



Московский институт электроники
и математики им. А.Н. Тихонова

DevOps/DevSecOps.
Безопасная разработка

2024

Конвейер безопасной разработки ПО

Елаев Сергей



План по теме

1. Теория. Стандарты. Методологии. Угрозы при БРПО.
2. Процессы БРПО. Описание конвейера и инструменты БРПО.



План занятия

1. ГОСТ 56939-20XX. БРПО. Общие требования
2. Модель OWASP SAMM
3. Угрозы по ГОСТ 58412-2019



ГОСТ Р 56939–2016 «Защита информации. Безопасная разработка программного обеспечения. Общие требования»

1. Сбор и анализ требований к разрабатываемому ПО;



ГОСТ Р 56939–2016 «Защита информации. Безопасная разработка программного обеспечения. Общие требования»

1. Сбор и анализ требований к разрабатываемому ПО;
2. Проектирование архитектуры ПО;



ГОСТ Р 56939–2016 «Защита информации. Безопасная разработка программного обеспечения. Общие требования»

1. Сбор и анализ требований к разрабатываемому ПО;
2. Проектирование архитектуры ПО;
3. Написание программного кода;



ГОСТ Р 56939–2016 «Защита информации. Безопасная разработка программного обеспечения. Общие требования»

1. Сбор и анализ требований к разрабатываемому ПО;
2. Проектирование архитектуры ПО;
3. Написание программного кода;
4. Тестирование ПО;



ГОСТ Р 56939–2016 «Защита информации. Безопасная разработка программного обеспечения. Общие требования»

1. Сбор и анализ требований к разрабатываемому ПО;
2. Проектирование архитектуры ПО;
3. Написание программного кода;
4. Тестирование ПО;
5. Инсталляция и поддержка приемки;



ГОСТ Р 56939–2016 «Защита информации. Безопасная разработка программного обеспечения. Общие требования»

1. Сбор и анализ требований к разрабатываемому ПО;
2. Проектирование архитектуры ПО;
3. Написание программного кода;
4. Тестирование ПО;
5. Инсталляция и поддержка приемки;
6. Обеспечение безопасности в процессе эксплуатации;



ГОСТ Р 56939–2016 «Защита информации. Безопасная разработка программного обеспечения. Общие требования»

1. Сбор и анализ требований к разрабатываемому ПО;
2. Проектирование архитектуры ПО;
3. Написание программного кода;
4. Тестирование ПО;
5. Инсталляция и поддержка приемки;
6. Обеспечение безопасности в процессе эксплуатации;
7. Управление документацией и конфигурацией ПО;



ГОСТ Р 56939–2016 «Защита информации. Безопасная разработка программного обеспечения. Общие требования»

1. Сбор и анализ требований к разрабатываемому ПО;
2. Проектирование архитектуры ПО;
3. Написание программного кода;
4. Тестирование ПО;
5. Инсталляция и поддержка приемки;
6. Обеспечение безопасности в процессе эксплуатации;
7. Управление документацией и конфигурацией ПО;
8. Управление инфраструктурой среды разработки;



ГОСТ Р 56939–2016 «Защита информации. Безопасная разработка программного обеспечения. Общие требования»

1. Сбор и анализ требований к разрабатываемому ПО;
2. Проектирование архитектуры ПО;
3. Написание программного кода;
4. Тестирование ПО;
5. Инсталляция и поддержка приемки;
6. Обеспечение безопасности в процессе эксплуатации;
7. Управление документацией и конфигурацией ПО;
8. Управление инфраструктурой среды разработки;
9. Управления человеческими ресурсами.

ГОСТ Р 56939–2016 «Защита информации. Безопасная разработка программного обеспечения. Общие требования»

1. Сбор и анализ требований к разрабатываемому ПО;
2. Проектирование архитектуры ПО;
3. Написание программного кода;
4. Тестирование ПО;
5. Инсталляция и поддержка приемки;
6. Обеспечение безопасности в процессе эксплуатации;
7. Управление документацией и конфигурацией ПО;
8. Управление инфраструктурой среды разработки;
9. Управления человеческими ресурсами.



