Федеральное государственное автономное образовательное учреждение высшего образования «Московский физико-технический институт (национальный исследовательский университет)»

УТВЕРЖДЕНО
Директор физтех-школы радиотехники и компьютерных технологий
А.В. Дворкович

Рабочая программа дисциплины (модуля)

по дисциплине: Защита информации
по направлению: Информатика и вычислительная техника
профиль подготовки: Компьютерные технологии и вычислительная техника
Физтех-школа Радиотехники и Компьютерных Технологий
кафедра радиотехники и систем управления
курс: 4
квалификация: бакалавр

Семестр, формы промежуточной аттестации: 7 (осенний) - Экзамен

Аудиторных часов: 60 всего, в том числе:
лекции: 30 час.
семинары: 30 час.
лабораторные занятия: 0 час.

Самостоятельная работа: 45 час.

Подготовка к экзамену: 30 час.

Всего часов: 135, всего зач. ед.: 3

Количество контрольных работ, заданий: 2

Программу составил: А.И. Колыбельников, доцент

Программа обсуждена на заседании кафедры радиотехники и систем управления 04.06.2020

Аннотация

Целью реализации курса «Защита информации» является совершенствование и приобретение профессиональных компетенций слушателей в сфере защиты информации. Курс охватывает широкий спектр современных методов защиты. На курсе рассматриваются основные методы криптографической защиты информации и управления доступом, даётся как исторический обзор, так и затрагиваются современные способы защиты и способ нейтрализации угроз на разных стадиях жизненного цикла информации. В рамках курса рассматривается классическая, квантовая и постквантовая криптография.

1. Цели и задачи

Цель дисциплины

дать студентам представление о фундаментальных принципах построения систем защиты информации.

Задачи дисциплины

- выработать у студентов представление о защите информации как о точной науке, основанной на Шенноновской теории информации;
- дать представление о существующих криптографических примитивах и протоколах, а также их современных реализациях (российских и международных стандартов);
- дать представление о применении теории групп и теории конечных полей в криптографии.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 Анализирует задачу, выделяя этапы ее решения, действия по решению задачи
	УК-1.2 Находит, критически анализирует и выбирает информацию, необходимую для решения поставленной задачи
	УК-1.3 Рассматривает различные варианты решения задачи, оценивает их преимущества и недостатки
	УК-1.4 Грамотно, логично, аргументированно формирует собственные суждения и оценки
	УК-1.5 Определяет и оценивает практические последствия возможных вариантов решения задачи
ОПК-1 Способен применять фундаментальные знания, полученные в области физико-математических и (или) естественных наук, и использовать их в профессиональной деятельности	ОПК-1.2 Способен строить математические модели, производить количественные расчеты и оценки
	ОПК-1.1 Способен анализировать поставленную задачу, намечать пути ее решения
	ОПК-1.3 Способен определять границы применимости полученных результатов
ОПК-4 Способен осуществлять сбор и обработку научно-технической и (или) технологической информации для решения фундаментальных и прикладных задач	ОПК-4.1 Владеет методами научного поиска и интеллектуального анализа информации при решении задач профессиональной деятельности
	ОПК-4.4 Владеет навыками работы с компьютером и компьютерными сетями с целью получения, хранения и обработки научной (технической, технологической) информации
ПК-4 Способен организовывать и управлять небольшим проектным коллективом, обеспечивать необходимое разделение ролей и обязанностей в ходе осуществления сложных проектов, связанных с созданием и использованием информационных технологий и систем	ПК-4.1 Знает методы управления большими и малыми проектами

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- общие принципы организации защиты информации;
- основы классической криптографии с секретным ключом;
- основы криптографии на открытых ключах;
- современные криптографические примитивы, математические основы их работы;
- простейшие, классические и современные криптографические протоколы, в том числе протоколы аутентификации и авторизации;
- основы криптоанализа примитивов и протоколов.

