

ЦБИ

Центр
безопасности
информации



Павлов Артем

Начальник отдела управления испытаниями
и контроля качества

Департамент испытаний ООО «ЦБИ»

Формирование и предъявление
требований безопасности к
программному обеспечению

Формирование требований к ПО

1. Проводится анализ ТЗ на разработку ПО: назначение ПО, область применения, пользователи, состав обрабатываемых данных, требования к самому ПО, возможные ограничения к разработке ПО, перечень заинтересованных сторон.
2. Определяется перечень требований к ПО и процессу его разработки: ограничения на основе функциональных/нефункциональных требований, требования безопасности в соответствии с нормативными документами регуляторов, требования к языкам программирования, требования к архитектуре, требования к применяемым технологиям и самому процессу разработки ПО, требования стандартов и проч.
3. Проводится контроль непротиворечивости и однозначности трактования перечня требований.
4. Проводится согласование перечня требований с Заказчиком, определение порядка и правил изменения требований.

Требования безопасности

ГОСТ Р ИСО/МЭК 15408-1-2012

3.1.62 Требование безопасности: Требование, изложенное на стандартизованном языке и направленное на достижение целей безопасности для объекта оценки.

3.1.60 Цель безопасности: Изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и/или предположениям.

Требования безопасности: Комплекс мер и правил, направленных на защиту информации и предотвращение появления уязвимостей в программном обеспечении.

Требования безопасности

Требование безопасности определяются

- в нормативных документах регуляторов
- по результатам оценки рисков и угроз

Основные источники сведений об угрозах

- БДУ ФСТЭК России
- зарубежные БД уязвимостей (например, CVE от MITRE)
- БД шаблонов компьютерных атак (CAPEC)
- результаты исследований
- отчеты компаний
- отчеты компьютерных криминалистов

ГОСТ Р 56939-2024. Защита информации. Разработка безопасного программного обеспечения. Общие требования.

5.3 Формирование и предъявление требований безопасности к ПО.

Цель

Обеспечение безопасности ПО посредством предъявления к нему требований и управления требованиями в процессе изменения (разработки) ПО.

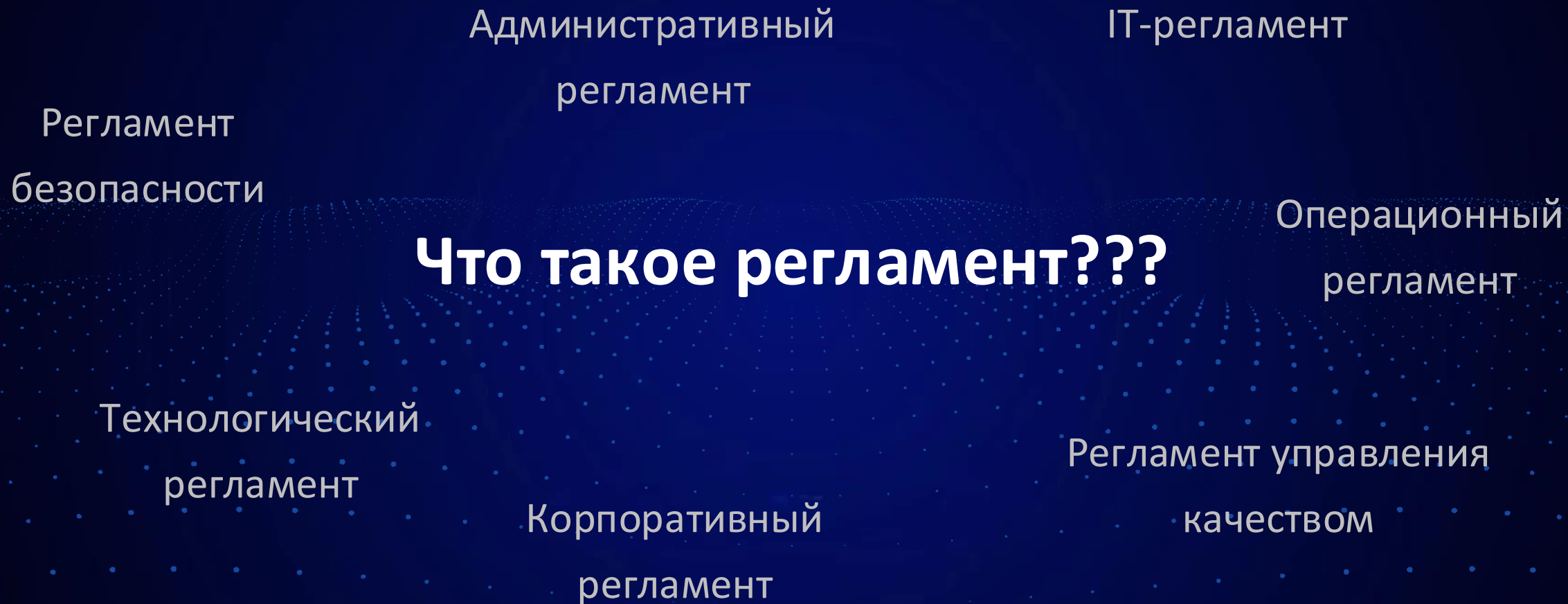
Требования к реализации

0. **Определить меры защиты информации для процесса.**
1. Разработать регламент управления требованиями безопасности ПО.
2. Предъявлять к ПО требования безопасности.
3. Вести учет предъявленных требований безопасности и контроль однозначности трактования и непротиворечивости набора требований безопасности ПО.
4. Осуществлять пересмотр набора требований безопасности на основе выполнения критериев пересмотра – с установленной периодичностью или при наступлении определённых событий.

