МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М.В.Ломоносова»

«Утверждаю»

Декан факультета ВМК МГУ
имени М.В. Ломоносова

академик _____ Е.И. Моисеев

«___» _____ 20 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Теоретико-кодовые конструкции в криптографии»

Уровень высшего образования – подготовка научно-педагогических кадров в аспирантуре

Направление подготовки – 10.06.01 «Информационная безопасность»

Направленность (профиль) – «Методы и системы защиты информации, информационная безопасность» (05.13.19)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

1. НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ

Теоретико-кодовые конструкции в криптографии

2. УРОВЕНЬ ВЫСШЕГО ОБРАЗОВАНИЯ

Подготовка научно-педагогических кадров в аспирантуре.

3. НАПРАВЛЕНИЕ ПОДГОТОВКИ, НАПРАВЛЕННОСТЬ (ПРОФИЛЬ) ПОДГОТОВКИ

Направление 10.06.01 «Информационная безопасность». Направленность (профиль) «Методы и системы защиты информации, информационная безопасность» (05.13.19).

4. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к специальным дисциплинам вариативной части образовательной программы и является обязательной для освоения в 1-м семестре обучения.

5. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательной программы:

Формируемые компетенции	Планируемые результаты обучения
Способность собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (СПК-2)	З1(СПК-2) ЗНАТЬ Средства обеспечения информационной безопасности. У1(СПК-2) УМЕТЬ провести анализ исходных данных для

	проектирования подсистем и средств обеспечения информационной безопасности В1(СПК-2) ВЛАДЕТЬ Навыками сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности
Способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности (ОПК-3)	З1 (ОПК-3) ЗНАТЬ принципы управления доступом в компьютерных системах, современные методы защиты информации при передаче ее по каналам связи, современные стандарты информационной безопасности У1(ОПК-3) УМЕТЬ: обосновать степень соответствия защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.
Способностью формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	З1(ОПК-1) ЗНАТЬ научные задачи в области обеспечения информационной безопасности

(ОПК-1);	У1(ОПК-1) УМЕТЬ: применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность В1(ОПК-1) ВЛАДЕТЬ: Навыками внедрения полученных результатов в практическую деятельность
Владение современными методами построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также методами разработки и реализации алгоритмов их решения на основе фундаментальных знаний в области математики и информатики (ПК-1)	З1 (ПК-1) ЗНАТЬ: современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения У1 (ПК-1) УМЕТЬ: применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения

	В1 (ПК-1) ВЛАДЕТЬ: навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методов разработки и реализации алгоритмов их решения
Способность разрабатывать и реализовывать алгоритмы организации работы современных вычислительных комплексов и компьютерных сетей (ПК-2)	З1 (ПК-2) ЗНАТЬ: современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения У1 (ПК-2) УМЕТЬ: применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения В1 (ПК-2) ВЛАДЕТЬ: навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и

	компьютерных сетей последнего поколения

Оценочные средства для промежуточной аттестации приведены в Приложении.

6. ОБЪЕМ ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетных единицы, всего 108 часов.

24 часов составляет контактная работа с преподавателем – 22 часа занятий лекционного типа, 0 часов занятий семинарского типа (семинары, научно-практические занятия, лабораторные работы и т.п.), 0 часов индивидуальных консультаций, 0 часа мероприятий текущего контроля успеваемости, 0 часа групповых консультаций, 2 часа мероприятий промежуточной аттестации.

84 часов составляет самостоятельная работа аспиранта.

7. ВХОДНЫЕ ТРЕБОВАНИЯ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Учащиеся должны владеть знаниями по операционным системам, компьютерным сетям, базам данных, дискретной математике и основам кибернетики в объеме, соответствующем основным образовательным программам бакалавриата и магистратуры по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки».

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе обучения используется программный пакет Beamer для подготовки слайдов лекций в среде LaTeX, программное средство просмотра pdf-файлов Adobe Reader, программное средство просмотра презентаций MS Power Point 2016.

9. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

В курсе рассматриваются основные проблемы и задачи, связанные с разработкой и анализом симметричных шифров. Основное внимание уделено программно-реализуемым шифрам потокового типа, строению основных блоков и узлов таких шифров, методам синтеза и анализа соответствующих криптографических примитивов, математической теории, на которой основаны данные методы.

