РАЗВИТИЕ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КИИ

Игорь Тарви

Руководитель направления защиты объектов критической информационной инфраструктуры

АО «ДиалогНаука»

23 апреля 2024 года, Москва

ДиалОгНаука

«Что нового и какие тенденции?» - обзор изменений в сфере КИИ:

- ✓ Новые полномочия ФСТЭК России
- ✓ Ключевые изменения в сфере КИИ в 2024 году

Практический опыт:

- ✓ На что регулятор требует обратить особое внимание при определении объектов КИИ
- ✓ Типовые ошибки субъектов КИИ при категорировании и подачи данных по объектам КИИ
- ✓ Типовые перечни объектов КИИ

Новые полномочия ФСТЭК России

Указом Президента Российской Федерации от 08.11.2023 г. № 846 ФСТЭК России предоставлены новые полномочия:

- ✓ Централизованный учет информационных систем и иных объектов КИИ по отраслям экономики;
- ✓ Мониторинг текущего состояния технической защиты информации и обеспечения безопасности значимых объектов КИИ;
- ✓ Оперативное информирование об угрозах безопасности информации и уязвимостях ИС и иных объектов КИИ;
- ✓ Оперативное доведение мер по технической защите от выявленных угроз и уязвимостей;
- ✓ Организация и проведение оценки эффективности деятельностям ОГВ и организаций по технической защите информации и обеспечению безопасности значимых объектов КИИ.

Методика оценки показателя состояния защиты информации и обеспечения безопасности ОКИИ

ФСТЭК России информирует: информационное сообщение ФСТЭК России от 12.02.2024 № 240/91/688 «О разработке методического документа ФСТЭК России **«Методика оценки показателя состояния защиты информации и обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации».**

Методика оценки показателя состояния защиты информации и обеспечения безопасности ОКИИ

Документом выделены следующие уровни защищенности:

Зеленый – минимальный/базовый, которым обеспечивается минимальный уровень защиты от угроз

Оранжевый – низкий, когда минимальный уровень защиты не обеспечивается, имеются предпосылки реализации угроз.

Красный – критический, когда минимальный уровень защиты не обеспечивается, имеется реальная возможность реализации угроз.

Методика оценки показателя состояния защиты информации и обеспечения безопасности ОКИИ

- ✓ Оценка проводится не реже одного раза в квартал в отношении всех ИС подлежащих защите.
- ✓ Внеочередная оценка проводится в случаях:
  - ➢ возникновения инцидентов ИБ;
  - ➢ изменения архитектуры ИС;
  - ➢ запроса руководителя организации;
  - ➢ по запросу ФСТЭК России.
- ✓ ФСТЭК России проверяет правильность расчета значения уровня показателя в срок не позднее 60 дней со дня получения от организации результатов расчета и направляет соответствующее уведомление либо запрашивает дополнительные сведения.
- ✓ В проекте приведены четыре группы показателей*, каждая из которых содержит свой весовой коэффициент:
  - ➢ организация и управление;
  - ➢ защита пользователей;
  - ➢ защита информационных систем;
  - ➢ мониторинг ИБ и реагирование.

*В каждой группе показателей указаны несколько частных показателей, которые характеризуют степень реализации отдельных мер по обеспечению безопасности от актуальных угроз.

Методика оценки зрелости деятельности в области защиты информации и обеспечения безопасности КИИ РФ

Применяется для оценки деятельности заместителя руководителя органа (организации), на которого возложены полномочия по обеспечению информационной безопасности органа (организации), и (или) структурного подразделения, осуществляющего функции по обеспечению информационной безопасности органа (организации).

Определяет показатели зрелости деятельности государственного органа, органа местного самоуправления, организации, в том числе субъекта КИИ по защите информации, не составляющей государственную тайну, и (или) обеспечению безопасности значимых объектов КИИ, а также порядок расчета показателя зрелости.

