USSC

Требования безопасности к разрабатываемому прикладному ПО значимых объектов КИИ (на основании приказа ФСТЭК России № 239 к безопасной разработке, испытаниям и поддержке ПО)

+7 (343) 379-98-34
USSC.RU
info@ussc.ru

USSC

Требования безопасности к разрабатываемому прикладному ПО значимых объектов КИИ (на основании приказа ФСТЭК России № 239 к безопасной разработке, испытаниям и поддержке ПО)

С 1 января 2023 года вступили в силу требования Приказа ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (Приказ ФСТЭК России № 239) к программному обеспечению (ПО), внедряемому в рамках создания, модернизации или ремонта значимого объекта критической информационной инфраструктуры (КИИ):

- требования по безопасной разработке ПО
- требования к испытаниям по выявлению уязвимостей в ПО
- требования к поддержке безопасности ПО

Разработчикам ПО в целях выполнения требований Приказа ФСТЭК России № 239 требуется внедрить в процесс разработки необходимые процедуры безопасности и инструменты по проверке ПО, такие как проверка ПО на наличие недекларированных возможностей и уязвимостей, проверка Open Source компонентов и библиотек на наличие уязвимостей, а также документально подтвердить внедрение данных процедур.

Среди существующих разных подходов к внедрению процессов безопасной разработки ПО, сформулированных в отечественных и зарубежных стандартах, можно выделить разрабатываемую и частично утвержденную серию национальных стандартов ГОСТ Р 56939 «Защита информация. Разработка безопасного программного обеспечения» (далее – серия ГОСТ Р 56939), предназначенных для разработчиков и производителей ПО, а также для организаций, выполняющих оценку соответствия процесса разработки ПО. Серия ГОСТ Р 56939 наиболее полно охватывает требования Приказа ФСТЭК России № 239 к безопасной разработке ПО на всех этапах жизненного цикла ПО.

Настоящий материал сформирован с учетом требований п. 29.3 Приказа ФСТЭК России № 239, основан на стандартах из серии ГОСТ Р 56939 и предназначен для разработчиков ПО и субъектов КИИ, выступающих в разных ролях и взаимодействующих между собой при внедрении процессов безопасной разработки ПО.

Материал содержит:

- Разъяснение требований Приказа ФСТЭК России № 239 к разрабатываемому прикладному ПО значимых объектов КИИ и особенностей реализации процесса безопасной разработки ПО.
- Чек-лист реализации процесса безопасной разработки, основанный на серии ГОСТ Р 56939.
- Лист самоконтроля для субъектов КИИ, позволяющий провести анализ выполнения требований к безопасной разработке ПО внешними организациями, осуществляющими разработку и (или) сопровождение ПО значимых объектов КИИ.
- Лист самоконтроля для субъектов КИИ, позволяющий оценить реализацию требований безопасности к ПО, разрабатываемому для значимых объектов КИИ. В качестве разработчика ПО могут также выступать субъекты КИИ, осуществляющие разработку ПО для собственных объектов КИИ.

НА КАКИЕ ТИПЫ ПО РАСПРОСТРАНЯЮТСЯ ТРЕБОВАНИЯ

Требования по безопасной разработке предъявляются к ПО, которое обеспечивает выполнение критических процессов значимых объектов КИИ, например:

- производственно-технологические системы координации, контроля и управления (SCADA, APS-, MES-, LIMS-системы)
- системы диспетчеризации различных сфер производственной деятельности (топливно-энергетический комплекс, энергетика, транспорт и др.)
- системы автоматизации бизнес-процессов (BPM-системы)
- государственные и муниципальные информационные системы
- системы управления ресурсами предприятия (ERP-, MRP-системы, такие как: 1С: Управление предприятием, 1С: ERP, SAP ERP и др.)
- программные продукты для автоматизированных банковских систем (ЦФТ-Банк, RS-Bank, Diasoft FA и прочие)
- биллинговые системы (FORIS BSS/OSS, Comverse One и прочие)

ТРЕБОВАНИЯ К ПО, ВНЕДРЯЕМОМУ НА ЗНАЧИМЫХ ОБЪЕКТАХ КИИ

Основным нормативным актом, регулирующим требования к ПО, внедряемому на значимых объектах КИИ, является **Приказ ФСТЭК России № 239.**

Для выполнения **требований по безопасной разработке ПО** необходимо:

- определить меры обеспечения по безопасной разработке ПО
- выстроить процесс безопасной разработки ПО
- документировать процесс безопасной разработки ПО
- назначить ответственных лиц за безопасную разработку ПО
- провести анализ угроз ИБ ПО (составить модели угроз)
- описать структуру ПО на уровне подсистем
- сопоставить функции ПО и интерфейсы, описанные в функциональной спецификации, с подсистемами ПО (для ПО, планируемого к применению в значимых объектах 1 категории значимости)