Меры защиты информации для процессов.

4.17 В ходе реализации процессов разработки безопасного ПО должны быть реализованы меры по защите информации, относящейся к этим процессам, — разграничение доступа к результатам исследований и тестирования, обеспечение защищенного хранения соответствующей информации и антивирусная защита. Меры защиты информации для процессов разработки безопасного ПО могут быть включены в регламенты реализации соответствующих процессов разработки безопасного ПО или содержаться в отдельном документе разработчика.

Необходимо описать все возможные риски и угрозы, которые могут привести к нарушению безопасности разрабатываемого ПО при реализации процесса или к нарушению самого процесса, а также меры безопасности, нейтрализующие данные угрозы.



Что такое регламент?

Регламент: документ, который:

- определяет состав и порядок выполнения задач в рамках реализации процесса;
- описывает стандарты (правила) выполнения задач;
- описывает меры безопасности, которые должны быть реализованы при выполнении регламента;
- определяет порядок контроля выполнения регламента;
- определяет ответственных лиц;
- определяет перечень необходимых ресурсов.

Зачем нужен регламент?

Определение ответственности.

Регламент чётко определяет, кто отвечает за выполнение конкретных задач и какие у него полномочия. Это исключает дублирование функций и перекладывание ответственности.

Описание последовательности действий.

Обеспечивает единообразие выполнения операций и снижает вероятность ошибок.

Выявление узких мест.

Регламент позволяет выявить неэффективные процессы и оптимизировать использование времени и ресурсов.

Зачем нужен регламент?

Установка критериев и показателей.

Позволяют оценить качество выполнения работ.

Обучение новых сотрудников.

Регламент помогает новичкам быстрее освоить необходимые навыки и знания.

Определение правил безопасности.

Регламент определяет правила безопасности, которые необходимо соблюдать при выполнении работы.

Упрощение контроля.

Проще следить за тем, как выполняются задачи: чётко описано кто, что, как и когда делает.

Структура регламента

1. Общие положения.
2. Требования безопасности к процессу.
3. Описание процесса.
4. Перечень необходимых ресурсов.
5. Обязанности сотрудников и их роли.
6. Порядок контроля.
7. Порядок внесения изменений.
8. Приложения.

Структура регламента

Общие положения.

В этом разделе указываются цели (назначение) и задачи регламента, область его применения, используемые термины и определения, а также ссылки на другие регламентирующие документы.

Требования безопасности к процессу.

В данном разделе детально описываются все возможные риски и угрозы, которые могут привести к нарушению безопасности разрабатываемого ПО при реализации данного процесса или к нарушению самого процесса, а также меры безопасности, нейтрализующие данные угрозы. При разработке данного раздела регламента необходимо использовать ГОСТ Р 58412-2019.

Структура регламента

Описание процесса.

В данном разделе детально описывается порядок выполнения конкретного процесса или деятельности. В нем описываются все этапы процесса , последовательность действий для каждого этапа, учитывающие меры безопасности, используемые ресурсы, требования к качеству, к безопасности и другие параметры.

Описание процесса должно содержать:

- наименование каждого этапа;
- перечень и последовательность выполнения мероприятий каждого этапа;
- действия сотрудников при выполнении мероприятий;
- описание входных и выходных данных.

Структура регламента

Перечень необходимых ресурсов.

В данном разделе указываются все ресурсы, необходимые для обеспечения непрерывного выполнения процесса в соответствии с установленными для него критериями качества.

Данный раздел, как минимум, должен включать:

- описание критериев качества процесса;
- описание требований к ресурсам в соответствии с критериями качества.

В качестве требований к ресурсам могут выступать требования к знаниям и навыкам специалистов, участвующих в реализации процесса, требования к применяемым инструментальным средствам, требования к входным данным процесса.

Структура регламента

Обязанности сотрудников и их роли.

В данном разделе четко определяется, кто отвечает за выполнение каждого этапа процесса и какие у него полномочия. Для каждого сотрудника должны быть определены его роль, описание его функций (возможных действий) в рамках каждого этапа процесса, его ответственность и полномочия, описание (порядок) взаимодействия сотрудников в рамках реализации мероприятий по каждому этапу процесса.

Структура регламента

Порядок контроля.

В этом разделе описывается, как и когда (при каких условиях, событиях) осуществляется контроль за выполнением регламента, кто проводит контроль, какие показатели (критерии) используются для оценки качества выполнения регламента и какие меры принимаются в случае выявления нарушений. Контроль за выполнением регламента может выполняться в рамках мероприятий СМК организации. В этом случае в данном разделе должны быть ссылки на документы СМК, применяемые для контроля качества выполнения регламента или процесса.