Рисунок 1.1 – Взаимосвязь ГОСТ Р 56939–2016 с национальными стандартами

ГОСТ Р 56939–2016 «Защита информации. Безопасная разработка программного обеспечения. Общие требования»

1. Сбор и анализ требований к разрабатываемому ПО;
2. Проектирование архитектуры ПО;
3. Написание программного кода;
4. Тестирование ПО;
5. Инсталляция и поддержка приемки;
6. Обеспечение безопасности в процессе эксплуатации;
7. Управление документацией и конфигурацией ПО;
8. Управление инфраструктурой среды разработки;
9. Управления человеческими ресурсами.

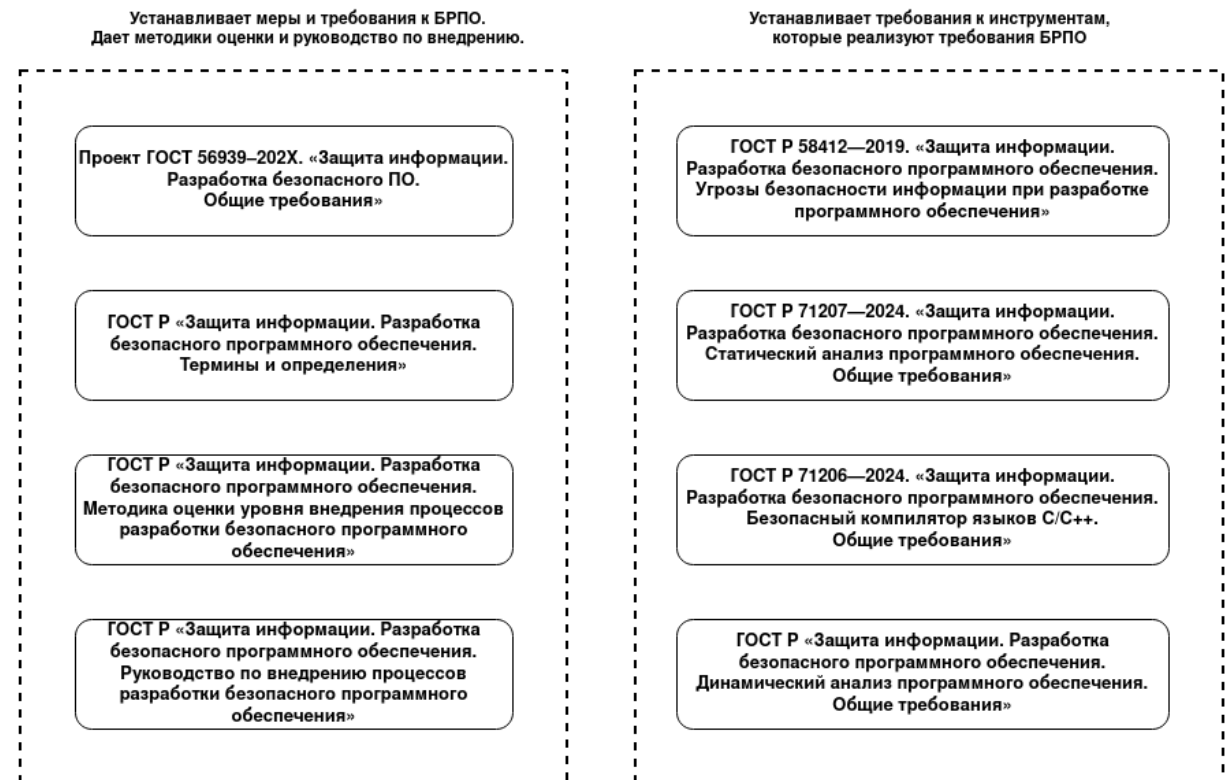


Рисунок 1.2 – Стандарты по безопасной разработке ПО



ГОСТ Р 56939–2016. БРПО.

