КОЛОНКА ГЛАВНОГО РЕДАКТОРА

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

Глазом моргнуть не успели – вот уже и лето, считай, половина 2024 г. осталось в прошлом.

Наиболее заметным событием в нашей предметной области за этот квартал было утверждение ФСТЭК России 02.05.2024 «Методики оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (далее – Методика). Предлагаю краткий реферат Методики, не претендующий на точность и полноту.

Методика определяет показатель, характеризующий текущее состояние технической защиты информации, не составляющей государственную тайну, и/или обеспечения безопасности значимых объектов критической информационной инфраструктуры (КИИ), его нормированное значение, а также порядок его расчета. Методика применяется для оценки состояния защиты информации (обеспечения безопасности объектов КИИ) в государственных и муниципальных органах, организациях, в том числе субъектах КИИ, и степени его соответствия минимально необходимому уровню защиты информации (безопасности объектов КИИ) от типовых актуальных угроз безопасности информации. В качестве минимально необходимого уровня задан состав мер, реализация которых предусмотрена нормативными правовыми актами государства, и который минимально достаточен для блокирования (нейтрализации) типовых актуальных угроз безопасности информации. При этом несоответствие значения указанного показателя установленному нормированному значению указывает на наличие в органе (организации) возможности реализации актуальных угроз безопасности информации или предпосылок для их реализации.

Методика применяется ФСТЭК России – для мониторинга текущего состояния защиты информации и/или обеспечения безопасности объектов КИИ, а также органом (организацией) – для оценки текущего состояния защиты информации и/или обеспечения безопасности объектов КИИ, разработке мер по повышению уровня защищенности и оценки эффективности деятельности соответствующих должностных лиц.

В качестве показателя, характеризующего состояние защиты информации (обеспечения безопасности объектов КИИ), в органе (организации) принят показатель текущего состояния защищенности Кзи, который характеризует степень достижения минимально необходимого уровня защиты информации (обеспечения безопасности объектов КИИ) от типовых актуальных угроз безопасности информации во временном интервале оценивания и заданных условиях эксплуатации информационных систем управления, информационно-телекоммуникационных сетей, иных объектов информатизации (далее – информационные системы). При минимально необходимом уровне защищенности Кзи = 1. Полученное значение Кзи является критерием необходимости принятия управленческих решений по реализации первоочередных мер по защите информации (обеспечению безопасности объектов КИИ) от актуальных угроз безопасности информации и их приоритетности.

Оценка Кзи включает: (а) сбор и анализ исходных данных, (б) оценку значений частных показателей безопасности и (в) расчет значения показателя Кзи и его сравнение с нормированным значением. Оценка Кзи проводится не реже одного раза в шесть месяцев. Периодичность и порядок оценки устанавливаются органом (организацией) во внутренних регламентах.

Указанная оценка может проводиться на основе результатов внутреннего контроля или внешней оценки соответствия (аудита безопасности), мониторинга информационной безопасности, оценки защищенности и/или аттестации информационных систем, иных

мероприятий по изучению и контролю уровня защищенности информации. О полученном по результатам расчета значении показателя Кзи, не соответствующем нормированному значению, информируется руководитель органа (организации) для принятия мер по защите информации. Также материалы и результаты оценки Кзи предоставляются в ФСТЭК России по ее запросу в целях оценки текущего состояния защиты информации и обеспечения безопасности объектов КИИ. ФСТЭК России может уточнить значение Кзи по результатам анализа представленных материалов. Внеочередная оценка Кзи проводится в случаях: (а) возникновения значимого инцидента информационной безопасности, (б) развития (изменения) архитектуры информационных систем, (в) запроса руководителя органа (организации) и (г) запроса ФСТЭК России.

В качестве исходных данных для оценки Кзи перечислены акты, протоколы, отчеты по результатам контроля и оценки уровня защищенности информации, организационно-распорядительные документы, эксплуатационная документация, результаты инвентаризации информационных систем, результаты опросов работников, результаты анализа функционирования программно-аппаратных средств информационных систем и мониторинга информационной безопасности. Перечислены основные компетенции специалистов, привлекаемых для сбора и анализа исходных данных. Установлены типовые мероприятия, проводимые указанными специалистами по сбору и анализу исходных данных в структурных подразделениях органа (организации). По результатам анализа определяются значения частных показателей безопасности, формируются выводы о реализации мероприятий (процессов) и достаточности мер по защите информации и обеспечению безопасности объектов КИИ.