уметь:

- анализировать соответствие степени защищённости криптографических примитивов современному уровню развития криптоанализа;
- выбирать подходящие криптографические примитивы и протоколы для использования в информационных системах и процессах организации.

владеть:

- простейшими методами оценки надёжности информационных систем с использованием криптографических средств;
- навыками совместного выполнения проектов.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Информация как предмет защиты	2	6		5
2	Защита от угрозы нарушения конфиденциальности информации	4	4		5
3	Аутентификации сообщений и идентификации сторон	4	4		5
4	Криптография на открытых ключах	6	4		5
5	Обеспечение целостности	4	2		5
6	Квантовая и постквантовая криптография	2	2		5
7	Протоколы безопасного обмена данными	2	2		5
8	Проектирование систем защиты информации	2	2		5
9	Понятие о компьютерной безопасности	4	4		5
Итого часов		30	30		45
Подготовка к экзамену		30 час.			
Общая трудоёмкость		135 час., 3 зач.ед.			

4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 7 (Осенний)

1. Информация как предмет защиты

Основные определения курса «защита информации». Теоретические основы, введение в работы Шеннона по защите информации. Использование математического аппарата теории информации в качестве теоретического базиса защиты информации. Понятие об абсолютно защищённых системах. Краткий исторический обзор.

2. Защита от угрозы нарушения конфиденциальности информации

Блоковые и потоковые шифры. Генераторы криптографически стойких псевдослучайных последовательностей.

3. Аутентификации сообщений и идентификации сторон

Протоколы распространения ключей.

4. Криптография на открытых ключах

Обеспечение конфиденциальности и целостности информации с использованием криптосистем RSA, El Gamal и криптосистем на основе эллиптических кривых. Гомоморфное шифрование.

5. Обеспечение целостности

Криптографически стойкие хеш-функции. Государственный стандарт «СТРИБОГ». Семейство хэш-функций SHA.

6. Квантовая и постквантовая криптография

Квантовые алгоритмы распространения ключа. Постквантовая криптография.

7. Протоколы безопасного обмена данными

Протоколы Kerberos, TLS, IPsec.

8. Проектирование систем защиты информации

Нормативно-правовое регулирование разработки СЗИ и СКЗИ в РФ, международные стандарты. Подходы к формированию модели угроз и модели нарушителя. Подходы к формированию мер противодействия нарушителю.

9. Понятие о компьютерной безопасности

Уязвимости информационных систем и методы защиты от них. Примеры информационных компонентов и систем, направленных на выполнение целей по защите информации. Методы поиска уязвимостей и их устранение Цикл безопасной разработки. Управление рисками.

5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Необходимое оборудование для лекций:
- учебная аудитория, оснащенная компьютером и мультимедийным оборудованием (проектор, звуковая система).

Обеспечение самостоятельной работы:
- доступ в интернет;
- доступ к научным журналам по университетской подписке (IEEE, ACM и д.р.).

6.Перечень рекомендуемой литературы

Основная литература

1. Введение в криптографию [Текст] : [учеб. пособие для вузов] / под ред. В. В. Ященко .— 4-е изд., доп. — М. : МЦНМО, 2012 .— 348 с.

2. Криптографические методы защиты информации [Текст] / С. М. Владимиров [и др.] ; М-во образования и науки РФ, Моск. физ.-техн. ин-т (гос. ун-т), Каф. радиотехники и систем управления - М.МФТИ,2016

3. Защита информации [Текст] : учеб. пособие для вузов / Э. М. Габидулин, А. С. Кшевецкий, А. И. Колыбельников ; М-во образования и науки РФ, Моск. физ.-техн. ин-т (гос. ун-т .— М. : МФТИ, 2011 .— 262 с.

Дополнительная литература

1. Лекции по алгебраическому кодированию [Текст] : учеб. пособие для вузов / Э. М. Габидулин ; М-во образования и науки РФ, Моск. физ.-техн. ин-т (гос. ун-т) .— М. : МФТИ, 2015 .— 107 с.