Для выполнения **требований к испытаниям по выявлению уязвимостей в ПО** необходимо регулярно проводить испытания:

- статический анализ исходного кода ПО
- фаззинг-тестирование ПО
- динамический анализ кода ПО (для ПО, применяемого на объектах КИИ 1 категории значимости)

Для выполнения **требований к поддержке безопасности в ПО** должны быть внедрены процедуры:

- отслеживание и исправление обнаруженных ошибок и уязвимостей
- информирование пользователей об уязвимостях ПО, компенсирующих мерах по защите информации или ограничениях по применению ПО, способах получения пользователями обновлений ПО и порядке проверки их целостности и подлинности
  информирование пользователей об окончании производства и (или) поддержки ПО (для ПО, планируемого к применению в значимых объектах 1 категории значимости)

USSC

ЧЕК-ЛИСТ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ К ПО, ВНЕДРЯЕМОМУ НА ЗНАЧИМОМ ОБЪЕКТЕ КИИ И ВЫПОЛНЯЮЩЕМУ ФУНКЦИИ ЗНАЧИМОГО ОБЪЕКТА КИИ ПО НАЗНАЧЕНИЮ

Что нужно сделать?

1. Разработать руководство по безопасной разработке

☐ Провести анализ требований к ПО — определить требования по безопасности ПО.

В качестве источника требований можно использовать Приказ ФСТЭК России № 239, профили защиты ФСТЭК России и отраслевые стандарты.

☐ Регламентировать процесс проектирования архитектуры ПО, в том числе процессы:

- анализа угроз безопасности и разработки модели угроз безопасности информации
- разработки проекта архитектуры ПО
- оценки рисков в отношении процесса разработки ПО

В качестве методического документа для разработки руководства по реализации мер по безопасной разработке ПО можно использовать ГОСТ Р 56939-2016.

☐ Регламентировать процесс написания кода и сборки ПО:

- определить перечень инструментов разработки ПО
- сформировать порядок оформления исходного кода ПО
- определить инструменты и порядок проведения статического анализа и экспертизы исходного кода ПО

☐ Регламентировать процесс квалификационного тестирования ПО — определить инструменты, порядок проведения и ответственных за проведение фаззинг-тестирования и динамического анализа кода ПО.

☐ Регламентировать процессы приемки и инсталляции ПО:

- порядок приемки ПО перед его запуском в продуктивной среде
- порядок передачи ПО в продуктивную среду
- состав и содержание эксплуатационных документов на ПО

☐ Регламентировать процесс эксплуатации ПО:

- назначить ответственных за техническую поддержку пользователей ПО
- сформировать порядок информирования пользователей об обновлениях ПО, обнаруженных уязвимостях и окончании технической поддержки
- назначить ответственных за поиск уязвимостей ПО и их устранение

☐ Регламентировать процесс обеспечения безопасности среды разработки:

- меры защиты от несанкционированного доступа
- резервное копирование
- регистрация изменений и событий безопасности
- реагирование на инциденты ИБ и др

☐ Регламентировать процесс обучения сотрудников — определить порядок и периодичность обучения всех сотрудников, задействованных в процессе разработки ПО.

Рекомендуется проводить обучение не реже одного раза в год.

2. Провести анализ угроз безопасности — выполнить моделирование угроз, которые могут возникнуть вследствие применения ПО, с целью выявления потенциальных угроз безопасности информации и обоснования требований по безопасности:

- [ ] Построить схему информационных потоков ПО.
- [ ] Определить потенциальные угрозы, которые могут возникнуть с учетом информационных потоков и применяемых сервисов.
- [ ] Определить меры нейтрализации угроз.

В качестве источников информации используются:

- *банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru)*
- *публикации проекта Open Web Application Security Project (OWASP)*
- *MITRE ATT&CK Matrix*
- *CWE top 25 и другие источники*

Для определения потенциальных угроз можно использовать методику и средства моделирования угроз STRIDE, OWASP, Agile Threat Modeling Toolkit и другие.
Модель угроз пересматривается при обнаружении новых угроз или изменении архитектуры ПО.

