интересах государственных и крупных корпоративных потребителей, а также апробация и внедрение пост-квантовых методов криптографической защиты информации в сетях связи;

– продвижение положений национальных стандартов Российской Федерации в международные и межгосударственные стандарты для их последующего применения на абонентских устройствах.

Предусматривается более быстрое достижение технологического суверенитета отрасли связи за счет частных и бюджетных инвестиций в разработку и производство отечественного телекоммуникационного оборудования, включая ЭКБ для него.

Организацию мониторинга и контроль за реализацией Стратегии осуществляет Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации.

Далее. Из информационных событий в летний период можно отметить лишь проведение X Международного военно-технического Форума «АРМИЯ-2023», отчет о работе на котором представлен Усачевым Н.А. в рубрике «Есть мнение!».

Разработка проектов новых предварительных национальных стандартов в области обеспечения Критической информационной инфраструктуры в авральном режиме проведена профильными рабочими группами технического комитета по стандартизации ТК167. Разработаны, опубликованы на сайте Росстандарта и представлены на общественное обсуждение проекты следующих ПНСТ:

– «Инфраструктура критическая информационная. Термины и определения»;

– «Инфраструктура критическая информационная. Доверенные программно-аппаратные комплексы. Общие положения»;

– «Инфраструктура критическая информационная. Доверенные интегральные микросхемы и электронные модули. Общие положения».

Приглашаем всех заинтересованных специалистов пронять участие в обсуждении проектов указанных стандартов на специальном заседании Предконференции №1 «Доверенная и экстремальная электроника» Российского Форума «Микроэлектроника

2023» 21 сентября 2023 г. (Предконференция пройдет с 18 по 21 сентября 2023 г.) в Москве. Программа и регистрация на сайте Форума.

Российский форум «Микроэлектроника 2023» состоится в период с 9 по 14 октября 2023 г. в Парке науки и искусства ФТ «Сириус» (Краснодарский край). Форум «Микроэлектроника» проводится с 2015 г. и зарекомендовал себя как основная российская коммуникационная площадка по широкому кругу вопросов стратегии научно-технологического развития микро- и радиоэлектронной отрасли, создания и применения электронной компонентной базы и программно-аппаратных комплексов, реализации стратегических научно-технических, промышленных и инновационных проектов, нормативно-правовой базы и стандартизации, создания цифровой экономики и обеспечения безопасности и технологического суверенитета страны (информация приведена на сайте https://microelectronica.pro/). Оператором Форума с 2016 г. является ООО «Проконф». В 2022 г. в Форуме приняли участие 1710 делегатов из 665 производственных предприятий, научных учреждений, ВУЗов, дизайн-центров, коммерческих структур.

В этом году уже 9-й по счету Форум «Микроэлектроника 2023» пройдет в очно-заочном формате с использованием новейших цифровых технологий. Форум включает две предконференции (в сентябре в Москве), пленарные заседания, научную конференцию, выставку, деловую программу и школу молодых ученых. Условия участия представителей высшей школы в Форуме традиционно являются льготными.

Пленарное заседание «Доверенные электронные системы и ПАК для критической гражданской инфраструктуры» состоится в первый день работы Форума – 10 октября 2023 г. с 15.00 до 18.30. Ожидаются выступления представителей ГК «Росатом» (А.Б. Шевченко), Росстандарт (А.П. Шалаев), ОАО «РЖД» (А.В. Глейм), ПАО «Сбербанк» (К.Р. Карапетян), НИЯУ МИФИ (В.И. Шевченко), СПбГПИ (Д.П. Зегжда), АО «НИИМА «Прогресс» (З.К. Кондрашов).

Также в Программе Форума предусмотрен трек обзорно-дискуссионных заседаний «Доверенные ЭКБ и РЭУ для критической гражданской инфраструктуры», который пройдет с 11 по 13 октября 2023 г. Координатором подготовки и модератором пленарного заседания и трека обзорно-дискуссионных заседаний по доверенности РЭУ и ЭКБ является Ваш покорный слуга. Наш журнал уже традиционно является доверенным информационным партнером Форума. От души приглашаю Вас зарегистрироваться и участвовать в работе Форума!

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