1. Сбор и анализ требований к разрабатываемому ПО;
2. Проектирование архитектуры ПО;
3. Написание программного кода;
4. Тестирование ПО;
5. Установка и поддержка приемки;
6. Обеспечение безопасности в процессе эксплуатации;
7. Управление документацией и конфигурацией ПО;
8. Управление инфраструктурой среды разработки;
9. Управления человеческими ресурсами.

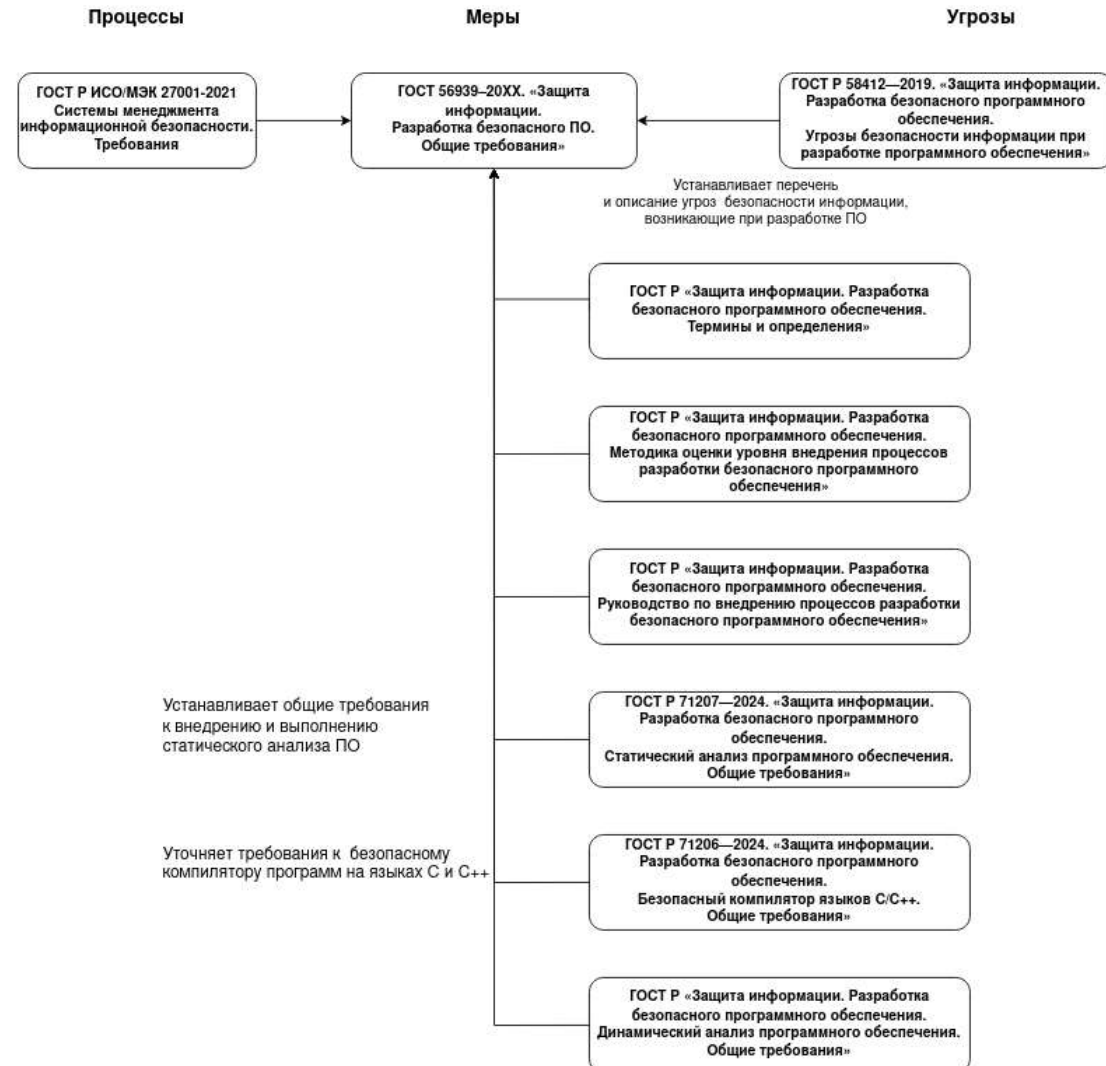


Рисунок 1.3 - Взаимосвязь ГОСТ Р 56939–20XX с другими стандартами



ГОСТ 56939-202X проект. БРПО. Общие требования

1. Процессный подход;
2. Построение плана развития БРПО;
3. Построение ролей и обязанностей сотрудников;
4. Обеспечение безопасности используемых секретов;



ГОСТ 56939-202X проект. БРПО. Общие требования. Процессы разработки безопасного программного обеспечения

1. 5.1 Планирование процессов разработки безопасного программного обеспечения;
2. 5.2 Обучение сотрудников
3. 5.3 Формирование и предъявление требований безопасности к программному обеспечению
4. 5.4 Управление конфигурацией программного обеспечения
5. 5.5 Управление недостатками и запросами на изменение программного обеспечения
6. 5.6 Разработка, уточнение и анализ архитектуры программного обеспечения
7. 5.7 Моделирование угроз и разработка описания поверхности атаки
8. 5.8 Формирование и поддержание в актуальном состоянии правил кодирования
9. 5.9 Экспертиза исходного кода
10. 5.10 Статический анализ исходного кода
11. 5.11 Динамический анализ кода программы



ГОСТ 56939-202X проект. БРПО. Общие требования. Процессы разработки безопасного программного обеспечения

- 12. 5.12 Использование безопасной системы сборки программного обеспечения
- 13. 5.13 Обеспечение безопасности сборочной среды программного обеспечения
- 14. 5.14 Обеспечение целостности кода при разработке программного обеспечения
- 15. 5.15 Обеспечение безопасности используемых секретов
