Федеральное государственное автономное образовательное учреждение высшего образования
"Национальный исследовательский университет "Высшая школа экономики"

МИЭМ
Департамент прикладной математики

Рабочая программа дисциплины
История криптографии

для образовательной программы 10.05.01 «Компьютерная безопасность»
направления подготовки 10.05.01 «Компьютерная безопасность»
специалитет

Разработчики программы:
Лось Алексей Борисович, к.т.н., доцент, e-mail: alos@hse.ru
Сорокин Александр Владимирович, asorokin@hse.ru

Одобрена на заседании Кафедры компьютерной безопасности «28» августа 2017 г.

Зав. Кафедрой А. Б. Лось _____

Рекомендована Академическим советом образовательной программы
«28»августа 2017 г., № протокола 6

Утверждена «28» августа 2017 г.
Академический руководитель образовательной программы
А. Б. Лось _____

Москва, 2017

1 Область применения и нормативные ссылки

Настоящая программа учебной дисциплины устанавливает минимальные требования к знаниям и умениям студента и определяет содержание и виды учебных занятий и отчетности.

Программа предназначена для преподавателей, ведущих данную дисциплину, учебных ассистентов и студентов специальности 10.05.01. «Компьютерная безопасность», обучающихся по специализации Математические методы защиты информации, изучающих дисциплину История криптографии.

Программа разработана в соответствии с:

- ОС ВО НИУ ВШЭ по специальности 10.05.01. «Компьютерная безопасность»;
- Образовательной программой специальности 10.05.01. «Компьютерная безопасность»;
- Рабочим учебным планом университета по специальности 10.05.01. «Компьютерная безопасность», специализации Математические методы защиты информации, утвержденным в 2016 г.

2 Цели освоения дисциплины

Целью освоения дисциплины История криптографии является формирование у студентов навыков, необходимых для решения следующих предусмотренных программой специальности 10.05.01. "Компьютерная безопасность" профессиональных задач:

- Разработка математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность объектов;
- Обоснование и выбор рационального решения по уровню обеспечения защищенности компьютерной системы с учетом заданных требований;
- Организация работ по выполнению требований режима защиты информации, в том числе обеспечению защиты информации ограниченного доступа (сведений, составляющих государственную тайну и конфиденциальной информации).

3 Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины студент должен:

Знать:

- Основные исторические этапы развития криптографии, ее влияние на ход развития событий;
- Простейшие типы шифров, их достоинства и недостатки, методы реализации;
- Методы криптоанализа простейших шифров;
- Методы оценки качества криптографической защиты;
- Современное состояние и области применения криптографических средств защиты информации.

Уметь:

- Применять на практике простейшие криптографические методы защиты информации;
- Применять на практике методы вскрытия простейших шифров;
- Оценивать качество криптографической защиты.

Иметь навыки (приобрести опыт):

- Применения простейших шифров;
- Криптоанализа простейших шифров;
- Формирования требований, предъявляемых к криптографическим средствам защиты информации.

В результате освоения дисциплины студент осваивает следующие компетенции:

Компетенция	Код по ФГОС/ НИУ	Дескрипторы – основные признаки освоения (показатели достижения результата)	Формы и методы обучения, способствующие формированию и развитию компетенции
Способность осознавать и учитывать социально значимые политические и экономические явления и процессы в профессиональной деятельности	ПК-1/ СЛК-М4	СД Способен формулировать требования к криптографическим средствам защиты информации в связи с социально значимыми политическими и экономическими явлениями Способен оценивать потенциальную стойкость криптографических систем защиты информации с учетом социально значимых явлений и процессов МЦ Обосновывает зависимость эволюции средств криптографической защиты информации от социально значимых политических и экономических событий и процессов	Лекционные занятия по дисциплине
Способность решать проблемы в профессиональной деятельности на основе анализа и синтеза	УК-5/ СК-Б4	РБ Знает основные типы простейших шифров Знает методы анализа простейших шифров СД Способен оценивать стойкость криптографических средств путем их анализа Способен создавать проекты новых криптографических средств путем синтеза МЦ Обосновывает важность качественного анализа криптографических средств перед их внедрением Объясняет переспективность разработки новых криптографических средств путем их синтеза из известных шифров	Лекции и семинарские занятия по дисциплине
Способность обеспечивать техническую, антивирусную, криптографическую защиту информации в компьютерных системах	ПК-18/ ИК-С12	РБ Знает основные категории криптографических средств защиты информации Знает основные классы современных криптографических средств МЦ Обосновывает важность использования криптографичеких средств защиты информации в информационных системах	Лекции основных разделов дисциплины