2. Лекции по теории информации [Текст] : учеб. пособие для вузов / Э. М. Габидулин, Н. И. Пилипчук ; М-во образования и науки, Моск. физ.-техн. ин-т (гос. ун-т), Каф. радиотехники .— М. : Изд-во МФТИ, 2007 .— 214 с.

7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Не используются

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)

Не предусмотрено.

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Внимательно слушать и конспектировать лекции, самостоятельно решать контрольные задачи, которые лектор задаёт в конце каждой лекции, анализировать ошибки, приходить на консультации к преподавателю, решать задачи из домашних заданий по мере поступления лекционного материала, не откладывая на последние дни перед указанным в задании сроком сдачи, в дополнение к лекциям читать учебные пособия по данному предмету и разбирать решения типовых задач, которые в пособии приведены.

ПРИЛОЖЕНИЕ

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению: Информатика и вычислительная техника
профиль подготовки: Компьютерные технологии и вычислительная техника
Физтех-школа Радиотехники и Компьютерных Технологий
кафедра радиотехники и систем управления
курс: 4
квалификация: бакалавр

Семестр, формы промежуточной аттестации: 7 (осенний) - Экзамен

Разработчик: А.И. Колыбельников, доцент

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 Анализирует задачу, выделяя этапы ее решения, действия по решению задачи
	УК-1.2 Находит, критически анализирует и выбирает информацию, необходимую для решения поставленной задачи
	УК-1.3 Рассматривает различные варианты решения задачи, оценивает их преимущества и недостатки
	УК-1.4 Грамотно, логично, аргументированно формирует собственные суждения и оценки
	УК-1.5 Определяет и оценивает практические последствия возможных вариантов решения задачи
ОПК-1 Способен применять фундаментальные знания, полученные в области физико-математических и (или) естественных наук, и использовать их в профессиональной деятельности	ОПК-1.2 Способен строить математические модели, производить количественные расчеты и оценки
	ОПК-1.1 Способен анализировать поставленную задачу, намечать пути ее решения
	ОПК-1.3 Способен определять границы применимости полученных результатов
ОПК-4 Способен осуществлять сбор и обработку научно-технической и (или) технологической информации для решения фундаментальных и прикладных задач	ОПК-4.1 Владеет методами научного поиска и интеллектуального анализа информации при решении задач профессиональной деятельности
	ОПК-4.4 Владеет навыками работы с компьютером и компьютерными сетями с целью получения, хранения и обработки научной (технической, технологической) информации
ПК-4 Способен организовывать и управлять небольшим проектным коллективом, обеспечивать необходимое разделение ролей и обязанностей в ходе осуществления сложных проектов, связанных с созданием и использованием информационных технологий и систем	ПК-4.1 Знает методы управления большими и малыми проектами

2. Показатели оценивания компетенций

В результате изучения дисциплины «Защита информации» обучающийся должен:

знать:

- общие принципы организации защиты информации;
- основы классической криптографии с секретным ключом;
- основы криптографии на открытых ключах;
- современные криптографические примитивы, математические основы их работы;
- простейшие, классические и современные криптографические протоколы, в том числе протоколы аутентификации и авторизации;
- основы криптоанализа примитивов и протоколов.

уметь:

- анализировать соответствие степени защищённости криптографических примитивов современному уровню развития криптоанализа;
- выбирать подходящие криптографические примитивы и протоколы для использования в информационных системах и процессах организации.

владеть:

- простейшими методами оценки надёжности информационных систем с использованием криптографических средств;
- навыками совместного выполнения проектов.