- 16. 5.16 Использование инструментов композиционного анализа
- 17. 5.17 Проверка кода на предмет внедрения вредоносного кода через цепочки поставок
- 18. 5.18 Функциональное тестирование
- 19. 5.19 Нефункциональное тестирование
- 20. 5.20 Обеспечение безопасности при выпуске готовой к эксплуатации версии программного обеспечения
- 21. 5.21 Безопасная доставка программного обеспечения пользователям



ГОСТ 56939-202X проект. БРПО. Общие требования. Процессы разработки безопасного программного обеспечения

- 22. 5.22 Обеспечение поддержки программного обеспечения на этапе эксплуатации пользователями
- 23. 5.23 Обеспечение реагирования на информацию об уязвимостях
- 24. 5.24 Поиск уязвимостей в эксплуатирующемся программном обеспечении
- 25. 5.25 Обеспечение безопасности при выводе программного обеспечения из эксплуатации



DevSecOps.

Процессы разработки безопасного программного обеспечения



DevSecOps.

Процессы разработки безопасного программного обеспечения

1. 5.1 Планирование процессов разработки безопасного программного обеспечения;
2. 5.3 Формирование и предъявление требований безопасности к программному обеспечению
3. 5.4 Управление конфигурацией программного обеспечения
4. 5.5 Управление недостатками и запросами на изменение программного обеспечения
5. 5.6 Разработка, уточнение и анализ архитектуры программного обеспечения
6. 5.7 Моделирование угроз и разработка описания поверхности атаки
7. 5.8 Формирование и поддержание в актуальном состоянии правил кодирования
8. 5.10 Статический анализ исходного кода
9. 5.11 Динамический анализ кода программы
10. 5.16 Использование инструментов композиционного анализа
11. 5.18 Функциональное тестирование

Фреймворк OWASP SAMM

1. Управление (Governance);
2. Проектирование (Design);
3. Разработка (Implementation);
4. Верификация (Verification);
5. Операции (Operations).