Наименование и краткое содержание разделов и тем дисциплины (модуля), форма промежуточной аттестации по дисциплине (модулю)	Всего (часы)	В том числе								
		Контактная работа (работа во взаимодействии с преподавателем), часы из них						Самостоятельная работа обучающегося, часы из них		
		Занятия лекционного типа	Занятия семинарского типа	Групповые консультации	Индивидуальные консультации	Учебные занятия, направленные на проведение текущего контроля успеваемости (коллоквиумы, практические контрольные занятия и др)*	Всего	Выполнение домашних заданий	Подготовка рефератов и т.п..	Всего
Тема 1. Основные понятия теории линейных кодов, исправляющих ошибки Понятия кода, линейного кода над конечным полем. Основные параметры линейного кода: длина, размерность, кодовое расстояние. Порождающая и проверочная матрица линейного кода. Связь исправляющей способности кода и кодового расстояния. Связь кодового расстояния и параметров проверочной матрицы. Граница Хэмминга, граница Варшамова-Гильберта, граница Синглтона.	6	2	-	-	-		2	4	-	4
Тема 2. Кодовые криптосистемы типа Мак-Элиса и типа	26	6	-	-	-	-	6	-	20	20

Нидеррайтера Общая конструкция криптосистемы типа Мак-Элиса на основе произвольного линейного кода, имеющего достаточно эффективные алгоритмы декодирования. Атаки с использованием связанных шифр-текстов на такого типа криптосистемы. Обоснование и оценка сложности такого типа атак. Общая конструкция криптосистемы типа Нидеррайтера. Проблема нумерации двоичных векторов фиксированного веса Хэмминга. Основные подходы её решения. Оценка сложности алгоритмов нумерации таких векторов. Вопросы эффективной программной реализации такого рода криптосистем.										
Тема 3. Двоичные коды Гоппы, классическая криптосистема Мак-Элиса. Конструкция двоичных кодов Гоппы на основе рациональных функций над конечным полем. Вывод явного вида проверочной матрицы. Связь кодов Гоппы и альтернатных кодов, построенных их кодов Рида—Соломона. Граница на кодовое расстояние двоичных кодов Гоппы. Различные виды кодов Гоппы: неприводимые и сепарабельные. Граница на кодовое расстояние сепарабельных кодов Годов. Алгоритм Паттерсона декодирования двоичных	32	12	-	-	-	-	12	20	-	20

неприводимых кодов Гоппы. Использование алгоритма Берлекемпа-Мэсси для декодирования двоичных сепарабельных кодов Гоппы. Примера построения кодов Гоппы. Общая конструкция криптосистемы Мак-Элиса и криптосистемы Нидеррайтера на сепарабельных кодах Гоппы. Оценка сложности алгоритмов генерации ключей, шифрования и расшифрования.										
Тема 4. Основные методы криптоанализа кодовых криптосистем. Два типа атака на кодовые криптосистемы: атаки декодирования, структурные атаки. Связь атак декодирования с задачей поиска слов малого веса. Атаки декодирования Стерна и её сложность. Возможная структурная атака на криптосистемы, построенные на основе двоичных сепарабельных кодов Гоппы.	42	2	-	-	-	-	2	30	10	40
5. Промежуточная аттестация – устный экзамен	2	2						0		
Итого	108	24						84		

10. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ УЧАЩИХСЯ

Самостоятельная работа учащихся состоит в изучении лекционного материала, учебно-методической литературы, подготовки к текущему контролю и промежуточной аттестации.

Литература для самостоятельной работы студентов в соответствии с тематическим планом .

Тема 1 «Основные понятия теории линейных кодов, исправляющих ошибки»

- ✓ Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. - М.: Связь, 1979
- ✓ Берлекэмп Э. Алгебраическая теория кодирования. М.:Мир. 1971. 477 с.
- ✓ Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. - М.: Мир, 1976
- ✓ Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования. М.: Мир. 1978. 576 с.

Тема 2 «Кодовые криптосистемы типа Мак-Элиса и типа Нидеррайтера»