Безопасная разработка ПО

ФСТЭК России разработан проект национального стандарта ГОСТ Р 56939 Защита информации. Разработка безопасного программного обеспечения. Общие требования

ГОСТы которые уже введены в действие:

- ✓ ГОСТ Р 71206-2024 «Защита информации. Разработка безопасного программного обеспечения. Безопасный компилятор языков С/С++. Общие требования».
- ✓ ГОСТ Р 71207-2024 «Защита информации. Разработка безопасного программного обеспечения. Статический анализ программного обеспечения. Общие требования».

Порядок сертификации процессов безопасной разработки ПО СрЗИ Официально опубликован приказ ФСТЭК России от 01.12.2023 № 240 «Об утверждении Порядка проведения сертификации процессов безопасной разработки программного обеспечения средств защиты информации».

Порядок вступает в силу с 01.06.2024

Сертификации процессов безопасной разработки ПО СрЗИ

Системы сертификации в РФ

До принятия приказа ФСТЭК России № 240

Сертификация непосредственно самих средств защиты информации:

1. Минобороны России;
2. СВР России;
3. ФСБ России;
4. ФСТЭК России.

После принятия приказа ФСТЭК России № 240

5. Новый вид сертификации – сертификация процессов безопасной разработки программного обеспечения средств защиты информации

Для чего нужен новый вид сертификации?

Приказ ФСТЭК России
№ 240

До принятия

Производители СрЗИ получают сертификат соответствия на свой продукт сроком на 5 лет.
Если в этот период в продукт необходимо внести какие-либо изменения (обновление, новые функции), производитель обязан провести дополнительные испытания сам, либо с привлечением испытательной лаборатории

После принятия

По итогу сертификации своих процессов безопасной разработки ПО СрЗИ, производитель сможет при каждом обновлении продукта не привлекать испытательную лабораторию, а проводить все необходимые испытания самостоятельно, после чего подавать полученные результаты по обновленному продукту в ФСТЭК России

Другие новости от ФСТЭК России на 2024 год

Разработан новый банк данных угроз – **БДУ АСУ ТП**

В планах ФСТЭК России на 2024 год:

- ✓ разработать Требования по обеспечению защищенности ГИС и значимых объектов КИИ РФ от несанкционированных воздействий типа «отказ в обслуживании»;
- ✓ подготовить обновленную методику определения актуальных угроз;
- ✓ будет пересмотрен и выставлен на общественное обсуждение проект методики расчета показателей экономической значимости.

Изменения в 187-ФЗ

В ГосДуму внесен законопроект «О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации», касающиеся уже осуществляемых мероприятий по импортозамещению на ЗОКИИ, категорирования с учетом типовых отраслевых перечней ОКИИ, а также необходимости разработки отраслевых методических документов по категорированию.

К чему готовиться?

Наделение Правительства РФ дополнительными полномочиями по установлению:

- ✓ требований к используемому ПО, ПАК, радиоэлектронному и телекоммуникационному оборудованию на ЗОКИИ, а также порядка и условий возможного использования иностранных составляющих;
- ✓ порядка и сроков перехода субъектов КИИ на отечественное ПО и аппаратную продукцию на ЗОКИИ, а также порядка мониторинга такого перехода.

Дополнения к правилам категорирования, на уровне 187-ФЗ:

- ✓ присвоение субъектами КИИ категории значимости своим объектам не только исходя из порядка, описанного в 127-ПП, но и с учетом методических указаний отраслевых регуляторов;
- ✓ Формирование отраслевыми регуляторами типовых перечни ОКИИ по согласованию с ФСТЭК России;
- ✓ методические указания, регламентирующие особенности категорирования для каждой сферы деятельности, также будут разрабатывать отраслевые регуляторы по согласованию с ФСТЭК России;
- ✓ законодательно закрепляется процесс мониторинга представления субъектами КИИ актуальных и достоверных сведений об имеющихся у них объектах КИИ. Устанавливаются сроки уведомления субъекта КИИ о выявленных неактуальных сведениях, сроки предоставления актуализированных сведений или обоснований об отсутствии необходимости исправления сведений.