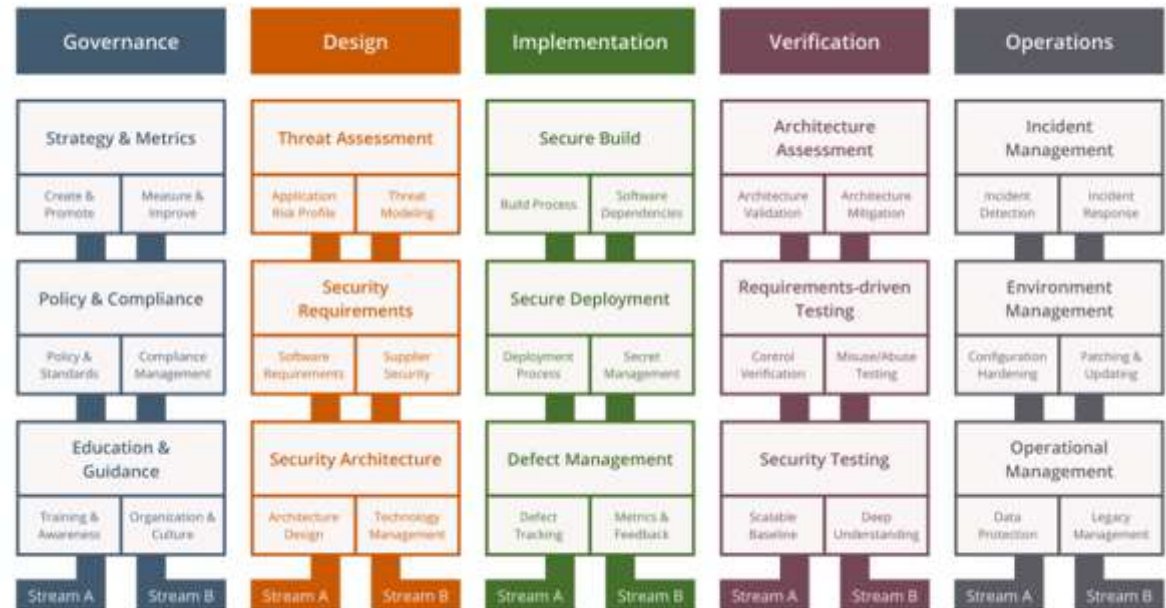


Рисунок 1.4 – Схематическое представление модели
безопасной разработке ПО OWASP SAMM v2