- ✓ Ван Тилборг Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. М.: Мир, 2006. — 471 с.
- ✓ Robert J. McEliece. "A public-key cryptosystem based on algebraic coding theory." Jet Propulsion Laboratory DSN Progress Report 42–44, 114–116. http://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF
- ✓ Harald Niederreiter. "Knapsack-type cryptosystems and algebraic coding theory." Problems of Control and Information Theory 15, 19–34. Problemy Upravlenija i Teorii Informacii 15, 159–166.
- ✓ Nicolas Sendrier. "Efficient generation of binary words of given weight." Pages 184–187 in: Colin Boyd (editor). Cryptography and Coding, 5th IMA conference, Cirencester, UK, December 18–20, 1995, proceedings. Lecture Notes in Computer Science 1025. Springer. ISBN 3-540-60693-9. http://www.springerlink.com/content/y43w30176331547m/fulltext.pdf
- ✓ Nicolas Sendrier. "Encoding information into constant weight words." Pages 435–438 in: Information theory, 2005. ISIT 2005. Proceedings. IEEE. http://ieeexplore.ieee.org/iel5/10215/32581/01523371.pdf?arnumber=1523371
- ✓ Thomas A. Berson. "Failure of the McEliece public-key cryptosystem under message-resend and related-message attack." Pages 213–220 in: Burton S. Kaliski, Jr. (editor). Advances in Cryptology—CRYPTO '97. 17th annual international cryptology conference, Santa Barbara, California, USA, August 17–21, 1997, proceedings. Lecture Notes in Computer Science 1294. Springer. http://www.springerlink.com/index/g6708p04m618g7r1.pdf
- ✓ Bhaskar Biswas, Nicolas Sendrier. "McEliece cryptosystem implementation: theory and practice." Pages 47–62 in: Johannes Buchmann, Jintai Ding (editors). Post-quantum cryptography, second international workshop, PQCrypto 2008, Cincinnati, OH, USA, October 17–19, 2008, proceedings. Lecture Notes in Computer Science 5299. Springer. http://www.springerlink.com/content/708316211158tt3g/
- ✓ Stefan Heyse. "Code-based cryptography: Implementing the McEliece scheme in reconfigurable hardware." Diploma thesis, Ruhr Universität Bochum. http://www.crypto.rub.de/imperia/md/content/texte/theses/da_heyse.pdf

✓ Thomas Eisenbarth, Tim Güneysu, Stefan Heyse, Christof Paar. "MicroEliece: McEliece for embedded devices." Pages 49–64 in: CHES '09: Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems, 2009. Lecture Notes in Computer Science 5747. Springer. http://www.springerlink.com/content/44818244160740r1/
✓ Stefan Heyse. "Low-Reiter: Niederreiter encryption scheme for embedded microcontrollers." Pages 165–181 in: Nicolas Sendrier (editor). Post-Quantum Cryptography, Third international workshop, PQCrypto 2010. Lecture Notes in Computer Science 6061. Springer. http://www.springerlink.com/content/uj3418uw97107012/
✓ Falko Strenzke. "A smart card implementation of the McEliece PKC." Pages 47–59 in: Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices. Lecture Notes in Computer Science 6033. Springer. http://www.springerlink.com/content/q241525l8t551182/
✓ Falko Strenzke. "How to implement the public key operations in code-based cryptography on memory-constrained devices." Cryptology ePrint Archive, Report 2010/465, 2010. http://eprint.iacr.org/2010/465/
✓ Stefan Heyse. "Implementation of McEliece Based on Quasi-dyadic Goppa Codes for Embedded Devices". Pages 143–162 in: Post-Quantum Cryptography 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011, proceedings Lecture Notes in Computer Science 7071. Springer. http://www.springerlink.com/content/1111u8m45r2215n5/
✓ Paulo S. L. M. Barreto, Richard Lindner, Rafael Misoczki. "Monoidic Codes in Cryptography." Pages 179–199 in: Post-Quantum Cryptography 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011, proceedings Lecture Notes in Computer Science 7071. Springer. http://www.springerlink.com/content/9v23w853vk80n024/
✓ Daniel J. Bernstein. "Simplified high-speed high-distance list decoding for alternant codes." Pages 200–216 in: Post-Quantum Cryptography 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011, proceedings Lecture Notes in Computer Science 7071. Springer. https://cr.yp.to/papers.html#simplelist

Тема 3 «Двоичные коды Гоппы, классическая криптосистема Мак-Элиса»

✓ Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. - М.: Связь, 1979
✓ Гоппа В.Д. Коды на алгебраических кривых, ДАН СССР 259 (1981):6, 1289-1290
✓ Nicholas J. Patterson. "The algebraic decoding of Goppa codes." IEEE Transactions on Information Theory IT-21, 203–207. MR 51:15175. http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/18/22749/01057049.pdf?arnumber=1057049
✓ Elia, Michele & Viterbo, Emanuele & Bertinetti, G. (1999). Decoding of binary separable Goppa codes using Berlekamp-Massey algorithm. Electronics Letters. 35. 1720 - 1721. 10.1049/el:19991190.
✓ Daniel J. Bernstein. "List decoding for binary Goppa codes." Pages 62–80 in: Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang Huaxiong Wang, Chaoping Xing (editors). Coding and Cryptology: Third International Workshop, IWCC 2011, Qingdao, China, May 30-June 3, 2011, proceedings. Lecture Notes in Computer Science 6639. Springer. https://cr.yp.to/papers.html#goppalist

