**Жуковский Евгений Владимирович Анализ безопасности киберфизических систем с использованием методов машинного обучения.**

ОГЛАВЛЕНИЕ ДИССЕРТАЦИИ

кандидат наук Жуковский Евгений Владимирович

Введение

1 Анализ угроз информационной безопасности программного обеспечения киберфизических систем

1.1 Особенности применения и построения КФС

1.2 Анализ программного и аппаратного обеспечения, входящего в состав

КФС

1.2.1 Анализ состава систем промышленного и медицинского назначения

1.3 Анализ угроз ПО КФС, связанных с наличием уязвимостей

1.3.1 Анализ уязвимостей компонентов систем промышленного назначения

1.3.1 Анализ уязвимостей компонентов систем медицинского назначения

1.3.2 Особенности уязвимостей в компонентах КФС

1.4 Анализ угроз ПО КФС, связанных с наличием вредоносных функциональных возможностей

1.4.1 Анализ функциональных возможностей ВПО, применяемого в целенаправленных атаках

1.4.2 Анализ функциональных возможностей ВПО, применяемого в целенаправленных атаках на компоненты КФС

1.5 Исследование существующих способов затруднения анализа безопасности ПО

1.5.1 Механизмы защиты программы от статического анализа

1.5.2 Механизмы защиты программы от динамического анализа

1.6 Выводы

2 Исследование существующих подходов и методов анализа безопасности

программного обеспечения

2.1 Методы преодоления механизмов защиты исполняемого кода от исследования

2.1.1 Методы преодоления механизмов защиты от статического анализа

2.1.2 Методы преодоления механизмов защиты от динамического анализа

2.2 Подходы к выявлению вредоносных функциональных возможностей в программном обеспечении с использованием методов машинного обучения

2.2.1 Выявление вредоносных исполняемых файлов на основе статического анализа

2.2.2 Выявление вредоносных исполняемых файлов на основе динамического анализа

2.3 Выводы

3 Подход к выявлению опасных функциональных возможностей ПО на основе многовариантного динамического анализа с использованием методов машинного обучения и символьного выполнения

3.1 Определение функциональных возможностей ПО на основе многовариантного динамического анализа поведения программы в изолированном окружении

3.2 Модель функционирования анализируемого процесса в вычислительной системе, учитывающая порождаемые им информационные потоки

3.3 Метод предварительной оценки потенциальной опасности путей выполнения программы на основе кластерного анализа вызываемых системных функций

3.4 Выявление скрытых функциональных возможностей в ПО с применением технологии динамического символьного выполнения

3.4.1 Использование графа характеристик для представления исполняемого кода анализируемой программы

3.4.2 Алгоритм выявления скрытых функциональных возможностей в ПО с применением технологии динамического символьного выполнения

3.5 Метод оптимизации выбора путей выполнения анализируемой программы с использованием машинного обучения с подкреплением

3.6 Критерии опасности выполняемых операций на основе анализа порождаемых ими информационных потоков с использованием показателей доверия и критичности

3.7 Методика обнаружения ВПО на основе многоэтапного анализа

безопасности программы

3.8 Выводы

4 Прототип системы анализа безопасности ПО КФС и результаты Экспериментальных исследований

4.1 Архитектура и схема функционирования разработанного прототипа системы анализа безопасности ПО КФС

4.2 Экспериментальные исследования возможности увеличения покрытия исполняемого кода программы и преодоления механизмов защиты от анализа

4.3 Экспериментальные исследования возможности выявления опасных функциональных возможностей в ВПО КФС

4.4 Выводы

Заключение

Список сокращений и условных обозначений

Список использованных источников

Приложение А

Приложение Б

ВВЕДЕНИЕ