Фреймворк OWASP SAMM

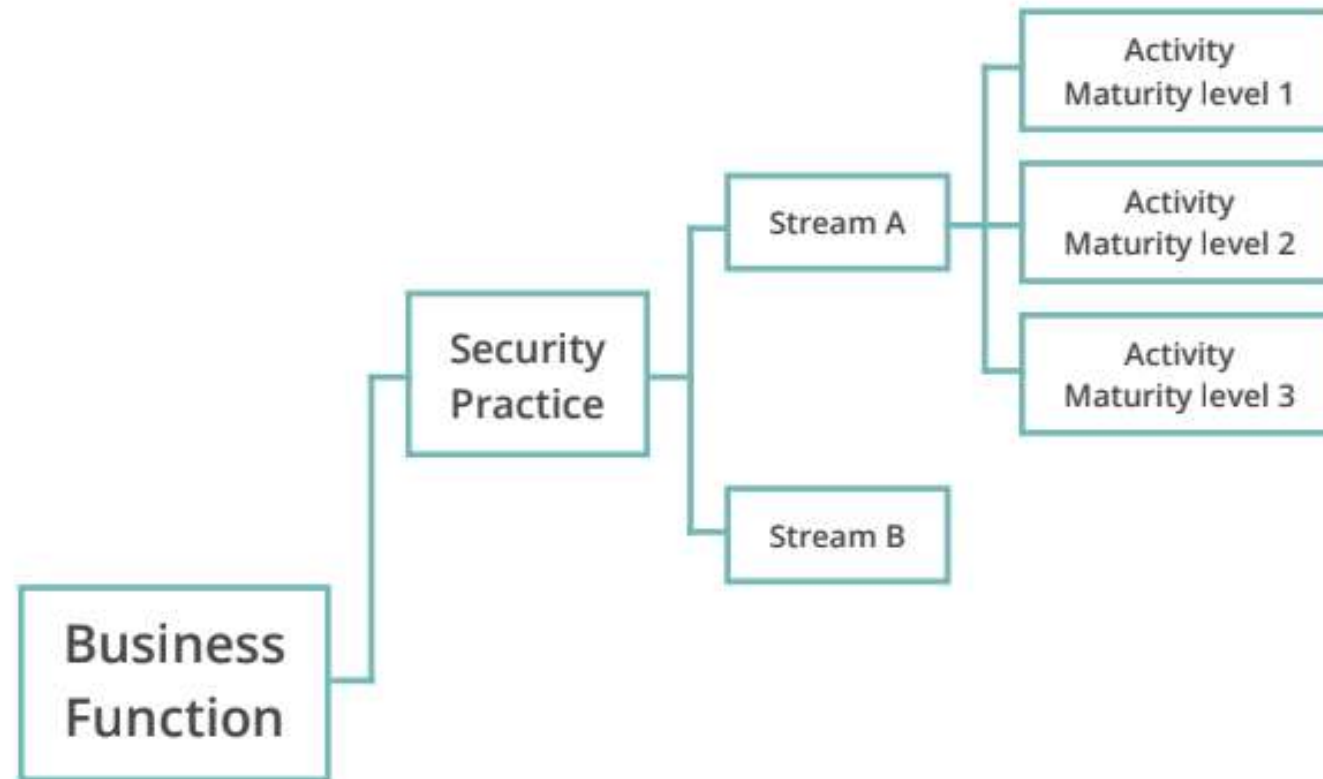


Рисунок 1.5 – Схематическое представление бизнес
функции по OWASP SAMM v2 ([Источник](#))



OWASP SAMM. Governance

SECURITY PRACTICE	STREAM A	STREAM B
Strategy & Metrics	Create & Promote	Measure & Improve
Policy & Compliance	Policy & Standards	Compliance Management
Education & Guidance	Training & Awareness	Organization & Culture



OWASP SAMM. Design

SECURITY PRACTICE	STREAM A	STREAM B
Threat Assessment	Application Risk Profile	Threat Modeling
Security Requirements	Software Requirements	Supplier Security
Security Architecture	Architecture Design	Technology Management



OWASP SAMM. Implementation

SECURITY PRACTICE	STREAM A	STREAM B
Secure Build	Build Process	Software Dependencies
Secure Deployment	Deployment Process	Secret Management
Defect Management	Defect Tracking	Metrics & Feedback



OWASP SAMM. Verification

SECURITY PRACTICE	STREAM A	STREAM B
Architecture Assessment	Architecture Validation	Architecture Mitigation
Requirements-driven Testing	Control Verification	Misuse/Abuse Testing
Security Testing	Scalable Baseline	Deep Understanding



OWASP SAMM. Operations

SECURITY PRACTICE	STREAM A	STREAM B
Incident Management	Incident Detection	Incident Response
Environment Management	Configuration Hardening	Patching & Updating
Operational Management	Data Protection	Legacy Management



OWASP SAMM. Operations

SECURITY PRACTICE	STREAM A	STREAM B
Incident Management	Incident Detection	Incident Response
Environment Management	Configuration Hardening	Patching & Updating
Operational Management	Data Protection	Legacy Management