✓ Paulo S. L. M. Barreto, Richard Lindner, Rafael Misoczki. "Decoding square-free Goppa codes over Fp." Cryptology ePrint Archive, Report 2010/372, 2010. http://eprint.iacr.org/2010/372/

Тема 4 «Основные методы криптоанализа кодовых криптосистем»

✓ Robert J. McEliece. "A public-key cryptosystem based on algebraic coding theory." Jet Propulsion Laboratory DSN Progress Report 42–44, 114–116. http://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF

✓ Dilip V. Sarwate. "On the complexity of decoding Goppa codes." IEEE Transactions on Information Theory 23, 515–516. http://www.ifp.illinois.edu/~sarwate/pubs/Sarwate77Complexity.pdf

✓ Jacques Stern. "A method for finding codewords of small weight." MR 1023683. Pages 106–113 in: Gerard D. Cohen, Jacques Wolfmann (editors). Coding theory and applications. Proceedings of the Third International Colloquium on Coding Theory held in Toulon, November 2–4, 1988. Lecture Notes in Computer Science 388, Springer. ISBN 0-387-51643-3. MR 90i:94001. http://www.springerlink.com/index/7g665155m26n9g72.pdf

✓ Anne Canteaut, Nicolas Sendrier. "Cryptanalysis of the original McEliece cryptosystem." MR 2000i:94042. Pages 187–199 in: Kazuo Ohta, Dingyi Pei (editors). Advances in cryptology—ASIACRYPT'98. Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security held in Beijing, October 18–22, 1998. Lecture Notes in Computer Science 1514, Springer. ISBN 3-540-65109-8. http://www.springerlink.com/index/64RNX94MG0Y32KNG.pdf

✓ Anne Canteaut, Florent Chabaud. "A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511." IEEE Transactions on Information Theory 44, 367–378. MR 98m:94043. ftp://ftp.inria.fr/INRIA/tech-reports/RR/RR-2685.ps.gz

✓ Anne Canteaut, Herve Chabanne. "A further improvement of the work factor in an attempt at breaking McEliece's cryptosystem." In: Pascale Charpin (editor). EUROCODE 94. http://www.inria.fr/rrrt/rr-2227.html

✓ Alexei E. Ashikhmin, Alexander Barg. "Minimal vectors in linear codes." IEEE Transactions on Information Theory 44, 2010–2017. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=705584

11. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ

Основная литература

1. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. - М.: Связь, 1979
2. Берлекэмп Э. Алгебраическая теория кодирования. М.:Мир. 1971. 477 с.
3. Ван Тилборг Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. М.: Мир, 2006. — 471 с.
4. Robert J. McEliece. "A public-key cryptosystem based on algebraic coding theory." Jet Propulsion Laboratory DSN Progress Report 42–44, 114–116. http://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF
5. Harald Niederreiter. "Knapsack-type cryptosystems and algebraic coding theory." Problems of Control and Information Theory 15, 19–34. Problemy Upravlenija i Teorii Informacii 15, 159–166.
6. Nicolas Sendrier. "Efficient generation of binary words of given weight." Pages 184–187 in: Colin Boyd (editor). Cryptography and Coding, 5th IMA conference, Cirencester, UK, December 18–20, 1995, proceedings. Lecture Notes in Computer Science 1025. Springer. ISBN 3-540-60693-9. http://www.springerlink.com/content/y43w30176331547m/fulltext.pdf
7. Nicolas Sendrier. "Encoding information into constant weight words." Pages 435–438 in: Information theory, 2005. ISIT 2005. Proceedings. IEEE. http://ieeexplore.ieee.org/iel5/10215/32581/01523371.pdf?arnumber=1523371
8. Thomas A. Berson. "Failure of the McEliece public-key cryptosystem under message-resend and related-message attack." Pages 213–220 in: Burton S. Kaliski, Jr. (editor). Advances in Cryptology—CRYPTO '97. 17th annual international cryptology conference, Santa Barbara, California, USA, August 17–21, 1997, proceedings. Lecture Notes in Computer Science 1294. Springer. http://www.springerlink.com/index/g6708p04m618g7r1.pdf
9. Bhaskar Biswas, Nicolas Sendrier. "McEliece cryptosystem implementation: theory and practice." Pages 47–62 in: Johannes Buchmann, Jintai Ding (editors). Post-quantum cryptography, second international workshop, PQCrypto 2008, Cincinnati, OH, USA, October 17–19, 2008, proceedings. Lecture Notes in Computer Science 5299. Springer. http://www.springerlink.com/content/708316211158tt3g/
10. Stefan Heyse. "Code-based cryptography: Implementing the McEliece scheme in reconfigurable hardware." Diploma thesis, Ruhr Universität Bochum. http://www.crypto.rub.de/imperia/md/content/texte/theses/da_heyse.pdf
11. Thomas Eisenbarth, Tim Güneysu, Stefan Heyse, Christof Paar. "MicroEliece: McEliece for embedded devices." Pages 49–64 in: CHES '09: Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems, 2009. Lecture Notes in Computer Science 5747. Springer. http://www.springerlink.com/content/44818244160740r1/
12. Stefan Heyse. "Low-Reiter: Niederreiter encryption scheme for embedded microcontrollers." Pages 165–181 in: Nicolas Sendrier (editor). Post-Quantum Cryptography, Third international workshop, PQCrypto 2010. Lecture Notes in Computer Science 6061. Springer. http://www.springerlink.com/content/uj3418uw97107012/
13. Falko Strenzke. "A smart card implementation of the McEliece PKC." Pages 47–59 in: Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices. Lecture Notes in Computer Science 6033. Springer. http://www.springerlink.com/content/q24152518t551182/

