СЕРГЕЙ ТАЛАНТОВ

БЕЗОПАСНЫЙ C++

РУКОВОДСТВО ПО БЕЗОПАСНОМУ ПРОЕКТИРОВАНИЮ И РАЗРАБОТКЕ ПРОГРАММ

Издательство АСТ
Москва

УДК 004.43
ББК 32.973.2
Т16

Талантов, Сергей.
Т16 Безопасный C++. Руководство по безопасному проектированию и разработке программ / Талантов С. — Москва: Издательство АСТ, 2025. — 416 с. — (Программирование для всех)

ISBN 978–5–17–173860–0

«Безопасный C++» — это глубокое погружение в аспекты программирования на C++. Книга предназначена для специалистов, которые хотят повысить уровень защиты своих приложений и научиться применять лучшие практики безопасности в реальных проектах.

Внутри четыре основных раздела:

- «Безопасность приложений» — ключевые принципы обеспечения безопасности, включая материал по бинарной отладке.
- «Безопасная реализация» — в этом разделе раскрываются низкоуровневые вопросы безопасности при написании программ на C++ — здесь о потенциальных проблемах и возможных решениях.
- «Безопасная архитектура» — о принципах построения безопасной архитектуры приложений, что позволит создавать более надёжные и устойчивые системы.
- «Безопасный процесс» — методики и практики повышения качества, надежности и безопасности разрабатываемого ПО.

Акцент книги — на практическом применении теоретических знаний, где будут представлены примеры и сценарии, которые можно адаптировать для использования в собственных проектах. Книга станет незаменимым ресурсом для разработчиков, стремящихся повысить уровень безопасности своих приложений и защитить их от потенциальных угроз.

УДК 004.43
ББК 32.973.2

ISBN 978–5–17–173860–0

Об авторе

Сергей Талантов — разработчик, архитектор программного обеспечения и чемпион безопасности, программирующий на языке C++ более 20 лет. Опыт работы в компаниях, занимающихся информационной безопасностью, Акронис и Лаборатории Касперского более 10 лет. Контрибьютор Chromium, член архитектурного комитета KasperskyOS. Постоянный спикер на конференциях C++ Russia, Highload.

Содержание

1. Безопасность приложений

Безопасность приложений — это одна из составных частей информационной безопасности. В этой части книги мы сделаем небольшой обзор основных понятий, касающихся безопасности в общем смысле и информационной безопасности, в частности. Чтобы разобраться, что относится к безопасности приложений, мы проследим путь этой дисциплины от самых высокоуровневых базовых концепций к более частным, касающихся непосредственно кода. Атрибуты, типы, модели и принципы безопасности — это то, что нас ждет в начале пути. Далее погрузимся глубже и узнаем, как на практике реализуется безопасность приложений. На этом уровне нас ждут уязвимости, угрозы, риски. Наконец, дойдем до бинарного уровня. Здесь поговорим про эксплойты и методы бинарной защиты.

1.1 Основы безопасности

Давайте начнем сначала! Эта глава — первый кирпичик в фундаменте. Здесь вы не найдете сложных технических подробностей или кода, но зато получите четкое представление о том, с чем имеете дело, и узнаете основные термины, которые пригодятся в дальнейшем. Если вы уже в курсе всего про безопасность приложений и информационную безопасность в целом, то можете смело пропустить эту главу и перейти к самому интересному.

1.1.1 Что такое безопасность

Чтобы поговорить о безопасности, нам нужно разобраться в некоторых базовых терминах. Не волнуйтесь, мы не будем вдаваться в сложные теории и длинные списки определений. Мы сосредоточимся только на самом важном, чтобы вы могли легко понять материал этой книги.

Безопасность — состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.[1]

Защищать можно все, что угодно, поэтому существуют разные виды безопасности: авиационная, биологическая, военная, пожарная и т.д. Нас в первую очередь будет интересовать **информационная**, которая, как логично было бы предположить, касается защиты информации.