3. Разработать проект архитектуры ПО — разработать документацию:

- [ ] Описать процедуру безопасной инициализации ПО.
- [ ] Описать структуру ПО на уровне подсистем и модулей ПО, назначение подсистем и модулей и их взаимодействия с другими подсистемами и модулями.
- [ ] Описать порядок реализации функций ПО для каждой подсистемы, в том числе и реализации функций безопасности ПО.
- [ ] Описать назначение и способы использования интерфейсов для каждой функции ПО и описание параметров, связанных с каждым интерфейсом.
- [ ] Определить и описать все используемых сторонних компонентов ПО.
- [ ] Описать процедуры периодического пересмотра и актуализации проекта архитектуры ПО в случае выявления новых угроз или изменения требований к ПО.

4. Внедрить регулярную процедуру статического анализа кода — проверку кода на наличие ошибок и уязвимостей без его выполнения.

Преимуществом статического анализа кода является обнаружение уязвимостей и ошибок на ранних стадиях разработки ПО непосредственно при написании кода. Максимальная эффективность этого метода достигается если статический анализатор интегрирован в систему разработки и проводит автоматические проверки.

5. Внедрить регулярную процедуру динамического анализа кода — проверку безопасности кода ПО при его выполнении.

Для проведения динамического анализа из исходного кода должен быть получен исполняемый файл. Динамический анализ выполняется с помощью наборов данных, которые подаются на интерфейсы ПО, поэтому эффективность анализа напрямую зависит от качества и объема входных данных для тестирования.

6. Внедрить регулярную процедуру фаззинг-тестирования — проверку безопасности ПО путем отправки заведомо неверных данных и анализа реакции ПО на них.

Основная цель фаззинг-тестирования — обнаружить непредусмотренные функции, ошибки и нарушения в работе ПО при подаче некорректных данных.

7. Регламентировать отслеживание и исправление обнаруженных ошибок и уязвимостей в ПО:

- [ ] Назначить сотрудников, ответственных за прием сообщений об ошибках и уязвимостях ПО от пользователей.
- [ ] Определить порядок поиска уязвимостей ПО.
- [ ] Определить способы связи для сообщения об ошибках и уязвимостях ПО (электронная почта, форма на сайте, горячая линяя).
- [ ] Определить порядок идентификации и классификации недостатков.
- [ ] Определить процедуры устранения недостатков и выпуска обновлений, в том числе должны быть определены процедуры экстренного устранения недостатков.
- [ ] Определить порядок информирования пользователей о новых обновлениях ПО, обнаруженных уязвимостях или об окончании поддержки ПО.

USSC

ЛИСТ САМОКОНТРОЛЯ ДЛЯ ВЛАДЕЛЬЦЕВ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

Владелец значимого объекта КИИ может осуществлять разработку ПО собственными силами либо передавать функции разработки (сопровождения) ПО внешним организациям.

Разработка (сопровождение) ПО осуществляется силами владельца объектов КИИ

Оцените:

1. Формализован ли процесс безопасной разработки (сопровождения) ПО на уровне требований в вашей организации? Выпишите перечень локальных нормативных актов вашей организации (стандартов, политик, положений), определяющих требования к процессу разработки (сопровождения) ПО. Проверьте, установлены ли требования к безопасной разработке ПО значимых объектов КИИ?

2. Регламентирован ли процесс безопасной разработки ПО для персонала вашей организации, осуществляющего разработку ПО? Выпишите перечень организационно-распорядительной документации вашей организации (регламентов, инструкций, правил), регламентирующих процессы разработки (сопровождения) ПО. Проверьте, установлены ли требования к безопасной разработке ПО значимых объектов КИИ, регламентированы ли процессы безопасной разработки ПО в документации?

3. Реализованы ли требования к безопасной разработке ПО значимых объектов КИИ на уровне технической и эксплуатационной документации ПО?

4. Выполняются ли правила и процедуры безопасной разработки (сопровождения) ПО для значимых объектов КИИ? Проверьте, соблюдаются ли сотрудниками, непосредственно участвующими в разработке ПО, установленные требования? Все ли процессы разработки соответствуют эталонным, установленным требованиями вашей организации?

Выполнение указанных выше трех базовых пунктов говорит о высоком уровне зрелости процессов безопасной разработки, необходимом для дальнейшего выполнения п. 29.3 Приказа ФСТЭК России № 239.

На основании проанализированной информации оцените уровень зрелости процессов безопасной разработки ПО в вашей организации:

1. Сформируйте перечень договоров с внешними организациями на оказание услуг по разработке (сопровождению) ПО значимых объектов КИИ:

1) _____

2) _____

3) _____

4) _____

5) _____

6) _____

7) _____

и т.д.

