Изи рубежка

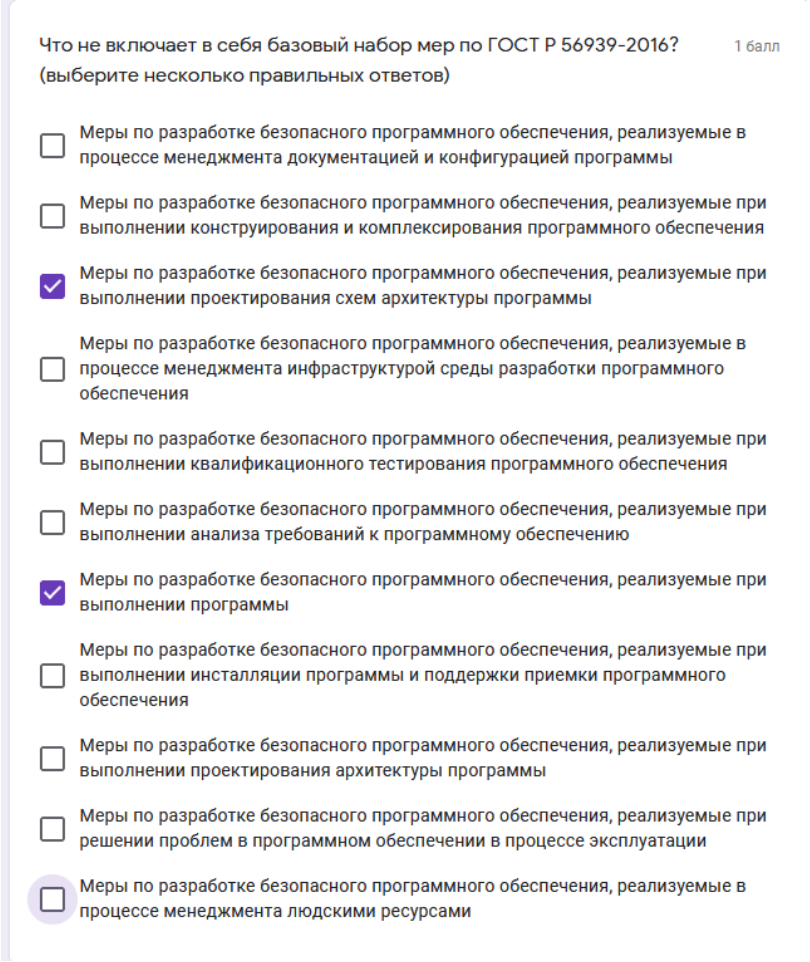
ГОСТ1: https://docs.cntd.ru/document/1200135525

ГОСТ2: https://docs.cntd.ru/document/1200164529

ГОСТ3: https://docs.cntd.ru/document/1200022653

Are you sl♂ves ready for a workout?
Yes sir!
Alright!

6. Что не включает в себя базовый набор мер по ГОСТ Р 56939-2016? (выберите несколько правильных ответов)



7. Что должно быть в результате успешной реализации мер по дизайну и архитектуре программного обеспечения? (выберите несколько правильных ответов)

Что должно быть в результате успешной реализации мер по дизайну и архитектуре программного обеспечения? (выберите несколько правильных ответов) 1 балл

- [x] требования по безопасности, предъявляемые к ПО, уточняют по результатам выполнения моделирования угроз безопасности информации, которые могут возникнуть вследствие применения ПО
- [ ] требования по безопасности, предъявляемые к ПО, уточняют по результатам создания моделирования угроз безопасности информации, которые могут возникнуть вследствие применения ПО
- [ ] проект архитектуры программы разрабатывают без учета необходимости выполнения требований по безопасности, предъявляемых к разрабатываемому ПО
- [x] проект архитектуры программы разрабатывают с учетом необходимости выполнения требований по безопасности, предъявляемых к разрабатываемому ПО
- [ ] формируют исходные коды (перечень выявленных потенциальных угроз безопасности информации), используемые при проведении динамического анализа кода программы, фаззинг-тестирования программы и тестирования на проникновение
- [x] формируют исходные данные (перечень выявленных потенциальных угроз безопасности информации), используемые при проведении динамического анализа кода программы, фаззинг-тестирования программы и тестирования на проникновение