3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

Наименование возможных тем курсовых работ (эссе):

1) Стеганография
2) Конфиденциальность
3) Анонимность
4) Хеш-функция
5) Целостность
6) Цифровая подпись
7) Подпись Нюберга-Руэппеля
8) Криптоанализ
9) Атака на основе шифротекста
10) Атака на основе открытых текстов
11) Атака на основе подобранного открытого текста
12) Атака на основе адаптивно подобранного открытого текста
13) Атака на основе подобранного шифротекста
14) Атака на основе подобранного ключа
15) Атака на основе связанных ключей
16) Бандитский криптоанализ
17) Социальная инженерия (безопасность)
18) side-channel криптоанализ
19) Дифференциальный криптоанализ
20) Линейный криптоанализ
21) Перебор по словарю
22) Полный перебор
23) Радужная таблица
24) Человек посередине (атака)
25) Шифрование
26) Поточный шифр
27) Генератор псевдослучайных чисел
28) Регистр сдвига с линейной обратной связью
29) Линейный конгруэнтный метод
30) Метод Фибоначчи с запаздываниями
31) Регистр сдвига с линейной обратной связью
32) Регистр сдвига с обобщённой обратной связью
33) Генератор Макларена — Марсальи
34) Криптографически стойкий генератор псевдослучайных чисел
35) Симметричные криптосистемы
36) Блочный шифр
37) Сеть Фейстеля
38) Лавинный эффект
39) Режим шифрования
40) AEAD Режим
41) Асимметричные криптосистемы
42) Гомоморфное шифрование
43) Криптографическая стойкость
44) Абсолютная криптографическая стойкость
45) Латинский квадрат
46) Шифр Вернама
47) Постквантовая криптография
48) Алгоритм Евклида
49) Соотношение Безу
50) Расширенный алгоритм Евклида

51) Сравнение по модулю
52) Группа (математика)
53) Мультипликативная группа кольца вычетов
54) Кольцо (математика)
55) Конечное поле
56) Многочлен над конечным полем
57) Простое число
58) Основная теорема арифметики
59) Решето Эратосфена
60) Факторизация целых чисел
61) P-алгоритм Полларда
62) P-1 метод Полларда
63) P+1 метод Уильямса
64) Алгоритм Диксона
65) Метод квадратичных форм Шенкса
66) Метод квадратичного решета
67) Метод Лемана
68) Метод факторизации Ферма
69) Общий метод решета числового поля
70) Специальный метод решета числового поля
71) Тест простоты
72) Тест AKS
73) Тест простоты Люка
74) Критерий Поклингтона
75) Малая теорема Ферма
76) Перебор делителей
77) Теорема Вильсона
78) Теорема Прота
79) Тест Люка — Лемера
80) Тест Миллера (теория чисел)
81) Тест Миллера — Рабина
82) Тест Пепина
83) Тест Соловея — Штрассена
84) Дискретное логарифмирование
85) Алгоритм COS
86) Алгоритм Адлемана
87) Алгоритм Гельфонда
88) Алгоритм Полига — Хеллмана
89) Алгоритм Шенкса
90) P-метод Полларда дискретного логарифмирования
91) Эллиптическая кривая
92) Теорема Хассе
93) Факторизация с помощью эллиптических кривых
94) История криптографии
95) Атбаш
96) Скитала
97) Диск Энея
98) Линейка Энея
99) Книжный шифр Энея
100) Квадрат Полибия
101) Шифр Цезаря
102) Тритемий, Иоганн
103) Кардано, Джероламо, Решётка Кардано
104) ☆ Шифр Бэкона