14. Falko Strenzke. "How to implement the public key operations in code-based cryptography on memory-constrained devices." Cryptology ePrint Archive, Report 2010/465, 2010. http://eprint.iacr.org/2010/465/
15. Stefan Heyse. "Implementation of McEliece Based on Quasi-dyadic Goppa Codes for Embedded Devices". Pages 143–162 in: Post-Quantum Cryptography 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011, proceedings Lecture Notes in Computer Science 7071. Springer. http://www.springerlink.com/content/1111u8m45r2215n5/
16. Paulo S. L. M. Barreto, Richard Lindner, Rafael Misoczki. "Monoidic Codes in Cryptography." Pages 179–199 in: Post-Quantum Cryptography 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011, proceedings Lecture Notes in Computer Science 7071. Springer. http://www.springerlink.com/content/9v23w853vk80n024/
17. Daniel J. Bernstein. "Simplified high-speed high-distance list decoding for alternant codes." Pages 200–216 in: Post-Quantum Cryptography 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011, proceedings Lecture Notes in Computer Science 7071. Springer. https://cr.yp.to/papers.html#simplelist
18. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. - М.: Связь, 1979
19. Гоппа В.Д. Коды на алгебраических кривых, ДАН СССР 259 (1981):6, 1289-1290
20. Nicholas J. Patterson. "The algebraic decoding of Goppa codes." IEEE Transactions on Information Theory IT-21, 203–207. MR 51:15175. http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/18/22749/01057049.pdf?arnumber=1057049
21. Elia, Michele & Viterbo, Emanuele & Bertinetti, G. (1999). Decoding of binary separable Goppa codes using Berlekamp-Massey algorithm. Electronics Letters. 35. 1720 - 1721. 10.1049/el:19991190.
22. Robert J. McEliece. "A public-key cryptosystem based on algebraic coding theory." Jet Propulsion Laboratory DSN Progress Report 42–44, 114–116. http://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF
23. Dilip V. Sarwate. "On the complexity of decoding Goppa codes." IEEE Transactions on Information Theory 23, 515–516. http://www.ifp.illinois.edu/~sarwate/pubs/Sarwate77Complexity.pdf
24. Jacques Stern. "A method for finding codewords of small weight." MR 1023683. Pages 106–113 in: Gerard D. Cohen, Jacques Wolfmann (editors). Coding theory and applications. Proceedings of the Third International Colloquium on Coding Theory held in Toulon, November 2–4, 1988. Lecture Notes in Computer Science 388, Springer. ISBN 0-387-51643-3. MR 90i:94001. http://www.springerlink.com/index/7g665155m26n9g72.pdf