Компетенция	Код по ФГОС/ НИУ	Дескрипторы – основные признаки освоения (показатели достижения результата)	Формы и методы обучения, способствующие формированию и развитию компетенции
Способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем	ПК-21/ ИК-С15	РБ Знает основные типы простейших шифров Знает методы анализа простейших шифров Знает основные категории надежности криптографических средств Знает формальные требования к абсолютно стойким шифрам	Лекции разделов «Основные принципы изучения криптографических систем», «Понятие абсолютно стойкого шифра».
Способность разрабатывать алгоритмы, реализующие современные криптографические методы защиты информации	ПК-27/ ИК-С21сКБ	РБ Знает основные категории криптографических средств защиты информации Знает основные классы современных криптографических средств Знает конкретные алгоритмы представителей основных классов современных криптографических средств МЦ Обосновывает важность использования криптографичеких средств защиты информации в информационных системах	Лекции основных разделов дисциплины
Способность оценивать эффективность криптографических алгоритмов защиты информации на основе реализуемых ими математических методов	ПК-28/ ИК-С22сКБ	РБ Знает основные типы простейших шифров Знает методы анализа простейших шифров Знает основные категории надежности криптографических средств Знает формальные требования к абсолютно стойким шифрам Знает однонаправленные преобразования, на которых основываются современные криптографические системы СД Способен оценивать стойкость криптографических средств путем их анализа Способен строить математические модели криптографических алгоритмов защиты информации Способен делать заключения о стойкости криптографических алгоритмов на основе анализа их математических моделей МЦ Обосновывает важность каче-	Лекции и семинарские занятия

Компетенция	Код по ФГОС/ НИУ	Дескрипторы – основные признаки освоения (показатели достижения результата)	Формы и методы обучения, способствующие формированию и развитию компетенции
		ственного анализа криптографических средств перед их внедрением	

4 Место дисциплины в структуре образовательной программы

Дисциплина «История криптографии» относится к числу дисциплин профессионального цикла (Major)

Изучение данной дисциплины базируется на следующих дисциплинах:

- История отечества,
- Алгебра.

Для освоения учебной дисциплины, студенты должны владеть следующими знаниями и компетенциями:

- Знание основных исторических событий;
- Знание основных понятий и результатов в области теории групп и полей.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении следующих дисциплин:

- Криптографические методы защиты информации;
- Криптографические протоколы.

5 Тематический план учебной дисциплины

№	Название раздела	Всего часов	Аудиторные часы			Самостоятельная работа
			Лекции	Семинары	Практические занятия	
1.	Основные принципы изучения криптографических систем	8	2	2		4
2.	Эволюция криптографии до XIX века	38	12	14		12
3.	Криптография на основе принципов Керхгоффса: XIX – середина XX века	38	12	14		12
5.	Понятие абсолютно стойкого шифра	9	2	1		6
6.	Современные блочные системы шифрования	16	2	2		12
7.	Асимметричные системы шифрования	16	2	2		12
8.	Перспективы криптографии и криптоанализа	10	2	2		6

6 Формы контроля знаний студентов

Тип контроля	Форма контроля	1 год				Параметры
		1	2	3	4	
Текущий	Домашняя работа			*	*	
Текущий	Контрольная работа			9	8	Письменная работа 80 минут
Итоговый	Экзамен				+	Устный теоретический экзамен

6.1 Критерии оценки знаний, навыков

На текущем и итоговом контроле знаний, в объеме изученного материала, студент должен продемонстрировать знание основных этапов развития криптографии, влияния ее применения на ход исторических событий, особенностей исторических криптографических систем.

При выполнении контрольной работы и домашнего задания студент должен продемонстрировать:

- Способность реализовать и использовать основные виды исторических криптографических систем;
- Способность разрабатывать криптографические системы, аналогичные изученным, указывать слабости рассматриваемых криптографических систем, формулировать требования к криптографическим системам для достижения требуемой стойкости.

Контрольные работы проводятся за 1-2 недели до конца 3 и 4 модулей (ориентировочно 9 и 8 недели соответственно). На контрольной работе студенту предлагается самостоятельно, без использования справочных материалов, выполнить 5 заданий, каждое из которых оценивается 0 – 2 баллами. Переписывание контрольной работы, как правило, не предусматривается. Студент, по уважительной причине, подтвержденной документально, не выполнявший контрольную работу, может получить право выполнить ее на последней неделе модуля, при этом о таком намерении он обязан сообщить преподавателю немедленно после окончания вынужденного отсутствия на занятиях. В этом случае студентам, желающим воспользоваться таким правом, назначаются единые день и время, в которые проводится переписывание.