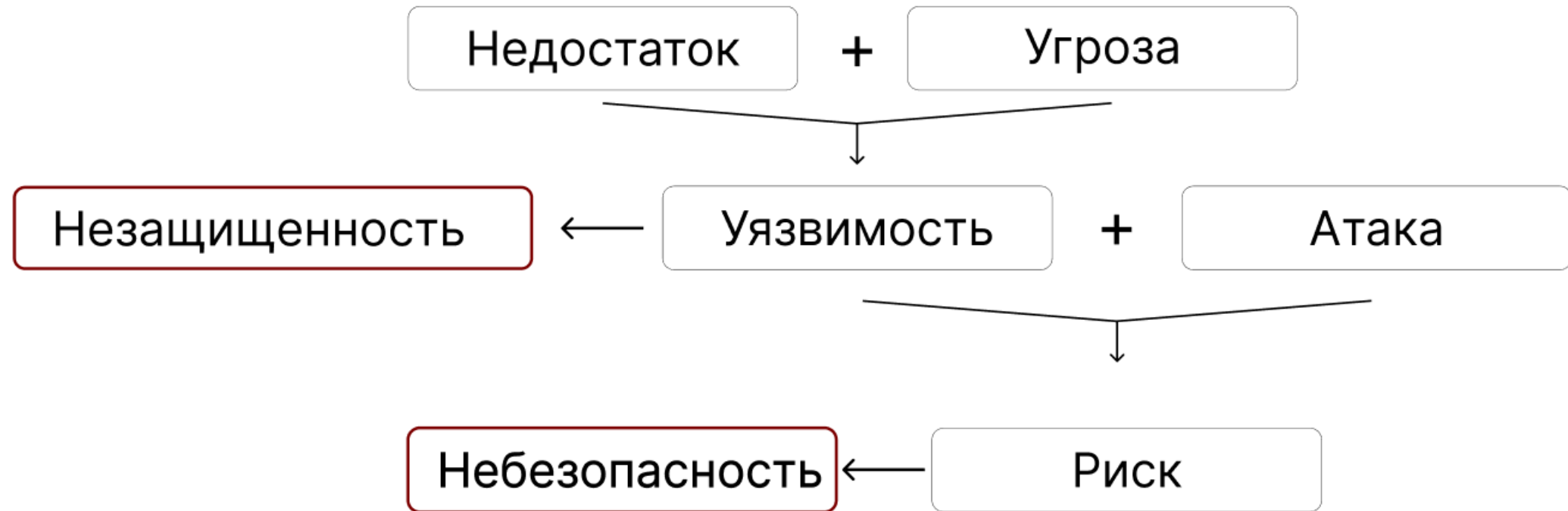


БРПО

1. ГОСТ 56939-20XX БРПО
2. Модель OWASP SAMM
3. Здравый смысл



Угрозы





Угрозы

1. Угрозы безопасности информации при выполнении анализа требований к программному обеспечению
2. Угрозы безопасности информации при выполнении проектирования архитектуры программы
3. Угрозы безопасности информации при выполнении конструирования и комплексирования программного обеспечения



Угрозы

1. Угрозы безопасности информации при выполнении анализа требований к программному обеспечению
2. Угрозы безопасности информации при выполнении проектирования архитектуры программы
3. Угрозы безопасности информации при выполнении конструирования и комплексирования программного обеспечения
4. Угрозы безопасности информации при выполнении квалификационного тестирования программного обеспечения
5. Угрозы безопасности информации при выполнении инсталляции программы и поддержки приемки программного обеспечения
6. Угрозы безопасности информации при решении проблем в программном обеспечении в процессе эксплуатации



Угрозы

1. Угрозы безопасности информации при выполнении анализа требований к программному обеспечению
2. Угрозы безопасности информации при выполнении проектирования архитектуры программы
3. Угрозы безопасности информации при выполнении конструирования и комплексирования программного обеспечения
4. Угрозы безопасности информации при выполнении квалификационного тестирования программного обеспечения
5. Угрозы безопасности информации при выполнении инсталляции программы и поддержки приемки программного обеспечения
6. Угрозы безопасности информации при решении проблем в программном обеспечении в процессе эксплуатации
7. Угрозы безопасности информации в процессе менеджмента документацией и конфигурацией программы
8. Угрозы безопасности информации в процессе менеджмента инфраструктурой среды разработки программного обеспечения
9. Угрозы безопасности информации в процессе менеджмента людскими ресурсами



Задание 1

Выбрать из ГОСТ 56939-202X проект один из процессов и описать в нотации BPMN