К чему готовиться?

Изменения правил мониторинга субъектов КИИ отраслевыми регуляторами:

- ✓ если в процессе мониторинга отраслевым регулятором выявлены недочеты (предоставленные сведения об объектах неполные и (или) неточные), то ФСТЭК России в 30-дневный срок направляет требование субъекту о необходимости корректировки сведений;
- ✓ субъект КИИ обязан в 10-дневный срок исправить сведения и направить их во ФСТЭК России либо обосновать отсутствие необходимости таких исправлений.

Наделение субъектов КИИ новыми обязанностями:

- ✓ соблюдение требований к используемому ПО на ЗОКИИ, описанных выше;
- ✓ обеспечение перехода на преимущественное использование отечественного ПО.

Проект изменений может вступить в силу уже с 1 марта 2025 года.

Обратите внимание!

С 01.09.24 не допускается использование субъектами КИИ в ЗОКИИ ПАК, приобретенных с 01.09.24 и не являющихся доверенными ПАК! Исключение – отсутствие произведенных в России доверенных ПАК, являющихся аналогами. Подтверждением об этом является заключение об отнесении продукции к пром. продукции, не имеющей произведенных в России аналогов, выданное Минпромторгом в соответствии с ПП РФ № 1135 от 20.09.17

- ✓ ПП-1478 устанавливает требования к ПО, используемому на ЗОКИИ, правила перехода на преимущественное использование российского ПО, а также правила согласования закупок иностранного ПО для его использования на ЗОКИИ. Срок до 01.01.25
- ✓ ПП-1912 утверждает порядок и правила перехода на преимущественное использование доверенных ПАК в составе ЗОКИИ, в том числе постановлением определены уполномоченные органы, ответственные за организацию такого перехода. Срок до 01.01.30
- ✓ Требования, сроки и порядок перехода на российское ПО и отечественную аппаратную продукцию на ЗОКИИ, функционирующих в банковской сфере и иных сферах финансового рынка, подлежат согласованию с Центральным банком Федеральным законом от 13.06.2023 № 243-ФЗ.

Большая часть перечней уже готова!

При категорировании объектов КИИ субъекты КИИ обязаны учитывать утвержденные перечни типовых объектов КИИ в рамках своей сферы деятельности, а также следить за актуальностью сведений о принадлежащих им объектах КИИ и предоставлять информацию по запросу государственных органов или юридических лиц. На текущий момент утверждены перечни типовых объектов КИИ для следующих сфер деятельности:

- ✓ банковская сфера и иные сферы финансового рынка;
- ✓ химическая промышленность;
- ✓ топливно-энергетический комплекс;
- ✓ транспорт;
- ✓ энергетика;
- ✓ здравоохранение;
- ✓ горнодобывающая промышленность (в части руд, камней);
- ✓ металлургическая промышленность;
- ✓ оборонная промышленность.

Порядок представления субъектами КИИ из сферы транспорта сведений об объектах КИИ

ФСТЭК России информирует* о порядке представления субъектами КИИ, осуществляющими деятельность в сфере транспорта, перечней объектов КИИ, подлежащих категорированию, а также сведений о присвоении объектам КИИ одной из категорий значимости либо не присвоения им одной из таких категорий.