2. Проверьте, включены ли в договоры с внешними организациями следующие требования:

Требования к ПО	**1**	**2**	**3**	**4**
	Да/ Нет/ Реализовано частично			
Функциональные требования к ПО				
Функциональные требования к безопасности ПО				
Требования к испытаниям по выявлению уязвимостей в ПО				
Требования о необходимом уровне сервиса (SLA) при оказании услуг разработки (сопровождения) ПО				
Требования к технической и эксплуатационной документации на создаваемое ПО				

В случае, если указанные выше требования не включены в договоры с внешними организациями на оказание услуг по разработке (сопровождению) ПО значимых объектов КИИ, необходимо пересмотреть требования к разрабатываемому ПО для дальнейшего выполнения п. 29.3 Приказа ФСТЭК России № 239.

3. Сформируйте перечень значимых объектов КИИ:

1) _____

2) _____

3) _____

4) _____

5) _____

6) _____

7) _____

и т.д.

4. Для каждого значимого объекта КИИ проведите оценку выполнения требований.

Требования к ПО	1	2	3	4
	Да/ Нет/ Реализовано частично			
На стадии определения требований к обеспечению безопасности значимого объекта КИИ				
Установлены ли Техническим заданием на создание (модернизацию, дооснащение) значимого объекта КИИ и (или) создание (модернизацию, дооснащение) подсистемы безопасности значимого объекта следующие требования:				
– требования по безопасной разработке прикладного ПО, выполняющего функции по назначению				
– требования к испытаниям по выявлению уязвимостей в ПО				
– требования к поддержке безопасности ПО				
– требования к составу и содержанию документации, включающей сведения об оценке соответствия ПО требованиям безопасности				
На стадии проектирования значимого объекта КИИ и (или) подсистемы безопасности значимого объекта КИИ				
Включены ли в проектную документацию на значимый объект КИИ (подсистему безопасности значимого объекта) следующие сведения:				
– сведения, подтверждающие наличие руководства по безопасной разработке ПО				
– сведения о проведении анализа угроз безопасности информации ПО				
– сведения о проекте архитектуры ПО на уровне подсистем и результатов сопоставления функций программного обеспечения и интерфейсов, описанных в функциональной спецификации, с его подсистемами **(для объектов КИИ 1 категории значимости)**				
– сведения о процедурах отслеживания и исправления обнаруженных ошибок и уязвимостей ПО				
– сведения о способах и сроках доведения разработчиком (производителем) ПО до его пользователей информации об уязвимостях ПО, о компенсирующих мерах по защите информации или ограничениях по применению ПО, способов получения пользователями ПО его обновлений, проверки их целостности и подлинности				
– сведения о наличии процедур информирования субъекта КИИ об окончании производства и (или) поддержки ПО **(для объектов КИИ 1 категории значимости)**				

На стадии проектирования значимого объекта КИИ и (или) подсистемы безопасности значимого объекта КИИ				
Проведены ли в отношении ПО испытания:				
– статический анализ кода ПО				
– фаззинг-тестирование ПО				
– динамический анализ кода ПО **(для объектов КИИ 1 категории значимости)**				

На основании ответов оцените необходимость корректировки требований к ПО и (или) проектной документации значимых объектов КИИ — в случае если для значимого объекта КИИ требования не выполняются либо выполняются частично, необходимо сформировать требования к значимому объекту КИИ, доработать проектную документацию на значимый объект КИИ и провести дополнительные испытания прикладного ПО на соответствие требованиям по безопасной разработке.

ЛИСТ САМОКОНТРОЛЯ ДЛЯ РАЗРАБОТЧИКОВ, ПО ДЛЯ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

Оцените, регламентирован ли процесс безопасной разработки ПО для персонала вашей организации, осуществляющего разработку ПО. Проведите анализ установленных требований к безопасной разработке ПО в организационно-распорядительной документации вашей организации:

Процессы безопасной разработки ПО	Да/ Нет/ Реализовано частично
Процесс проектирования архитектуры ПО	
Процесс написания кода и сборки ПО	
Процесс квалификационного тестирования ПО	
Процессы приемки и инсталляции ПО	
Процесс эксплуатации ПО	
Процесс обеспечения безопасности среды разработки	
Процесс обучения сотрудников	

При разработке ПО для значимого объекта КИИ:

1. Определите перечень ПО, в отношении которого заказчиком установлены требования к безопасной разработке, либо ПО, которое планируется разработать и (или) внедрить в рамках создания, модернизации, дооснащения значимых объектов КИИ:

1) _____

2) _____

3) _____

4) _____

5) _____

6) _____

7) _____

8) _____

и т.д.