105) Книжный шифр
106) Омофоническая замена
107) Шифр подстановки
108) Полиалфавитный шифр
109) Шифр Виженера
110) Метод Касиски
111) Индекс совпадений
112) Автокорреляционный метод (криптоанализ)
113) Шифр Хилла
114) Чёрный кабинет
115) Ловелль, Джеймс
116) Шифр Плейфера
117) Керкгоффс, Огюст, Принцип Керкгоффса
118) Телеграмма Циммермана
119) Найджел де Гри
120) Уильям Монтгомери
121) Энигма
122) «Бюро шифров»
123) Генрих Зигальский
124) Ежи Рожицкий
125) Мариан Реевский
126) Бертран, Гюстав
127) Шмидт, Ганс-Тило
128) Криптологическая бомба
129) Циклометр
130) Блетчли-парк
131) Гордон Велчман
132) Макс Ньюман
133) Bombe
134) Тьюринг, Алан
135) Машина Лоренца
136) M-209
137) Хеш-функция
138) Adler-32
139) Циклический избыточный код
140) JH
141) HAVAL
142) LM hash
143) MD2
144) MD4
145) MD5
146) N-Hash
147) PJW-32
148) RIPEMD-160
149) SHA-1
150) SHA-2
151) SHA-3
152) Snefru
153) TTH
154) ГОСТ Р 34.11-94
155) ГОСТ Р 34.11-2012
156) NESSIE
157) Two-Track-MAC
158) UMAC

159) CBC-MAC
160) HMAC
161) Whirlpool
162) SHA-256, SHA-384, SHA-512
163) SHA-3 (конкурс)
164) BLAKE (хеш-функция)
165) BMW Hash function
166) CubeHash
167) ECHO
168) Fugue (хеш-функция)
169) Grøstl
170) Hamsi
171) JH
172) Keccak
173) Luffa (хеш-функция)
174) SHABAL
175) SHAvite-3
176) SIMD (хеш-функция)
177) Skein
178) Поточный шифр
179) A3 (шифр)
180) A5
181) A8 (шифр)
182) RC4
183) SEAL
184) VMPC
185) eSTREAM
186) F-FCSR
187) Grain
188) HC-256
189) MICKEY
190) Rabbit
191) Salsa20
192) SOSEMANUK
193) Trivium
194) Алгоритм Берлекампа
195) Симметричные криптосистемы
196) AES (конкурс)
197) CAST-256
198) CRYPTON
199) DEAL
200) DFC
201) E2
202) FROG
203) HPC
204) LOKI97
205) MAGENTA
206) MARS
207) RC6
208) Rijndael
209) ☆ SAFER+
210) Serpent
211) Twofish
212) SQUARE

213) NESSIE
214) MISTY1
215) Camellia
216) SHACAL-2
217) ACE Encrypt
218) PSEC-KEM
219) RSA-KEM
220) Blowfish
221) DES
222) 3DES
223) IDEA
224) RC5
225) ГОСТ 28147—89
226) NUSH
227) TEA
228) XTEA
229) XXTEA
230) Асимметричные криптосистемы
231) Односторонняя функция
232) Алгоритм Диффи — Хеллмана
233) Задача о ранце
234) Односторонняя функция с потайным входом
235) Асимметричные криптосистемы
236) IEEE P1363
237) RSA
238) DSA
239) Схема Эль-Гамаля
240) ГОСТ Р 34.10-2001
241) NESSIE
242) ECDSA
243) RSA-PSS
244) SFLASH
245) McEliece
246) Протоколы с нулевым разглашением
247) Раскраска графа
248) Гамильтонов цикл
249) Слепая подпись
250) Доказательство с нулевым разглашением
251) Проблема гроссмейстера
252) Обман, выполненный мафией
253) Обман с несколькими личностями
254) Протоколы тайного голосования
255) Протоколы распространения ключей
256) Протоколы распространения ключей
257) Протокол Диффи — Хеллмана
258) MTI
259) STS
260) Схемы разделение секрета
261) Разделение секрета
262) Схема разделения секрета Шамира
263) Векторная схема разделения секрета
264) Схема Миньотта
265) Схема Асмута — Блума
266) Схема Карнина — Грина — Хеллмана

