Кафедра автоматизации информационной безопасности
Магистерская программа «Информационная безопасность компьютерных систем»

по учебному плану элективные курсы: ***21.02.2019***
1 семестр – нет, 2 семестр – 1 экзамен, 3 семестр – 1 экзамен, 4 семестр – 1 зачет

Список элективных спецкурсов для магистров
Весенний семестр 2018-19

1. **Теория кодирования и криптография/ Coding theory and cryptography,** Чижов Иван Владимирович
   среда, 14:35, ауд. 612

Курс посвящен квантовым криптографическим системам с открытым ключом, стойкость которых основывается на сложности некоторых задач из теории кодов, исправляющих ошибки. Слушатели познакомятся с некоторыми интересными классами кодовых криптосистем, а также с методами их криптографического анализа.

2. **Теоретико-числовые алгоритмы в криптографии/Number Theoretic algorithms in Cryptography,** Черепнёв Михаил Алексеевич,
   пятница, 14:35, ауд. 604

В курсе рассматриваются Алгоритмы быстрого умножения чисел и матриц. Быстрые операции в больших конечных полях. Быстрое обращение матриц, приведение целочисленных матриц к Эрмитовой и Смитовой нормальным формам. Метод Ланцоша решения разреженных систем. Блочные алгоритмы Монтгомери, Копперсмита, Ланцоша-Паде.

3. **Введение в практическую информационную безопасность/Introduction to practical information security,** Гамаюнов Денис Юрьевич, Петухов Андрей Александрович *вторник, 18:00, ауд. 685*

В курсе рассматриваются базовые проблемы безопасности приложений и анализа защищенности приложений, при этом акцент в курсе сделан на практические задания и знакомство с процессом непрерывного обучения в игровой форме соревнований по информационной безопасности (CTF). Рассматриваются следующие темы: уязвимости веб-приложений и атаки на них, бинарные уязвимости и атаки на них.

4. **Методы обнаружения уязвимостей в бинарных программах/Methods for binary vulnerabilities detection,** Гамаюнов Денис Юрьевич, Воронов Михаил Сергеевич,
   четверг, 18:00, ауд. 505

В курсе рассматриваются основные проблемы и задачи, связанные с уязвимостями программного обеспечения, их обнаружением, эксплуатацией и защитой от них на архитектурах x86 и amd64. Рассматриваются типовые варианты уязвимостей целочисленного переполнения, переполнения буфера в стеке и куче, использования после освобождения, уязвимости использования неправильного типа. Изучаются на примерах возможности их эксплуатации на актуальных версиях программного обеспечения и операционных систем Windows, Linux. А также подробно рассматриваются основные механизмы защиты от эксплуатации уязвимостей, предоставляемые данными операционными системами и популярными компиляторами Visual C++/gcc актуальных версий.

Весенний семестр 2017-18

1. **Теоретико-числовые алгоритмы в криптографии**, *Черепнёв Михаил Алексеевич, четверг 10:35, ауд. 604*

2. **Теория кодирования и криптография**, *Чижов Иван Владимирович*

3. **Построение и анализ алгоритмов**, *каф. АЯ, профессор, д.т.н. Ульянов Михаил Васильевич*

Осенний семестр 2017-18

Введение в p-адический анализ и его криптографические приложения, *Анашин Владимир Сергеевич , среда, 16:20, ауд. 604*