Домашние задания выдаются и проверяются на семинарских занятиях и оцениваются по 10-балльной шкале. Оценка за домашние задания $O_{д/з1}$, $O_{д/з2}$ рассчитывается как среднее арифметическое домашних заданий за 1 и 2 модуль. Способ округления оценок – арифметический (с недостатком при значениях первой цифры дробной части от «0» до «4» и с избытком при значениях первой цифры дробной части от «5» до «9»).

На итоговом контроле знаний студент должен продемонстрировать знания:

- Исторических этапов развития криптографических систем;
- Основных классов исторических и существующих криптографических систем, достоинств и недостатков каждого из них;
- Основных методов криптографического анализа различных классов исторических криптографических систем.

7 Содержание дисциплины

Разделы	**Темы**	
1		Основные принципы изучения криптографических систем

	1.1	Основные параметры криптографических систем
	1.2	Шифры замены
	1.3	Метод частотного анализа шифров простой замены
	1.4	Шифры перестановки
	1.5	Метод анализа шифров перестановки с конечной длиной блока
2.		Эволюция криптографии до XIX века
	2.1	Безключевая тайнопись древнего мира
	2.2	Криптографические системы античности
	2.3	Создание метода частотного анализа в арабском мире
	2.4	Методы усовершенствования шифра простой замены
	2.5	Шифры многоалфавитной замены
3		Криптография на основе принципов Керхгоффса: XIX – середина XX века
	3.1	Шифры Плейфера и «Два квадрата»
	3.2	Шифр Вижинера
	3.3	Криптоанализ шифра Вижинера
	3.4	Шифр Вернама
	3.5	Дисковый шифратор Джефферсона
	3.6	Криптография Первой мировой войны. Радиоперехват и телеграмма Циммермана
	3.7	Роторные шифровальные машины
	3.8	Криптоанализ шифровальной машины «Энигма»
4		Понятие абсолютно стойкого шифра
	4.1	Понятие «совершенного шифра» в работах Клода Шеннона
	4.2	Критерии абсолютно стойкого шифра
	4.3	Построение абсолютно стойкого шифра на основе шифра Вернама
5		Современные блочные системы шифрования
	5.1	Проект «Люцифер» исследования методов построения блочных шифров
	5.2	Сеть Фейстеля
	5.3	Шифры DES и «Магма»
	5.4	SP-сеть
	5.5	Шифры AES и «Кузнечик»
6		Асимметричные системы шифрования
	6.1	Принципы построения асимметричных системм шифрования
	6.2	Протокол Диффи-Хеллмана
	6.3	Криптосистема RSA
7		Перспективы криптографии и криптоанализа
	7.1	Проект PGP и распространение стойкой криптографии
	7.2	Перспективы криптоанализа
	7.3	Квантовая криптография и Sponge-конструкции

8 Образовательные технологии

Для проведения отдельных семинарских занятий применяется дисплейных класс с установленными программными эмуляторами различных криптографических средств, в частности роторных шифраторов, в том числе шифровальной машины «Энигма».

9 Порядок формирования оценок по дисциплине

Преподаватель оценивает работу студентов на семинарских занятиях: оценивается активность студентов в дискуссиях, правильность решения задач на семинаре, качество подготовки выступлений с докладами. Оценки за работу на семинарских занятиях преподаватель выставляет в рабочую

ведомость. Накопленная оценка по 10-ти балльной шкале за работу на семинарских занятиях определяется перед окончанием 4 модуля и перед итоговым контролем - $O_{аудиторная}$.

Накопленная оценка за текущий контроль учитывает результаты студента по текущему контролю следующим образом:

$$O_{накопленная} = 0{,}8 * O_{текущий} + 0{,}2 * O_{ауд}$$

где $O_{текущий}$ включает оценки за контрольную работу и домашние задания: $O_{к/р1}$, $O_{к/р2}$, $O_{д/з1}$, $O_{д/з2}$

$$O_{текущий} = 0{,}4 * O_{к/р1} + 0{,}2 * O_{д/з1} + 0{,}4\ O_{к/р2} + 0{,}2 * O_{д/з2};$$

Способ округления накопленной оценки текущего контроля: арифметический.

Результирующая оценка за дисциплину рассчитывается следующим образом:

$$O_{результ} = 0{,}7 * O_{накопл} + 0{,}3 *\cdot O_{экз}$$

Способ округления накопленной оценки итогового контроля в форме экзамена: арифметический.

На пересдаче студенту не предоставляется возможность получить дополнительный балл для компенсации оценки за текущий контроль.