267) OAuth
268) OpenID
269) SSL / TLS
270) Kerberos
271) SPKM
272) Windows Live ID
273) SKIP
274) MS-CHAP
275) Адлеман, Леонард Макс
276) Андерсон, Росс
277) Бэббидж, Чарльз
278) Бихам, Эли
279) Бирюков, Алекс
280) Даймен, Йоан
281) Диффи, Уитфилд
282) Калиски, Барт
283) Фридрих Касиски
284) Келси, Джон
285) Кнудсен, Ларс
286) Мэсси, Джеймс
287) Мёрфи, Шон
288) Рэймен, Винсент
289) Ривест, Рональд Линн
290) Сюэцзя, Лай
291) Фейстель, Хорст
292) Фридман, Уильям Фредерик
293) Хейз, Говард
294) Хандшух, Хелен
295) Хеллман, Мартин
296) Хилл, Лестер
297) Циммерман, Филипп
298) Шамир, Ади
299) Шеннон, Клод Элвуд
300) Шнайер, Брюс
301) Эль-Гамаль, Тахер
302) Кан, Дэвид
303) Сингх, Саймон
304) «Китаб аль-Маумма» («Книга тайного языка»)
305) Трактат о дешифровке криптографических сообщений
306) Послание монаха Роджера Бэкона
307) Трактат о шифрах
308) Военная криптография (книга)
309) Математическая теория связи
310) Communication Theory of Secrecy Systems
311) Encyclopedia of Cryptography and Security
312) The Codebreakers
313) MI-8
314) Комната 40
315) АНБ
316) Центр национальной компьютерной безопасности США
317) Эшелон (секретная служба)
318) ФАПСИ
319) AES (конкурс)
320) CHES

321) CRYPTREC
322) eSTREAM
323) NESSIE
324) Конференция RSA
325) Золотой жук
326) Пляшущие человечки
327) Скремблер
328) Авторизация
329) Одноразовый пароль
330) Токен (авторизации)
331) Time-based One-time Password Algorithm
332) HOTP
333) Аутентификация
334) Схема Шнорра
335) Критерии определения безопасности компьютерных систем
336) AACS
337) Common Scrambling Algorithm
338) Content Scramble System
339) DeCSS
340) Digital Rights Management
341) HDCP
342) Mandatory Managed Copy
343) Trusted Platform Module
344) Незаконное простое число
345) Арифметика с большими целыми числами
346) Алгоритм быстрого возведения в степень
347) Электронные деньги
348) Bitcoin

Возможные темы курсового проекта (групповая работа):

Постквантовая криптография
1. Реализация шифра «»
Состав проекта: реализация шифра, реализация системы создания ключа, хранения ключа, смены
ключа. Оценка скорости шифрования. Оценка лавинного эффекта для блочных шифров. Оценка применимости одной из атак.

2. Распределение ключа
3. Создание ключа, распределение между узлами, смена ключа безопасное хранение.

1.2 Гомоморфное шифрование
4. Реализация гомоморфного шифра, оценка обьема ключа в зависимости от объема сообщений, создание, смена ключей. Оценка скорости шифрования
1.3 Система защиты для IoT
5. Выбор протокола для защиты. Обеспечение конфиденциальности и целостности. Смена ключей и паролей на устройствах.
6. Атаки на существующие протоколы.
7. Симметричный шифр для IoT
8. Контроль целостности для IoT
9. Управление паролями в IoT
10. Управление ключами в IoT

1.4 Физически не клонируемые функции

11. Реализация и сравнение физически неклонируемых функций
12. Реализация атак на PUF
1.5 Системы голосования
13. Реализация и оценка качества и скорости системы голосования
14. Атаки на существующие системы голосования
1.6 Оценка стойкости отечественной криптографии
15. Атаки на поиск коллизий в Стрибоге
16. Реализация атак на Кузнечик
17. Анализ S-блоков Кузнечика
18. Обзор методов создания S-блоков и реализация генератора с изменяемым набором проверок
19. Оценка стойкости электронной подписи
20. Оценка XSL структур
21. Оценка XL структур
22. Формирование списка нелинейных функций для блока 4-8 бит и оценка их нелинейности

