



Анализ кода и информационная безопасность

Осенний семестр 2025 г.



МГУ / ВМК / СП

Лекции

- Лектор — Соловьёв Михаил Александрович.
- Блок 01.
 - Лекция 01. Технологии разработки безопасного ПО.
 - Лекция 02. Основные понятия безопасности информации.
 - Лекция 03. Ошибка типа «переполнение буфера».
- Блок 02.
 - Лекция 04. Статический анализ исходного кода с целью поиска ошибок.
 - Лекция 05. Абстрактная интерпретация.
 - Лекция 06. Отладка и инструментирование.
 - Лекция 07. Фаззинг и символьное выполнение.
 - Лекция 08. Слайсинг.

Лекции

- Блок 03.
 - Лекция 09. Анализ бинарного кода.
 - Лекция 10. Статическое дизассемблирование.
 - Лекция 11. Восстановление потока управления и функций программы.
 - Лекция 12. Слайсинг по трассе и анализ помеченных данных.
 - Лекция 13. Анализ обращений к памяти в бинарном коде.
- Блок 04.
 - Лекция 14. Введение в сетевую безопасность.

Практические задания

- Все задания сдаются через сайт курса.
- У каждого студента будет индивидуальный вариант по каждому заданию.

- Задание 01. Ошибка типа «переполнение буфера».
 - От 0 до 20 баллов.
 - Предполагаемые сроки: с 19.09 по 03.10.
- Задание 02. Динамическое инструментирование бинарного кода.
 - От 0 до 10 баллов.
 - Предполагаемые сроки: с 10.10 по 24.10.
- Задание 03. Анализ трассы выполнения программы (две части).
 - От 0 до 30 баллов.
 - Предполагаемые сроки: с 14.11 по 12.12.

Экзамен и итоговая оценка

1. Экзамен в устной форме:
 - в билете два вопроса;
 - возможны дополнительные вопросы по всему лекционному материалу;
 - устный ответ оценивается по пятибалльной системе – E .
2. Набранные баллы за практические задания переводятся в оценку за практику по таблице – P . Таблица будет вывешена на сайте.
3. Итоговая оценка выставляется как функция E и P . Также будет вывешена на сайте.

Экзамен и итоговая оценка

Задание	Баллы
01	0 – 20
02	0 – 10
03.1	0 – 15
03.2	0 – 15
Всего	0 – 60

Оценка за практику	Баллы
«Отлично»	≥ 48 (80%)
«Хорошо»	≥ 36 (60%)
«Удовлетворительно»	≥ 24 (40%)

	Прак. – 5	Прак. – 4	Прак. – 3	Прак. – 2
Экз. – 5	5	5	4	3
Экз. – 4	5	4	4	3
Экз. – 3	4	3	3	3
Экз. – 2	3	2	2	2

Необходимые знания и умения

1. Работа в UNIX-окружении — практические задания будут выдаваться в виде образов виртуальной машины с ОС Debian.
2. Язык Си.
3. Язык ассемблера для x86 (16-, 32- или 64-разрядные варианты). На лекциях и в практических заданиях работа ведётся с 64-разрядным кодом. Перед началом работы с ассемблерным кодом на лекциях будет дана краткая справка по 64-разрядной архитектуре x86-64.
4. Базовые представления о компиляторных технологиях: граф потока управления, отношение доминирования, SSA-форма, распределение регистров в ходе кодогенерации.
5. Базовый математический аппарат: полурешётки, решётки, теорема Клини о неподвижной точке.
6. Потребуется читать литературу на английском языке.

Техническое обеспечение

- Сайт курса: <https://caiscourse.ru/>.
 - Будет работать со следующей недели.
 - Аннотации, слайды лекций и ссылки на литературу автоматически становятся доступны в момент начала соответствующей пары.
 - Для сдачи практических заданий необходимо будет зарегистрироваться на сайте.
- Электронная почта: 2025@caiscourse.ru.
- Telegram-канал: [@caiscourse2025](https://t.me/caiscourse2025).