10 Учебно-методическое и информационное обеспечение дисциплины

10.1 Основная литература

1. Сингх С., Книга шифров. Тайная история шифров и их расшифровки. - М.: Астрель, 2007. – 448 с.
2. Соболева Т. А. История шифровального дела в России. — М.: ОЛМА-ПРЕСС Образование, 2002. — 512 с.
3. Бабаш А. В., Шанкин Г. П. Криптография (аспекты защиты). — М .: СОЛОН-ПРЕСС, 2007. – 512 с.
4. Чмора А. Л. Современная прикладная криптография. – М.: “Гелиос АРВ”, 2001. – 256 с.

10.2 Дополнительная литература

1. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. - М.: “Гелиос АРВ”, 2001. – 480 с.

10.3 Программные средства

Для успешного освоения дисциплины, студент использует следующие программные средства:

- Программные эмуляторы роторных шифраторов, шифровальной машины «Энигма».

11 Материально-техническое обеспечение дисциплины

При проведении отдельных семинарских занятий используется дисплейный класс с установленными программными эмуляторами криптографических средств.

12 Примерный перечень вопросов к экзамену

1. Общее понятие шифра, элементы шифра.
2. Основные операции, используемые для построения шифров. Классы шифров на осное таких операций. Примеры представителей таких классов.
3. Шифр простой замены. Мощность ключевого множества для алфавита конечной длины. Методы криптоанализа шифра простой замены, основания для их применимости. Стойкость шифра простой замены.
4. Шифр простой перестановки. Мощность ключевого множества для блоков конечной длины. Криптоанализ шифра простой перестановки, основания для его реализации. Стойкость шифра простой перестановки.
5. Пути усиления шифра простой замены.
6. Шифр простой замены биграмм. Мощность ключевого множества для алфавита конечной длины. Методы криптоанализа шифра простой замены биграмм, основания для их применимости. Стойкость шифра простой замены биграмм.
7. Шифры Плейфера и «Два квадрата». Мощность ключевых множеств для алфавитов конечной длины, являющейся полным квадратом. Связь с мощностью ключевого множества шифра простой замены биграмм. Стойкость шифров Плейфера и «Два квадрата». Преимущества и недостатки по сравнению с шифром простой замены биграмм.
8. Шифр омофонной замены. Основные принципы построения. Стойкость относительно шифра простой замены. Методы криптоанализа шифра омофонной замены.
9. Шифр «Решетка Кардано». Мощность ключевого множества для блока конечной длины, являющейся полным квадратом. Связь с мощностью ключевого множества шифра простой перестановки для блока той же длины. Преимущества и недостатки по сравнению с шифром простой перестановки.
10. Диск Альберти. Различные режимы применения и стойкость по сравнению с шифром простой замены. Закономерности связи шифротекста и открытого текста в отдельных режимах.
10. Шифр Вижинера. Стойкость относительно шифра простой замены. Метод определения длины и символов короткого ключа для шифра Вижинера (тест Касисски).
11. Шифр Вижинера с длинным осмысленным ключом. Метод восстановления ключа и открытого текста по шифртексту.
12. Особенности применения шифров в военном деле. Требования к шифрам для военных на основе книги Керкгоффса «Военная криптография». Принцип Керкгоффса.
13. Дисковый шифратор Джефферсона и цилиндр Базери. Основные характеристики, мощность ключевого множества в зависимости от различных параметров. Взаимосвязь между открытым и зашифрованным текстом, сохраняющаяся при использовании шифратора Джефферсона.
14. Шифровальные машины первой половины XX века. Основные принципы создания, эволюция, основные представители. Достоинства и недостатки шифроваьных машин.
15. Роторные электромеханические шифраторы на примере машины «Энигма». Основные принципы построения, ключевые элементы, сохраняющиеся закономерности взаимосвязи между открытым и зашифрованным текстом. Основные подходы к криптоанализу «Энигмы».
16. Криптоанализ Энигмы.
17. Понятие абсолютно стойкого (идеального) шифра. Основные требования, метод построения путем модификации шифра Вижинера.
18. Современные блочные шифры. Основные принципы построения, примеры блочных шифров.
19. Шифры на основе сети Фейстеля – DES и шифр «Магма».
20. Шифры на основе SP-сети – «Rijndael» и «Кузнечик»
21. Понятие симметричных и асимметричных систем шифрования. Основные принципы построения и различия. Протокол выработки общего ключа Диффи-Хеллмана. Криптографическая система RSA.

20. Понятие электронной цифровой подписи. Принцип использования асимметричной системы шифрования в качестве системы генерации и проверки электронной цифровой подписи. Понятие функции хэширования.

21. Криптографическое средство PGP, история и устройство.

22. Понятие квантовой криптографии – принципы, протокол взаимодействия абонентов.