1.7 Наложенные средства защиты
23. WAF
24. IPS
25. DPI
26. Антивирус

1.8 Симметричные шифры
27. Анализ стойкости одного из существующих и эксплуатируемых симметричных шифров
28. Реализация системы шифрования (включая схему управления ключами) имеющую прикладную ценность
29. Реализация существующего симметричного шифра, со скоростью шифрования выше существующих аналогов
30. Оценка шифрующих свойств криптопримитивов
1.9 Асимметричные шифры
31. Реализация схем формирования ЭП и шифрования быстрее существующих аналогов

Контрольно-измерительные материалы включают три контрольных работы по полтора часа на лекциях, а также эссе (курсовая работа) на выбранную студентом тему; групповая курсовая работа (практическая работа) на выбранную группой из трех-пяти студентов тему.

Оценивание курсовых работ (эссе):

Курсовая работа выполняется самостоятельно, по утвержденной семинаристом теме. Темы курсовых работ у студентов одного курса обучения не должны пересекаться. Утверждение темы курсовой работы происходит путем заявления темы на электронную почту (допускаются иные каналы согласования тем курсовых работ, при условии, если семинарист объявит о них не позднее чем за две недели до срока окончания приема тем работ) преподавателя и получения от него одобрения. Тема работы должна быть заявлена не позже 15 октября. За каждые две недели просрочки подачи темы без уважительной причины снимается 1 балл оценки курсовой работы.

Курсовая работа должна содержать не менее 6 листов текста 12 кеглем с одинарным интервалом без учета картинок и таблиц. Работа оформляется в соответствии с ГОСТ.

Курсовая работа не должна содержать заимствований более 5 предложений из одной работы. В случае цитат какой-либо из работ обязательно должны быть приведены ссылки на данную работу.

После окончания написания работы, студент высылает работу преподавателю для предварительного оценивания качества работы. В случае, если преподаватель находит критические ошибки в работе, он отправляет отзыв с указанием ошибок студенту с просьбой их устранить.

Работа оценивается по шкале от 0 до 10 баллов.

10 баллов – работа полностью описывает рассматриваемую предметную область и может быть рекомендована в качестве публикации в научном журнале. Возможно наличие научных результатов.

9 – работа полностью описывает рассматриваемую предметную область и может быть рекомендована в качестве публикации на одном из профильных ресурсов сети интернет. Возможно наличие новых технических результатов.

8- работа полностью описывает рассматриваемую предметную область. Подобное исследование (обзор) ранее не публиковались на русском языке в доступных для поиска источниках. Работа может быть рекомендована в качестве публикации на одном из профильных ресурсов сети интернет.

7 – работа описывает предметную область, но у преподавателя есть замечания к качеству описания.

6 – работа не полностью описывает предметную область, у преподавателя есть замечания к качеству или студент не смог ответить на вопросы по работе.

5 – работа не полностью описывает предметную область, у преподавателя есть замечания к качеству и студент не смог ответить на вопросы по работе.

4 – работа содержит ошибки.

3 – работа содержит грубые ошибки.

1,2 – работа заимствована, работа не выполнена.

Дополнительные 10 баллов за работу студент может заработать путем публикации работы на конференции МФТИ, профильном интернет-ресурсе (habr или аналоге).

Дополнительные 20 баллов за работу студент может заработать путем публикации работы в Трудах МФТИ или любом другом профильном научном рецензируемом журнале. Оценка за работу может быть выставлена по факту приема материалов к публикации.

В случае публикации эссе в научных журналах или изложении на научной конференции в составе коллектива баллы за эссе делятся среди авторов.

Оценивание курсовых проектов:

Работа оценивается по шкале от 0 до 10 баллов.

10 баллов – Проект реализован полностью и без ошибок. Возможно наличие научных результатов.

9 – проект реализован полностью и без ошибок. Возможно наличие новых технических результатов.

8- Проект реализован полностью, но не содержит новизны. Подобное исследование (обзор) ранее не публиковались на русском языке в доступных для поиска источниках. Работа может быть рекомендована в качестве публикации на одном из профильных ресурсов сети интернет.