В результате успешной реализации мер:

- программа должна быть создана с учетом требований по безопасности, установленных в процессе анализа требований к ПО;

- при создании программы должны быть использованы только идентифицированные разработчиком ПО инструментальные средства с определенными опциями (настройками);

- в исходном коде программы должны быть выявлены и устранены недостатки программы (потенциально уязвимые конструкции);

- необходимо сформировать исходные данные (перечень выявленных потенциально уязвимых конструкций в исходном коде программы), используемые при проведении динамического анализа кода программы, фаззинг-тестирования программы и тестирования на проникновение.

8. Как называется передача исходного кода программного обеспечения на хранение независимой третьей стороне?

software escrow
https://en.wikipedia.org/wiki/Source_code_escrow

9. Когда должен быть внедрён процесс управления изменениями?

10. Что позволяет оценить реализацию в программе механизмов проверки входных данных?

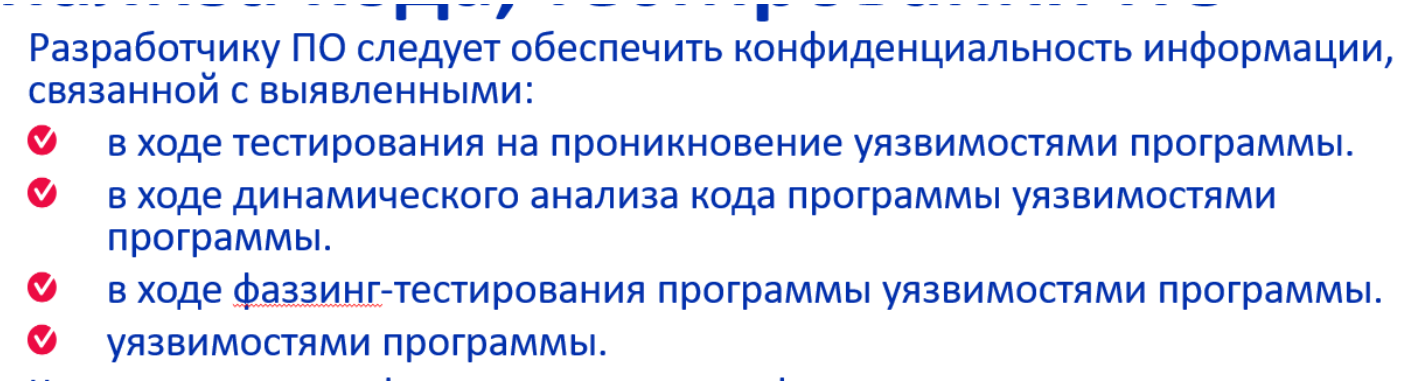
Проверка на защищенность ? +?

Ф♂ззинг-тестирование?

Регулярное автоматизированное сканирование на уязвимости позволяет выявить и устранить уязвимости до выпуска продукта. На данном этапе также рекомендуется выполнить фаззинг тестирование, чтобы проверить, что программа корректно отвечает, как на ожидаемые, так и на случайные входные значения, - это позволяет идентифицировать ошибки переполнения буфера, проверки входных параметров и проблемы безопасности.

11. Какой информации разработчику ПО следует обеспечить защиту? (выберите несколько правильных ответов)

верно? НЕВЕРНО. Верно всё.



12. Кто является целевой аудиторией стандарта ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»? (выберите несколько правильных ответов)

Разработчики программного обеспечения
Производители программного обеспечения

оценщики

Настоящий стандарт предназначен для разработчиков и производителей программного обеспечения, а также для организаций, выполняющих оценку соответствия процесса разработки программного обеспечения требованиям настоящего стандарта.?????
Органы по сертификации оборудования?

