



Тема: Разработка и апробация методики самотестирования программного обеспечения в соответствии с требованиями к безопасной разработке ПО

Докладчик: Д.И.Правиков



План работы ЭнергоЦИБ на 2024 г. (утвержден протоколом ЭГКБ от 25.01.2024 г.)

2.1.27. Оценка качества программного обеспечения стартапов и иного программного обеспечения по критерию выполнения требований безопасной разработки

Целью оценки качества программного обеспечения стартапов и иного программного обеспечения, предлагаемого к использованию на предприятиях членов АЦЭ, по критерию выполнения требований безопасной разработки, является повышение защищенности объектов критической инфраструктуры предприятий за счет снижения уровня угроз в цепочке поставок программного обеспечения.

Общая схема оценки качества программного обеспечения





Разработаны проекты документов:

- обоснование необходимости реализации процессов безопасной разработки ПО;
- методика самотестирования разработанного и предлагаемого к внедрению на предприятия участников Ассоциации ПО;
- чек-лист результатов самотестирования;
- шаблон технического заключения по результатам тестирования.



Основные позиции чек-листа

- Наличие решения руководства о реализации процесса РБПО
- Наличие человеческих ресурсов на реализацию процесса РБПО
- Наличие процесса обучения работников требованиям к процессу РБПО
- Наличие документальных свидетельств реализации процесса РБПО
- Наличие процесса использования систем хранения исходного кода, дистрибутива и сборки программного обеспечения
- Наличие процесса обеспечения безопасности сборочной среды программного обеспечения, системы хранения исходного кода и реализован процесс обеспечения целостности кода при разработке программного обеспечения и передаче дистрибутива пользователю
- Наличие процесса формирования и предъявления требований безопасности к ПО
- Наличие эксплуатационной документации и документации в части определения поверхности атаки
- Наличие процесса композитного анализа
- Проверка процесса разработки на предмет внедрения вредоносного кода через цепочки поставок
- Наличие процесса функционального тестирования
- Наличие процесса статического анализа исходного кода
- Наличие процесса управления уязвимостями
- Наличие процесса поддержки программного обеспечения
- Декларация обязательства через год обеспечить выполнение базового уровня соответствия требованиям по РБПО



Платформа для автоматизации бизнес-процессов без программирования Low-Code



СИСТЕМЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА





- Получение обратной связи по результатам апробации
- Возможная корректировка методики
- Возможное подключение других стартапов