В Методике представлена таблица с перечнем используемых частных показателей безопасности, их наименованиями и максимальными значениями. Если по результатам проведенного анализа сделаны выводы, что меры по защите информации реализованы, соответствующему частному показателю присваивается установленное максимальное значение, в противном случае – нулевое. Далее установлены порядок расчета значения Кзи и типовые варианты выводов о текущем состоянии защиты информации (обеспечения безопасности объектов КИИ) в органе (организации) в зависимости от полученного значения Кзи.

В случае если по результатам расчета получено значение Кзи, характеризующее состояние защищенности как низкое или критическое, разрабатывается план реализации мероприятий по достижению следующего уровня защиты от актуальных угроз в сроки до проведения следующей плановой оценки показателя Кзи.

В целом, очевидно, что ФСТЭК России в соответствие с расширением своего функционала предприняла конкретные шаги по практической организации системы мониторинга текущего состоянии защиты информации и обеспечения безопасности объектов КИИ.

Рабочая группа «Доверенные ИС» (РГ «ДИС») ТК 167 продолжает интенсивную работу над проектами предварительных национальных стандартов (ПНСТ) на доверенные ЭКБ для ПАК объектов КИИ, сконцентрировав основные усилия на разработке Общих технических условий (ОТУ) на Микросхемы интегральные. Принципиальным отличием данного проекта ОТУ от всех предыдущих является задание требований не только к изделиям данного класса однородной продукции, но также к процессам стадий их жизненного цикла (начиная с разработки и производства), а также к их участникам. При этом основной акцент сделан на перспективные программно-управляемые цифровые СБИС, создаваемые по субмикронным проектным нормам в условиях современных контрактных производств, т.к. именно этот класс изделий микроэлектроники является наиболее массовым и критичным для создания доверенных ПАК объектов КИИ.

КОЛОНКА ГЛАВНОГО РЕДАКТОРА

Многие из отмеченных подходов могут являться избыточными для простых ИС с проектными нормами 0,35 мкм и выше, создаваемых на «традиционных», в основном, оборонных, предприятиях полного цикла, но доля их гражданской продукции в ПАК объектов КИИ не является преобладающей и критичной. Также не всегда учтены особенности других специфичных классов ИС (аналоговых, преобразователей информации, приемо-передающих, оптоэлектронных, полузаказных, …), хотя по возможности будут отмечены общие рекомендации по обеспечению и контролю доверенности перечисленных классов изделий и процессов стадий их жизненного цикла.

К сожалению, «нельзя объять необъятное» – тем более в условиях жесткого цейтнота и инициативного, никем не финансируемого, характера этой работы. Кроме того, предполагается, что у РГ «ДИС» будет еще 3 года на доработку и уточнение ПНСТ на пути их преобразования в ГОСТ.

С целью повышения эффективности и практической востребованности создаваемых проектов ПНСТ в марте с.г. РГ «ДИС» уже второй раз провела выездное заседание «на земле» – на сей раз в г. Воронеже на базе предприятия «ВЗПП-С». Мнение Харченко М.Э. – члена РГ «ДИС» и непосредственного организатора выездного заседания по его итогам – представлено в рубрике «События и мнения». Со своей стороны хотел бы поблагодарить воронежских коллег за гостеприимство и отличную организацию нашей работы.

Среди наиболее эмоциональных вопросов местной аудитории был такой: распространяются ли разрабатываемые стандарты на оборонную ЭКБ. Еще раз хотел бы подчеркнуть: не распространяются, речь идет о гражданской продукции, а оборонная ЭКБ создается и поставляется по комплексу государственных военных стандартов «Климат-8» и соответствующим ОТУ. Созвучно с этим вопросом в рубрике «События и мнения» представлен взгляд д.т.н., профессора Тельца В.А. на то, к какой категории качества следовало бы относить доверенные ИС для КИИ. Следующее выездное заседание РГ «ДИС» намечено на август с.г. в г. Калуга.

Рассматриваемый период был отмечен целым букетом профильных выставок, конференций и заседаний. Личные впечатления непосредственных участников этих мероприятий, членов РГ «ДИС»: Усачева Н.А., Панарской Е.Г., Кессаринского Л.Н., Харченко М.Э. и Покровского И.А. – представлены в рубрике «События и мнения».

И в завершение, еще раз о Российском Форуме «Микроэлектроника 2024»: подготовка идет полным ходом, открыта регистрация участников на сайте Форума. Обзорно-аналитическое заседание с презентацией проблематики Форума состоялось в рамках деловой программы выставки «Экспоэлектроника» в апреле с.г.

До скорой встречи на страницах журнала БИТ и на Форуме «Микроэлектроника 2024»!

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