Структура регламента

Порядок внесения изменений.

В этом разделе описывается процедура внесения изменений в регламент, кто и при каких условиях имеет право это делать и как эти изменения утверждаются.

Приложения.

В этом разделе могут быть представлены дополнительные сведения, необходимые для реализации регламента: формы документов, шаблоны, инструкции, схемы и другие материалы, необходимые для выполнения регламента.

Порядок формирования регламента

1. Определяется область действия регламента.
2. Проводится описание процесса: кто, когда и какие действия будет выполнять, а также результаты этих действий.
3. Определяется перечень необходимых ресурсов для успешного выполнения регламента.
4. Определяется порядок контроля (различные метрики и показатели) для оценки эффективности и соблюдения регламента.
5. Определяется порядок и правила внесения изменений в регламент (кто может вносить изменения, с кем согласовываются и кем утверждаются изменения, когда вступают в силу)
6. Определяются критерии внесения изменений в регламент (изменение состава группы разработки, изменение состава применяемых средств, изменение перечня мероприятий по реализации регламента).
7. Определяется состав специалистов, участвующих в реализации регламента, их роли, обязанность и ответственность в рамках выполнения регламента.
8. Проводится контроль компетенций специалистов с последующим обучением (если необходимо).
9. Проводится доведение регламента до всех участников процесса.

Регламент управления требованиями безопасности ПО

Пункт 5.3.3.1 ГОСТ Р 56939-2024

Регламент управления требованиями безопасности ПО должен включать следующие положения:

- порядок предъявления требований безопасности ПО;
- порядок предоставления требований безопасности ПО исполнителям;
- порядок отслеживания процесса предоставления, получения и выполнения требований безопасности ПО;
- критерии пересмотра требований безопасности ПО (периодически, при наступлении определенных событий).

Порядок предъявления требований безопасности ПО

Определяет основные правила предъявления требований безопасности ПО с учетом требований безопасности к процессу:

- кто может предъявлять требования;
- основания для предъявления требований;
- правила оформления (описания) требований ;
- порядок контроля однозначности трактования и непротиворечивости требований;
- порядок пересмотра и внесения изменений в требования;
- порядок согласования и утверждения требований.

Порядок предоставления требований безопасности ПО исполнителям

Определяет основные правила предоставления требований исполнителям и содержит следующие сведения:

- способы обеспечения безопасности требований (меры по нейтрализации угроз) при их предоставлении пользователям;
- состав ответственных за предоставление доступа исполнителей к требованиям;
- роли исполнителей и описание их прав доступа к требованиям;
- способы предоставления доступа исполнителей к требованиям.

Порядок отслеживания процесса предоставления, получения и выполнения требований безопасности ПО

Определяет основные правила отслеживания процесса предоставления, получения и выполнения требований безопасности ПО и содержит следующие сведения:

- описание статусов реализации требований;
- способы отслеживания текущего статуса реализации требований;
- перечень применяемых средств автоматизации и указаний по их конфигурации и настройке;
- описание порядка эскалации требований.

Критерии пересмотра требований безопасности ПО

Содержит перечень критериев пересмотра требований безопасности ПО (периодически, при наступлении определенных событий).

Примеры критериев (по событиям):

- появление новых угроз безопасности информации;
- противоречия в реализации с другими требованиями;
- изменение области применения ПО;
- изменение архитектуры ПО;
- изменение бизнес-функций ПО.

Набор требований безопасности ПО

Пункт 5.3.3.2 ГОСТ Р 56939-2024.

Набор требований безопасности ПО должен содержать следующую информацию:

- идентификатор требования безопасности ПО;
- формулировку требования безопасности ПО;
- дату предъявления требований безопасности ПО;
- приоритет/важность требования безопасности ПО;
- предполагаемые сроки реализации;
- сведения о сотрудниках (подразделениях), предъявивших требования;
- сведения о сотрудниках (подразделениях), принявших требования к реализации;
- ограничения по реализации требований;
- критерии реализации требований.

Учет предъявляемых требований безопасности ПО

Пункт 5.3.3.3 ГОСТ Р 56939-2024.

Артефакты реализации требований, подтверждающие осуществление учета предъявленных требований безопасности ПО, должны включать, как минимум, следующую информацию:

- сведения о принятии требований к реализации, подтверждающие однозначность трактования и непротиворечивость набора требований безопасности ПО;
- текущий статус реализации требований;
- сведения об изменениях статуса реализации предъявленных требований безопасности ПО;
- сведения об изменениях предъявленных требований безопасности ПО.

Уточнение набора требований безопасности ПО

Пункт 5.3.3.4 ГОСТ Р 56939-2024

Набор требований безопасности ПО, уточненный по результатам выполнения требований 5.3.2.4 (после пересмотра с установленной периодичностью или при наступлении определённых событий), должен содержать информацию об особенностях реализации требований безопасности ПО в процессе разработки ПО, принятых решениях по корректировкам требований безопасности ПО в процессе разработки.

Спасибо за внимание!



<https://t.me/CyBearIn>



<https://cbi-info.ru>