**УДК 004.056.53**

# ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ СКРЫТЫХ КАНАЛОВ В ПРОЦЕССЕ ПРОЕКТИРОВАНИЯ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

**Архипов Н. Д.** (Университет ИТМО)
**Научный руководитель – к.т.н. Таранов С. В.**
(Университет ИТМО)

В данной работе предложены методы защиты от угроз скрытых каналов в процессе проектирования безопасного программного обеспечения. На основе рассмотренных методов разработан фреймворк для обнаружения скрытых каналов.

**Введение.**

Постоянно растущие угрозы утечки данных связаны с тем, что злоумышленники используют скрытые каналы для кражи данных без возможности обнаружения ни программной средой, ни средствами защиты информации (межсетевой экран, системы обнаружения вторжений). При этом в российском законодательстве отсутствуют нормативные документы, которые регламентируют методы защиты программного обеспечения от скрытых каналов, кроме ГОСТ Р 53113.1–2008 «Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения» и ГОСТ Р 53113.2–2009 «Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов», которые, во-первых, относятся к автоматизированным системам, а не к программному обеспечению. Во-вторых, в ГОСТах содержится вводная информация по защите автоматизированных систем от скрытых каналов. В-третьих, ГОСТы сравнительно давно изданы и теряют актуальность в современном информационном мире.

**Основная часть.**

Предлагается разработать комплекс мер, направленных на обнаружение и предотвращение появления скрытых каналов по памяти и по времени в процессах жизненного цикла программного обеспечения, и на их основе разработать фреймворк, который будет содержать следующие паттерны:

– Трассировка вызовов программного обеспечения, осуществляющая контроль соответствия связей между информационными и функциональными модулями;

– Архитектура программного обеспечения для проверки взаимодействия компонентов программного обеспечения;

– Отслеживание выполнения процессов, в результате которого анализируются вмешательства во взаимодействие между системными процессами;

– Анализ сетевого трафика программного обеспечения для отслеживания скрытой передачи данных от встроенного агента к злоумышленнику:

- Модуляция размера блока данных (например, IP-пакета или TCP-сегмент);
- Модуляция значения поля заголовка;
- Зарезервированный/неиспользуемый шаблон в полях заголовка.
- Скорость передачи пакета.

**Выводы.**

Для испытаний предлагается использовать статистические тесты (метрики: автокорреляция, регулярность, энтропия, критерий Колмогорова-Смирнова, мультимодальный анализ). Таким образом, в результате научной работы проведённые тесты

позволят оценить эффективность разработанного фреймворка для обнаружения скрытых каналов.

| | |
|---|---|
| Архипов Н. Д. (автор) | Подпись |
| Таранов С. В. (научный руководитель) | Подпись |