АННОТАЦИЯ рабочей программы дисциплины

ФТД.В.01 «МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»

Направление подготовки/специальность 10.04.01 Информационная безопасность

Объем трудоемкости: 2 зачетных единицы.

Цель дисциплины:

Целью изучения дисциплины «Методы и средства криптографической защиты информации» является изложение основополагающих принципов защиты информации с помощью криптографических методов и средств, а также примеров реализации этих методов на практике.

Задачи дисциплины:

Основные задачи освоения дисциплины:

- формирование целостного представления о современных организационных, технических, алгоритмических и других методах и средствах защиты компьютерной информации, используемых в современных криптосистемах, знакомство с законодательством и стандартами в этой области.

В результате освоения дисциплины студент должен:

Знать:

- правовые основы защиты компьютерной информации,
- математические основы криптографии
- организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях,
- стандарты, модели и методы шифрования,
- методы идентификации пользователей,
- основы инфраструктуры систем, построенных с использованием публичных и секретных ключе.

Уметь:

- применять известные методы и средства поддержки информационной безопасности в компьютерных системах,
- проводить сравнительный анализ, выбирать методы и средства,
- оценивать уровень защиты информационных ресурсов в прикладных системах;

Иметь навыки (приобрести опыт):

- передачи конфиденциальной информации по каналам связи,
- установления подлинности передаваемых сообщений и хранимой информации (документов, баз данных)
- выбирать методы и средства защиты информации.

Место дисциплины в структуре образовательной программы:

Курс «Методы и средства криптографической защиты информации» относится к части, формируемой участниками образовательных отношений блока Б1 Дисциплины (модули) и является обязательной.

Для изучения дисциплины студент должен владеть знаниями, умениями и навыками по дисциплинам: «Алгебра», «Дискретная математика», «Теория графов и ее приложения», «Комбинаторный анализ», «Безопасность операционных систем», «Теория алгоритмов и вычислительных процессов», «Программирование в компьютерных сетях», «Криптографические протоколы», с которыми дисциплина связана логически и содержательно-методически.

Дисциплина предшествует изучению дисциплин: «Безопасные методы извлечения информации из сетевых источников», «Разработка и реализация проектов в сфере информационной безопасности».

Требования к уровню освоения дисциплины

Изучение данной учебной дисциплины направлено на формирование у обучающихся универсальных/ общепрофессиональных/ профессиональных компетенций (УК/ОПК/ПК):

Код и наименование индикатора*	Результаты обучения по дисциплине *(знает, умеет, владеет (навыки и/или опыт деятельности))*
ПК-1 Способен осуществлять экспериментальные исследования в области криптографических и технических систем и средств обеспечения информационной безопасности	
ПК-1.1. Знает методы, применяемые при исследовании криптографических и технических систем и средств обеспечения информационной безопасности	Знание методов реализации систем защиты информации и действующих политик безопасности в компьютерных системах.
ПК-1.2. Умеет проводить экспериментальные исследования в области криптографических и технических систем и средств обеспечения информационной безопасности	Умеет применять математические методы при исследовании криптографических алгоритмов
ПК-1.3. Владеет практическими навыками представления результатов экспериментальных исследований в области криптографических и технических систем и средств обеспечения информационной безопасности.	Владеет методиками оценки эффективности реализации систем защиты информации и навыками работы с программными средствами общего и специального назначения.

Основные разделы дисциплины:
Встроенные средства обеспечения безопасности распространенных операционных систем и серверов различных сетевых протоколов, криптографические методы защиты информации в компьютерных системах и сетях, стохастические методы защиты информации.

Курсовые работы:
Учебным планом не предусмотрены.

.

Форма проведения аттестации по дисциплине: экзамен.

Основная литература

1. Торстейнсон, П. Криптография и безопасность в технологии .NET : руководство / П. Торстейнсон, Г. А. Ганеш ; перевод с англ. В. Д. Хорева под редакцией С. М. Молявко. - 5-е изд. (эл.). - Москва : Лаборатория знаний, 2024. - 482 с. - URL: https://e.lanbook.com/book/418025 (дата обращения: 17.01.2025). - Режим доступа: для авториз. пользователей. - ISBN 978-5-93208-734-3. - Текст : электронный.
2. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. - 2-е изд., испр. - Москва : Юрайт, 2022. - 473 с. - URL: https://urait.ru/bcode/489242 (дата обращения: 26.01.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-534-12474-3. - Текст : электронный.
3. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. - Москва : Юрайт, 2022. - 349 с. - URL: https://urait.ru/bcode/489919 (дата обращения: 30.05.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-534-02883-6. - Текст : электронный.

Составитель:
канд, техн, наук,
доцент кафедры ВТ ФКТ и ПМ Руденко О.В.