Дополнительная литература

1. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. - М.: Мир, 1976

2. Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования. М.: Мир. 1978. 576 с.
3. Bhaskar Biswas, Nicolas Sendrier. "McEliece cryptosystem implementation: theory and practice." Pages 47–62 in: Johannes Buchmann, Jintai Ding (editors). Post-quantum cryptography, second international workshop, PQCrypto 2008, Cincinnati, OH, USA, October 17–19, 2008, proceedings. Lecture Notes in Computer Science 5299. Springer. http://www.springerlink.com/content/708316211158tt3g/
4. Stefan Heyse. "Code-based cryptography: Implementing the McEliece scheme in reconfigurable hardware." Diploma thesis, Ruhr Universität Bochum. http://www.crypto.rub.de/imperia/md/content/texte/theses/da_heyse.pdf
5. Thomas Eisenbarth, Tim Güneysu, Stefan Heyse, Christof Paar. "MicroEliece: McEliece for embedded devices." Pages 49–64 in: CHES '09: Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems, 2009. Lecture Notes in Computer Science 5747. Springer. http://www.springerlink.com/content/44818244160740r1/
6. Stefan Heyse. "Low-Reiter: Niederreiter encryption scheme for embedded microcontrollers." Pages 165–181 in: Nicolas Sendrier (editor). Post-Quantum Cryptography, Third international workshop, PQCrypto 2010. Lecture Notes in Computer Science 6061. Springer. http://www.springerlink.com/content/uj3418uw97107012/
7. Falko Strenzke. "A smart card implementation of the McEliece PKC." Pages 47–59 in: Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices. Lecture Notes in Computer Science 6033. Springer. http://www.springerlink.com/content/q241525l8t551182/
8. Falko Strenzke. "How to implement the public key operations in code-based cryptography on memory-constrained devices." Cryptology ePrint Archive, Report 2010/465, 2010. http://eprint.iacr.org/2010/465/
9. Stefan Heyse. "Implementation of McEliece Based on Quasi-dyadic Goppa Codes for Embedded Devices". Pages 143–162 in: Post-Quantum Cryptography 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011, proceedings Lecture Notes in Computer Science 7071. Springer. http://www.springerlink.com/content/1111u8m45r2215n5/
10. Paulo S. L. M. Barreto, Richard Lindner, Rafael Misoczki. "Monoidic Codes in Cryptography." Pages 179–199 in: Post-Quantum Cryptography 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011, proceedings Lecture Notes in Computer Science 7071. Springer. http://www.springerlink.com/content/9v23w853vk80n024/
11. Daniel J. Bernstein. "Simplified high-speed high-distance list decoding for alternant codes." Pages 200–216 in: Post-Quantum Cryptography 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011, proceedings Lecture Notes in Computer Science 7071. Springer. https://cr.yp.to/papers.html#simplelist
12. Daniel J. Bernstein. "List decoding for binary Goppa codes." Pages 62–80 in: Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang Huaxiong Wang, Chaoping Xing (editors). Coding and Cryptology: Third International Workshop, IWCC 2011, Qingdao, China, May 30-June 3, 2011, proceedings. Lecture Notes in Computer Science 6639. Springer. https://cr.yp.to/papers.html#goppalist

13. Paulo S. L. M. Barreto, Richard Lindner, Rafael Misoczki. "Decoding square-free Goppa codes over Fp." Cryptology ePrint Archive, Report 2010/372, 2010. http://eprint.iacr.org/2010/372/
14. Anne Canteaut, Nicolas Sendrier. "Cryptanalysis of the original McEliece cryptosystem." MR 2000i:94042. Pages 187–199 in: Kazuo Ohta, Dingyi Pei (editors). Advances in cryptology—ASIACRYPT'98. Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security held in Beijing, October 18–22, 1998. Lecture Notes in Computer Science 1514, Springer. ISBN 3-540-65109-8. http://www.springerlink.com/index/64RNX94MG0Y32KNG.pdf
15. Anne Canteaut, Florent Chabaud. "A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511." IEEE Transactions on Information Theory 44, 367–378. MR 98m:94043. ftp://ftp.inria.fr/INRIA/tech-reports/RR/RR-2685.ps.gz
16. Anne Canteaut, Herve Chabanne. "A further improvement of the work factor in an attempt at breaking McEliece's cryptosystem." In: Pascale Charpin (editor). EUROCODE 94. http://www.inria.fr/rrrt/rr-2227.html
17. Alexei E. Ashikhmin, Alexander Barg. "Minimal vectors in linear codes." IEEE Transactions on Information Theory 44, 2010–2017. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=705584

Ресурсы информационно-телекоммуникационной сети «Интернет»

1. www.google.com
2. http://pqcrypto.org/
3. https://link.springer.com/
4. http://eprint.iacr.org
5. https://arxiv.org/

Информационные технологии, используемые в процессе обучения

1. Программный пакет Beamer для подготовки слайдов лекций в среде LaTeX
2. Программное обеспечение для создания и просмотра pdf-документов Adobe Reader
3. Программное обеспечение для создания и просмотра презентаций MS Power Point

Активные и интерактивные формы проведения занятия

№ п\п	Тип занятия или внеаудиторной работы	Вид и тематика (название) интерактивного занятия
1	Лекция 11	Лекция-конференция на тему «Использование различных типов кодов для построения кодовых криптосистем»

Материально-техническая база

Для преподавания дисциплины требуется класс, оборудованный маркерной или меловой доской и проектором.

