

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 С++. 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 С++» — это глубокое погружение в аспекты программирования на С++. 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 С++ — 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, надёжности 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

© Сергей Талантов, текст
© ООО Издательство «АСТ»

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

Об авторе.	3
О книге	4
Благодарности	6
Введение	9
1. БЕЗОПАСНОСТЬ ПРИЛОЖЕНИЙ	12
1.1 Основы безопасности.	12
1.1.1 Что такое безопасность.	13
1.1.2 Функциональная и информационная безопасность.	14
1.1.3 Триада информационной безопасности	16
1.1.4 Золотой стандарт безопасного доступа.	18
1.1.5 Модели безопасности.	20
1.1.6 Принципы безопасности	22
1.2 Уязвимости, угрозы и риски	23
1.2.1 Классификация уязвимостей и угроз	25
1.2.2 Оценка уязвимостей.	28
1.2.3 Базы данных уязвимостей	32
1.2.3.1 CVE	32
1.2.3.2 CWE	33
1.2.3.3 OWASP Top 10	36
1.2.3.4 CAPEC.	37
1.2.4 Модель угроз	39
1.2.5 Модель нарушителя	42
1.2.6 Выявление угроз	43
1.3 Эксплойты.	45

1.3.1	Переполнение стека	45
1.3.2.	Уязвимый код	50
1.3.3	Отказ в обслуживании	52
1.3.4	Изменение поведения программы	52
1.3.5	Выполнение произвольного кода	53
1.3.6	Повышение привилегий	58
1.3.7	Удаленное управление	60
1.3.8	Шелл–код	63
1.3.9.	Каталоги эксплойтов	68
1.4	Защита	69
1.4.1	Неисполняемая память	70
1.4.2	Рандомизация адресного пространства	76
1.4.3	Стековая канарейка	80
1.4.4	Позиционно независимый код	84
1.5	C++ и безопасность	87
2	БЕЗОПАСНАЯ РЕАЛИЗАЦИЯ	89
2.1	Строки	89
2.1.1	Инициализация нулевым указателем	91
2.1.2	Инвалидация итераторов	93
2.1.3	Выход за границы	96
2.1.4	Особенность SSO	97
2.1.5	Строковое представление	98
2.1.6	Определение длины	101
2.1.7	Строковые функции языка C	104
2.1.8	Резюме	106
2.2	Динамическая память	107
2.2.1	Как устроена куча	108
2.2.2	Использование памяти после удаления и висячие указатели	113
2.2.3	Разные операторы выделения и освобождения памяти	114

2.2.4 Особенности размещающего оператора new.	116
2.2.5 Отсутствие проверки результата выделения памяти.	118
2.2.6 Двойное удаление.	119
2.2.7 Ловушки умных указателей.	121
2.2.8 Динамическая память на стеке	124
2.2.9 Функции управления памятью языка С	125
2.2.9 Резюме	126
2.3 Инициализация	127
2.3.1 Способы инициализации	127
2.3.2 Сужающие преобразования.	136
2.3.3 Auto–переменные	138
2.3.4 Резюме	139
2.4 Арифметические операции.	140
2.4.1 Беззнаковые целые	143
2.4.2 Знаковые целые.	145
2.4.3 Битовые операции	150
2.4.4 Преобразования типов	151
2.4.5 Вещественные числа.	153
2.4.6 Резюме	158
2.5 Многопоточность.	159
2.5.1 Завершение работы.	160
2.5.2 Ошибки синхронизации	163
2.5.3 Взаимные блокировки	169
2.5.4 Резюме	173
2.6 Файлы	174
2.6.1 Пути	174
2.6.2 Состояние гонки.	176
2.6.3 Права доступа	180
2.6.4 Резюме	180
2.7 Криптография.	181
2.7.1 Симметричное шифрование	183
2.7.2 Асимметричное шифрование	192

2.7.3 Хеширование	201
2.7.4 Хеширование с ключом	206
2.7.5 Цифровая подпись	210
2.7.6 Случайные числа	214
2.7.7 Протоколы	220
2.7.8 Резюме	230
3 БЕЗОПАСНАЯ АРХИТЕКТУРА	232
3.1 Операционная и конструктивная безопасность	232
3.2 Паттерны безопасности	234
3.2.1 Одноразовый объект	235
3.2.2 Валидация	243
3.2.3 Объект–значение	248
3.2.4 Безопасное журналирование	254
3.2.5 Безопасная связь	261
3.2.6 Аутентификатор	264
3.2.7 Безопасный прокси	269
3.2.8 Домены безопасности	275
3.2.9 Монитор безопасности	285
3.2.10 Политика безопасности	294
3.2.11 Безопасное хранилище	305
3.2.12 Сессия	315
3.2.13 Микроядро	319
3.3 Архитектуры и методологии	326
4 БЕЗОПАСНЫЙ ПРОЦЕСС	336
4.1 Работа с кодом	337
4.2 Статический анализ	342
4.3 Сборка и укрепление	350
4.4 Динамический анализ	360
4.5 Фаззинг тестирование	366
4.6 DevSecOps	370

Заключение	377
Библиография	379
Глоссарий	384
ПРИЛОЖЕНИЯ	403
Приложение 1: эксплойт для обхода стековой канарейки	403
Приложение 2: эксплойт для обхода позиционно независимого кода	404
Приложение 3: опасные функции языка С и их безопасные альтернативы	406
Приложение 4: реализация функции memzero.	408

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, касающимся 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 2446-1 «О безопасности»

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



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 ▲

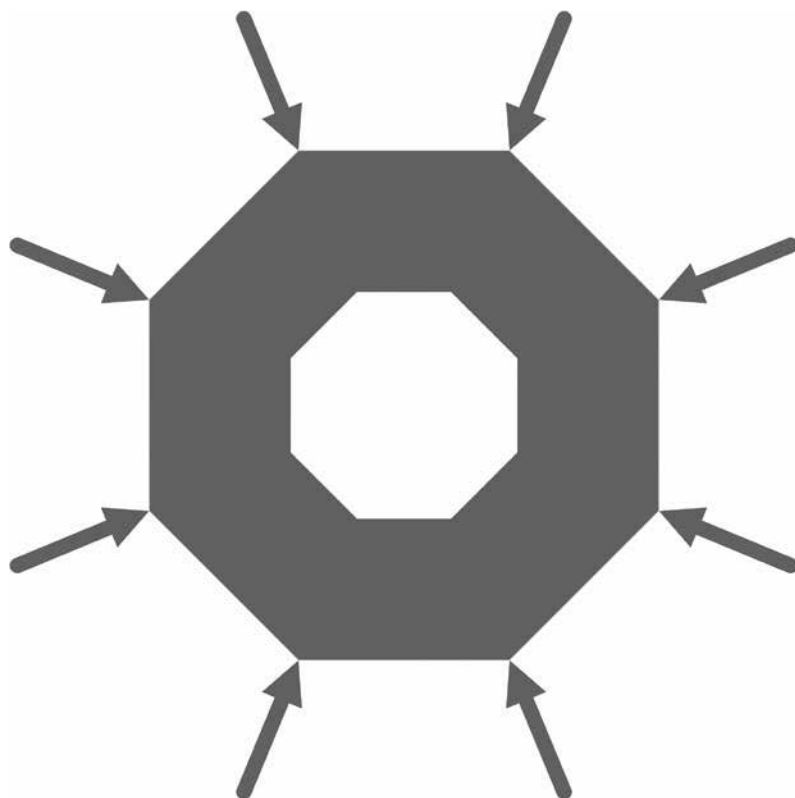


Рисунок 1.2 Информационная безопасность

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>