Информационная безопасность — безопасность, связанная с угрозами в информационной сфере.[2]

Информация в современном мире обрабатывается в основном с использованием компьютеров, которые объединяют в себе аппаратное и программное обеспечение — такую информационную безопасность можно назвать компьютерной. Далее еще сузим предметную область и введём термин «безопасность приложений», который касается именно разработки программного обеспечения и направлен на предотвращение уязвимостей в программном коде. Место безопасности приложений в общей иерархии безопасности показано на рисунке ниже (Рисунок 1.1).

Обеспечение **безопасности приложений** — это процесс применения мер и средств контроля и управления и измерений к приложениям организации с целью осущест–

[1] Закон РФ от 5 марта 1992 г. N 2446–I «О безопасности»

[2] СТО БР ИББС–1.0–2014 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения.

вления менеджмента риска, возникающего в результате их использования.[1]

Рисунок 1.1 Безопасность приложений в общей иерархии безопасности

1.1.2 Функциональная и информационная безопасность

Стоит отметить, что в английском языке есть два термина, обозначающих безопасность: **security** и **safety** — различия между ними весьма существенны, хотя в русском языке в большинстве случаев их объединяют и используют как синонимы.

Термин **security** обозначает безопасность со стороны внешней среды (Рисунок 1.2). Это безопасность от внешних атакующих, других программ и любых действий, угрожающих системе — обычно именно эту безопасность имеют в виду по умолчанию. Иногда ее называют **кибербезопасностью** (если контекст касается вычислительных машин, сетей, компьютерных систем) или просто **информационной безопасностью** (если контекст более общий).

[1] ГОСТ Р ИСО/МЭК 27034–1–2014 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность приложений.

Кибербезопасность — это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных.[1]

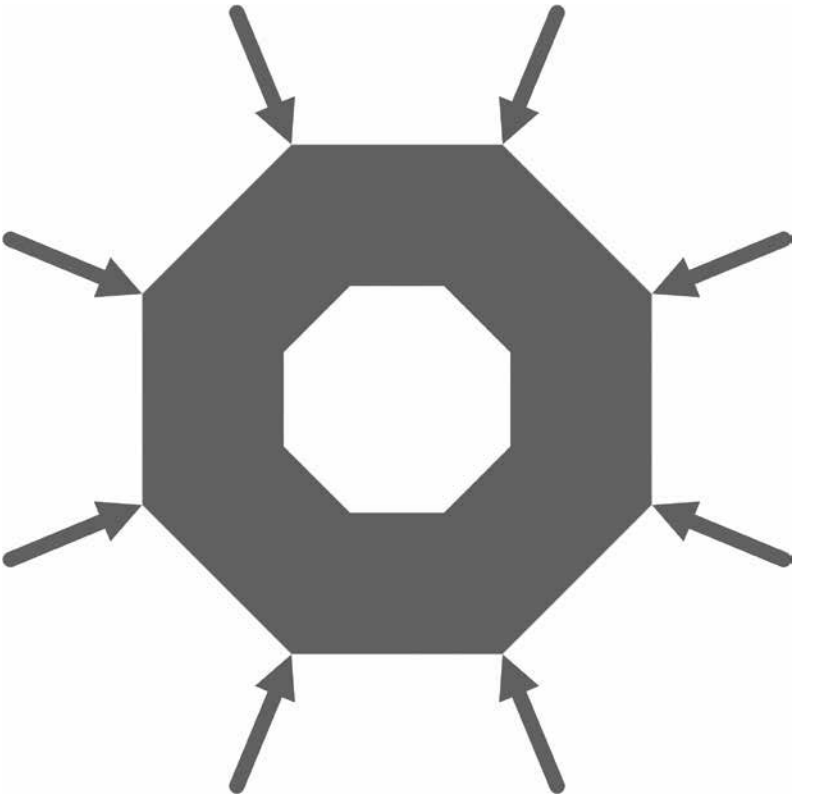

Рисунок 1.2 Информационная безопасность

Термин **safety** обозначает безопасность самой системы при возможных нарушениях ее работы (Рисунок 1.3). Например, в случае ошибки или намеренного повреждения ПО медицинского оборудования, оно может повлечь смерть пациентов и таким образом стать первичной угрозой. При исключении риска сбоев и неполадок такое оборудование становится безопасным от внутренних угроз. Иногда такую безопасность в русском языке называют **функциональной**.

[1] https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security