12. ЯЗЫК ПРЕПОДАВАНИЯ

Русский

13. РАЗРАБОТЧИК ПРОГРАММЫ, ПРЕПОДАВАТЕЛИ

к.ф.-м.н. Чижов Иван Владимирович

Приложение

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

«Теоретико-кодовые конструкции криптографии»

Средства для оценивания планируемых результатов обучения, критерии и показатели оценивания приведены ниже.

РЕЗУЛЬТАТ ОБУЧЕНИЯ по дисциплине (модулю)	КРИТЕРИИ и ПОКАЗАТЕЛИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТА ОБУЧЕНИЯ по дисциплине (модулю) *(критерии и показатели берутся из соответствующих карт компетенций, при этом пользуются либо традиционной системой оценивания, либо БРС)*					ОЦЕНОЧНЫЕ СРЕДСТВА
	1	2	3	4	5	
	Неудовлетворительно	Неудовлетвори-тельно	Удовлетвори-тельно	Хорошо	Отлично	
ЗНАТЬ: принципы управления доступом в компьютерных системах, современные методы защиты информации при передаче ее по каналам связи, современные стандарты информационной безопасности З1 (ОПК-3)	Отсутствие знаний	Фрагментарные представления о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, современных стандартах информационной безопасности	В целом сформированные, но неполные знания о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, современных стандартах информационной безопасности	Сформированные, но содержащие отдельные пробелы знания о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, современных стандартах информационной безопасности	Сформированные систематические знания о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, современных стандартах информационной безопасности	Устный экзамен
УМЕТЬ: обосновать степень соответствия	Отсутствие умений	Фрагментарные умения обоснования степени соответствия	В целом успешное, но не систематическое	Успешное, но содержащее отдельные	Сформированное умение обоснования степени соответствия	Контрольные работы

защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности. У1(ОПК-3)		защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.	умение обоснования степени соответствия защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.	пробелы умение обоснования степени соответствия защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.	защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.	
ЗНАТЬ: современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения З1 (ПК-1)	Отсутствие знаний	Фрагментарные представления о современных методах построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методах разработки и реализации алгоритмов их решения	В целом сформированные, но неполные знания о современных методах построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методах разработки и реализации алгоритмов их решения	Сформированные, но содержащие отдельные пробелы знания о современных методах построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методах разработки и реализации алгоритмов их решения	Сформированные систематические знания о современных методах построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методах разработки и реализации алгоритмов их решения	Устный экзамен
УМЕТЬ: применять	Отсутствие умений	Фрагментарные умения применять	В целом успешное, но не	Успешное, но содержащее	Сформированное умение применять	Контрольные работы

современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения У1 (ПК-1)		современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения	систематическое умение применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения	отдельные пробелы умение применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения	современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения	
ВЛАДЕТЬ: навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методов разработки и реализации алгоритмов их решения В1 (ПК-1)	Отсутствие навыков	Фрагментарное владение навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методов разработки и реализации алгоритмов их решения	В целом успешное, но не полное владение навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методов	Успешное, но содержащее отдельные пробелы владение навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных	Сформированное владение навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методов разработки и реализации алгоритмов их решения	Контрольные работы, реферат

			разработки и реализации алгоритмов их решения	методов разработки и реализации алгоритмов их решения		
ЗНАТЬ: современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения Код З1 (ПК-2)	Отсутствие знаний	Фрагментарные представления о современных методах разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	В целом сформированные, но неполные знания о современных методах разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Сформированные, но содержащие отдельные пробелы знания о современных методах разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Сформированные систематические знания о современных методах разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Устный экзамен
УМЕТЬ: применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения Код У1 (ПК-2)	Отсутствие умений	Фрагментарные умения применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	В целом успешное, но не систематическое умение применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Успешное, но содержащее отдельные пробелы умение применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего	Сформированное умение применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Устный экзамен

				поколения		
ВЛАДЕТЬ: навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения Код В1 (ПК-2)	Отсутствие навыков	Фрагментарное владение навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	В целом успешное, но не полное владение навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Успешное, но содержащее отдельные пробелы владение навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Сформированное владение навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Устный экзамен
ЗНАТЬ: научные задачи в области обеспечения информационной безопасности З1(ОПК-1)	Отсутствие знаний	Фрагментарные представления о научных задачах в области обеспечения информационной безопасности	В целом сформированные, но неполные знания о научных задачах в области обеспечения информационной безопасности	Сформированные, но содержащие отдельные пробелы о научных задачах в области обеспечения информационной безопасности	Сформированные систематические знания о научных задачах в области обеспечения информационной безопасности	Устный экзамен
УМЕТЬ: применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных	Отсутствие умений	Фрагментарные умения применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных	В целом успешное, но не систематическое умение применять для задачи в области обеспечения ИБ решения	Успешное, но содержащее отдельные пробелы умение применять для задачи в области обеспечения ИБ решения	Сформированное умение применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных	Устный экзамен