2. В отношении установленного ПО проверьте, реализованы ли требования к безопасной разработке:

Требования к ПО	1	2	3	4
	Да/ Нет/ Реализовано частично			
Разработано ли руководство по безопасной разработке ПО, определяющее все необходимые меры обеспечения безопасной разработки ПО?				
Проведен ли в отношении внедряемого ПО анализ угроз?				
Разработан ли проект архитектуры, включающий описание структуры ПО на уровне подсистем и результатов сопоставления функций ПО и интерфейсов, описанных в функциональной спецификации, с его подсистемами **(обязательно только для объектов КИИ 1 категории значимости)**				
Проводится ли в отношении установленного ПО статический анализ кода?				
Проводится ли в отношении установленного ПО фаззинг-тестирование?				
Проводится ли в отношении установленного ПО динамический анализ кода? **(обязательно только для объектов КИИ 1 категории значимости)**				
Регламентированы ли в документации к ПО процедуры отслеживания и исправления обнаруженных ошибок и уязвимостей ПО?				
Регламентированы ли в документации к ПО процедуры информирования пользователей об уязвимостях ПО, компенсирующих мерах по защите информации или ограничениях по применению ПО, способах получения пользователями обновлений ПО и порядке проверки их целостности и подлинности				
Регламентированы ли в документации к ПО процедуры информирования пользователей об окончании производства и (или) поддержки ПО? **(обязательно только для объектов КИИ 1 категории значимости)**				

На основании ответов оцените необходимость корректировки технической и (или) эксплуатационной документации ПО, разрабатываемого для значимых объектов КИИ – в случае если требование не выполняется либо выполняется частично, необходимо доработать техническую и (или) эксплуатационную документацию ПО и провести его дополнительные испытания на соответствие требованиям по безопасной разработке ПО.

Какие трудности могут возникнуть?

При выполнении требований по безопасной разработке ПО возникает много сложностей как у Субъектов КИИ, так и у компаний, разрабатывающих ПО для значимых объектов КИИ.

Субъекты КИИ, как правило, сталкиваются с необходимостью проведения оценки соответствия внедряемого ПО требованиям Приказа ФСТЭК России № 239, при этом отсутствуют собственные инструменты для проверки ПО и, как правило, недостаточно компетенций для проведения качественной оценки ПО.

Основная проблема компаний-разработчиков — отсутствие временных ресурсов и специалистов с необходимым уровнем компетенций для выстраивания полноценного процесса безопасной разработки по всем направлениям (анализ архитектуры безопасности, анализ кода, тестирование ПО, отслеживание и исправление ошибок и др.). На каждое направление требуются специалисты и, соответственно, дополнительные финансовые затраты.

Для того, чтобы полноценно запустить процесс безопасной разработки, необходимо пройти следующие этапы:

1. Сформировать собственный подход и описать цикл безопасной разработки ПО.
2. Сформировать команду специалистов и распределить между ними ответственность.
3. Выбрать инструменты для анализа программного кода и архитектуры, тестирования ПО.
4. Выстроить процессы безопасной разработки ПО.

Чем мы можем помочь?

№ п/п	Услуги УЦСБ	Описание предоставляемых услуг
1.	Аудит процесса безопасной разработки ПО	Обследование текущих процессов разработки ПО, оценка степени и полноты внедрения мер по обеспечению безопасности разработки ПО, степени соответствия процессов разработки ПО требованиям Приказа ФСТЭК России № 239
2.	Внедрение и сопровождение средств анализа и защиты	· Подбор необходимого инструментария для анализа кода, анализа уязвимостей, обеспечения безопасности среды разработки · Пилотирование и внедрение поставляемых решений и продуктов · Сопровождение продуктов и поддержка их работоспособности
3.	Внедрение и сопровождение процессов безопасной разработки ПО	Разработка комплекса мероприятий, направленных на внедрение процессов безопасной разработки ПО и привидение их в соответствие требованиям Приказа ФСТЭК России № 239
4.	Проведение технических проверок	· Тестирование на проникновение · Статический анализ кода и анализ зависимостей · Сканирование инфраструктуры разработки на наличие уязвимостей · Динамический анализ ПО
5.	Подготовка к сертификации программного обеспечения	· Проведение технических проверок и формирование протоколов проведения испытаний · Разработка пакета документации для подготовки к сертификации ПО
6.	Предоставление сервисов DevSecOps	· Обработка отчетов · Анализ критичности и уязвимости функционала · Консультирование по выявленным уязвимостям · Анализ защищенности ПО
7.	Предоставление экспертных консультаций	· Консультации разработчиков по уязвимостям и типам атак · Консультации по применимым требованиям к ПО · Консультации по методикам, инструментам и лучшим практикам безопасной разработки ПО