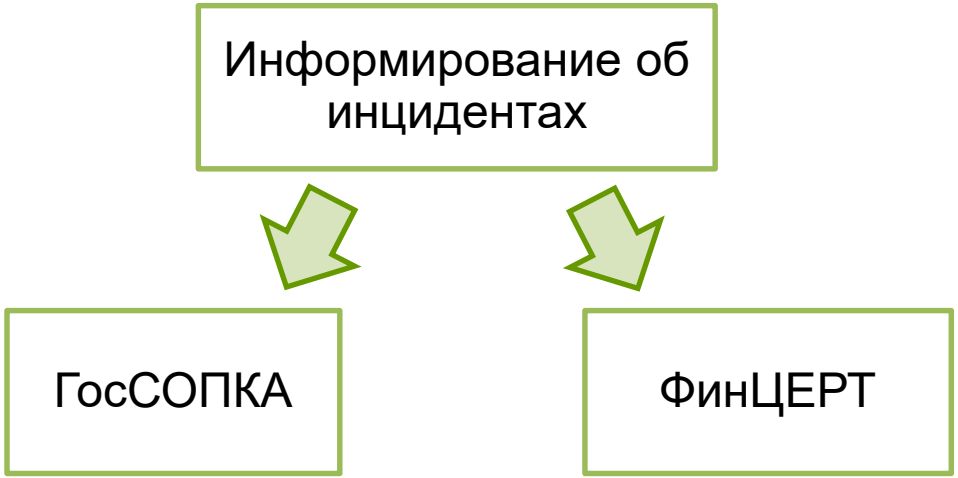
Необходимо направлять указанные выше сведения на рассмотрение:

- ✓ в центральный аппарат ФСТЭК России, если субъект КИИ является федеральным органом исполнительной власти, подведомственным учреждением или организацией, осуществляющей деятельность в двух и более субъектах РФ;
- ✓ в управление ФСТЭК России по федеральному округу для всех остальных субъектов КИИ.

*Источник: Информационное сообщение ФСТЭК России от 06.03.2024 № 240/82/580 «О порядке представления субъектами критической информационной инфраструктуры сведений о результатах присвоения объектам критический информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

Информирование об инцидентах

- ✓ п.5 приказа ФСБ России от 19 июня 2019 г. N 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»
- ✓ Статья 9.2 ФЗ № 187 «О Безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017



Уточняющее пояснение по реагированию на компьютерные инциденты для финансовых организаций

Для субъектов КИИ, владеющих ЗОКИИ, осуществляющих деятельность в банковской и других сферах финансового рынка, присутствуют уточнения в **282 Приказе ФСБ России**, а также **в методических рекомендациях Банка России МР-14 и МР-15**:

- ✓ возможным способом информирования ФСБ России о КИ и результатах мероприятий по реагированию на них является передача соответствующей информации в Банк России с использованием технической инфраструктуры Банка России — Автоматизированной системы обработки инцидентов ФинЦЕРТ Банка России (АСОИ ФинЦЕРТ);
- ✓ для направления и получения информации с помощью АСОИ ФинЦЕРТ рекомендуется направить в Банк России и НКЦКИ информацию о соответствующем согласии, в случае если ранее данные сведения не направлялись.
- ✓ рекомендуется использовать перечень компьютерных инцидентов и компьютерных атак, описанных в стандарте Банка России СТО БР БФБО-1.5-2023.

Обратите внимание!

На что следует обратить внимание при категорировании ОКИИ

- ✓ Обязателен к применению перечень типовых отраслевых объектов КИИ!

На что следует обратить внимание при подаче данных об ОКИИ

- ✓ АРМ администраторов должны включаться в состав ОКИИ!
- ✓ Наличие сопряжения ОКИИ с ЛВС имеющей подключение к Интернет = наличие подключения ОКИИ к Интернет!

Типовые ошибки

Типовые ошибки при категорировании КИИ

- ✓ Рассмотрены не все процессы
- ✓ Рассмотрены не все системы
- ✓ Не учтены филиалы, представительства

Типовые ошибки при подаче данных по объектам КИИ

- ✓ Указаны не все адреса размещения компонентов ОКИИ
- ✓ Не приведены расчеты (обоснование) присвоения/не присвоения категории значимости и полученных значений;
- ✓ Не указаны модели оборудования/версии ПО входящих в состав ОКИИ
- ✓ Незаполненные поля в форме данных по ОКИИ направляемой в ФСТЭК России

Вопросы

Спасибо за внимание!

115230, г. Москва, 1-й Нагатинский проезд, д. 10, стр. 1

Телефон: +7 (495) 980-67-76

Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru

e-mail: itarvi@DialogNauka.ru