научных исследований, внедрять полученные результаты в практическую деятельность У1(ОПК-1)		научных исследований, внедрять полученные результаты в практическую деятельность	методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	научных исследований, внедрять полученные результаты в практическую деятельность	
ВЛАДЕТЬ: Навыками внедрения полученных результатов в практическую деятельность В1(ОПК-1)	Отсутствие навыков	Фрагментарное владение навыками внедрения полученных результатов в практическую деятельность	В целом успешное, но не полное владение навыками внедрения полученных результатов в практическую деятельность	Успешное, но содержащее отдельные пробелы владение навыками внедрения полученных результатов в практическую деятельность	Сформированное владение навыками внедрения полученных результатов в практическую деятельность	устный экзамен
ЗНАТЬ Средства обеспечения информационной безопасности З1(СПК-2)	Отсутствие знаний	Фрагментарные представления о средствах обеспечения информационной безопасности	В целом сформированные, но неполные знания о средствах обеспечения информационной безопасности	Сформированные, но содержащие отдельные пробелы о средствах обеспечения информационной безопасности	Сформированные систематические знания о средствах обеспечения информационной безопасности	Устный экзамен
УМЕТЬ провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной	Отсутствие умений	Фрагментарные умения проводить анализ исходных данных для проектирования подсистем и средств обеспечения	В целом успешное, но не систематическое умение проводить анализ исходных данных для проектирования	Успешное, но содержащее отдельные пробелы проводить анализ исходных данных для	Сформированное умение проводить анализ исходных данных для проектирования подсистем и средств обеспечения	Устный экзамен

безопасности У1(СПК-2)		информационной безопасности	подсистем и средств обеспечения информационной безопасности	проектирования подсистем и средств обеспечения информационной безопасности	информационной безопасности	
ВЛАДЕТЬ Навыками сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности В1(СПК-2)	Отсутствие навыков	Фрагментарное владение Навыками сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	В целом успешное, но не полное владение навыками сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Успешное, но содержащее отдельные пробелы владение навыками навыками сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Сформированное владение навыками навыками сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Устный экзамен

Фонды оценочных средств, необходимые для оценки результатов обучения

Каждый учащийся в процессе обучения готовит научный проект, который заключается в построении кодовой криптосистемы на основе какого-либо типа кодов. Для построенной кодовой криптосистемы должны быть указаны:

1) Алгоритм генерации ключей, оценка сложности
2) Открытый ключ
3) Секретный ключ
4) Алгоритм шифрования, оценка сложности
5) Алгоритм расшифрования, оценка сложности
6) Описываются возможные типа атак на криптосистему, известные из открытых источников.

Возможные типы кодов для научной работы:

1) Коды Хэмминга
2) Коды Рида—Маллера первого порядка
3) Коды Рида—Соломона
4) Расширенные коды Хэмминга
5) Эквидистантные коды (коды, дуальные к коду Хэмминга).

Методические материалы для проведения процедур оценивания результатов обучения

Особенности организации процесса обучения

Для эффективного освоения курса рекомендуется перед каждым занятие привести в порядок конспекты лекций. После каждого занятия рекомендуется найти и прочитать дополнительную литературу по теме лекции и прочитать свои конспекты.

Система контроля и оценивания

За выполнение научной работы выставляются баллы. Оценивается:

1) Полнота описания алгоритмов (<=1 балл)
2) Корректность описания алгоритмов (<=1 балл)
3) Корректность получения оценок сложности алгоритмов (<=1 балл)
4) Полнота описания возможных атака (<= 1 балл)
5) Библиография, посвящённая исследованию такого типа криптосистем (<= 1 балл).

По каждому параметру выставляется, которая равна доле полноты/корректности параметра. Далее все баллы суммируются и округляются. Полученная значение является итоговой оценкой.

Пример: 1) 1 2) 1 3) 0,7 4) 0,2 5) 1, в итоге

1 + 1 + 0, 7 + 0,2 + 1 = 3,7 -> оценка 4 (“хорошо”).

Структура и график контрольных мероприятий

Защита научной работы в конце семестра.