Т.е. в Госте одно, а в презентации Маркиной другое))))
оценщики -не основная, но аудитория

Настоящий стандарт предназначен для разработчиков и производителей программного обеспечения, а также для организаций, выполняющих оценку соответствия процесса разработки программного обеспечения требованиям настоящего стандарта.

13. Зачем необходимы реестры и базы уязвимостей?

Накапливаем знания о уязвимостях, чтобы избежать потенциальных рисков, с которыми они связаны

14. Что должно содержать требование по реализации меры в соответствии с ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения.

Общие требования»? (выберите несколько правильных ответов)

При написании требования оно должно содержать:

- Уникальный идентификатор требований.
- Название.
- Процесс жизненного цикла ПО.
- Достигаемая цель.
- Элементы действий разработчика.
- Элементы содержания и представления документированных свидетельств.
- Элементы действий оценщика.

5.1.3 Требования к реализации мер по разработке безопасного программного обеспечения

5.1.3.1 Разработчик ПО должен определить требования по безопасности, предъявляемые к разрабатываемому ПО.

Для организации работ, выполняемых в процессах жизненного цикла ПО, и подтверждения соответствия требованиям настоящего стандарта документация разработчика ПО должна содержать перечень определенных требований по безопасности, предъявляемых к разрабатываемому ПО.

Примечание - В качестве источников для формирования требований разработчик ПО может использовать требования законов, нормативных правовых актов, отраслевых стандартов, перечень требований пользователя, сценарии применения ПО. Например, могут быть определены следующие требования к ПО:

- к обеспечению идентификации и аутентификации;

- обеспечению защиты от несанкционированного доступа к информации;

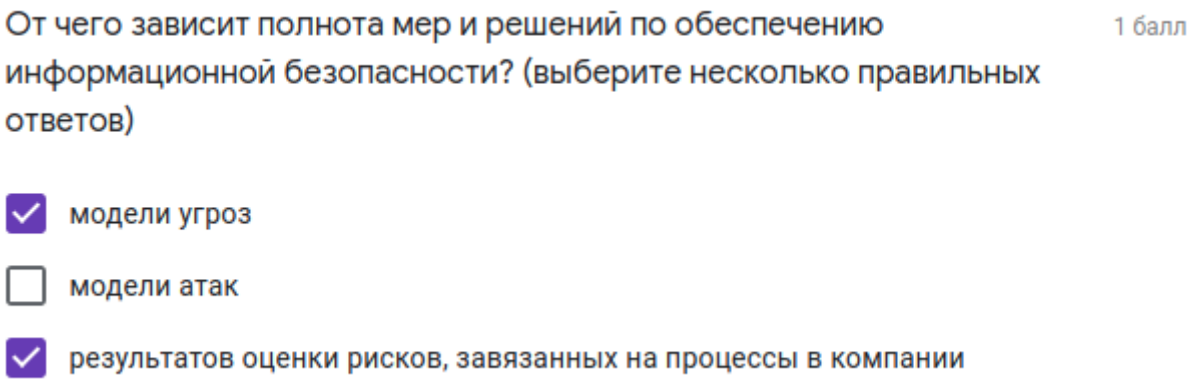
- обеспечению регистрации событий;

- контролю точности, полноты и правильности данных, поступающих в программу;

- обработке программных ошибок и исключительных ситуаций.

это не то да?
ТО!

15. От чего зависит полнота мер и решений по обеспечению информационной безопасности? (выберите несколько правильных ответов)



модель угроз точно подходит, модель атак непонятно вообще существует или нет, а третье ну там тоже вроде бы должно быть

16. Что необходимо проверять дополнительно при обеспечении информационной безопасности?

(тут не написано что несколько правильных ответов в скобочках поэтому думаю так)