7 – Проект реализован полностью, но у преподавателя есть замечания к качеству и новизне.

6 – Проект реализован не полностью, у преподавателя есть замечания к качеству или студент не смог ответить на вопросы по работе.

5 – Проект реализован не полностью у преподавателя есть замечания к качеству и студент не смог ответить на вопросы по работе.

4 – Проект содержит ошибки, не хватает части базового функционала.

3 – Проект содержит грубые ошибки.

1,2 – Проект заимствован, работа не выполнена.

Дополнительные 10 баллов группа зарабатывает в случае, если проект повторяет ранее полученные научные результаты, обобщает результаты нескольких исследований

Дополнительные 20 баллов группа зарабатывает за получение новых научных результатов, в результате проекта или создание прототипа продукта, однозначно востребованного на рынке. Проект выбирается один из всех проектов отдельного семинариста. В этом случае результаты проекта рекомендуются к публикации. При этом, публикация результатов проекта не засчитывается как эссе.

Оценивание контрольных работ:

Каждая контрольная работа оценивается максимум на 10 баллов, баллы за конкретные выполненные задания определяются преподавателем в зависимости от сложности заданий.

4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

Перечень контрольных вопросов для сдачи экзамена:

1) Цели, задачи и методы защиты информации. Примеры выполнения целей по защите информации без использования криптографических средств.

2) Криптология, криптоанализ, криптография. Криптографические примитивы. Основные определения и примеры использования. Код, шифр, ключ, хеш-функция, криптографический протокол, цифровая подпись, etc. Принцип Керкгоффса.

3) Применение основ теории информации в криптографии. Абсолютно защищённые шифры, критерии, расстояние единственности (с выводом).

4) Криптоанализ моноалфафитных и полиалфавитных шифров.

5) Введение в блочные шифры. Особенности построения блочных шифров на примере (в сравнении) шифров AES и ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015.

6) ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018) Режимы шифрования. Описание, плюсы и минусы каждого из режимов. Оценка объемов ключевой информации для шифрования в каждом из режимов.

7) Блочный шифр стандарта ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) (подробно).

8) Блочный шифр стандарта AES (подробно).

9) Современные блочные шифры на примере (в сравнении) ГОСТ и AES. Требования к современным блочным шифрам.

10) Генераторы случайной и псевдослучайной последовательностей, их свойства, оценка возможности использования в криптографии. Линейно-конгруэнтный генератор, генератор на основе единственного регистра с линейной обратной связью.

11) Криптографически стойкие генераторы псевдослучайной последовательности. Поточные шифры и требования к ним. Возможность создания поточных шифров из блочных. Плюсы и минусы подобного подхода. Объединение генераторов на основе РСЛОС для создания криптографически стойкого генератора псевдослучайной последовательности.

12) Современные поточные шифры на примере семейства шифров A5/x. Требования, характеристики и анализ защищённости.

13) Современные поточные шифры на примере RC4. Требования, характеристики и анализ защищённости.

14) Генераторы псевдослучайных последовательностей. Свойства, принципы построения для использования в криптографии.

15) Хэш-функции и их использование в криптографии. Свойства, принципы построения криптографически стойких хэш-функций (стандарта США или ГОСТ Р 34.11-2012 (ГОСТ 34.11-2015) «СТРИБОГ»). Структуры Меркла-Дамгарда, Миагучи-Пренеля.

16) Односторонние функции с потайной дверцей. Пример, не связанный с задачами из области теории чисел (т.е. не факторизация, не дискретный логарифм, etc.) Возможность использования односторонних функций в криптографии. Общие идеи использования криптографии с открытым ключом. Проблемы криптографической стойкости, производительности.

17) RSA. Доказательство корректности, использование для шифрования и электронной подписи. Проблемы, лежащие в основе криптографической стойкости RSA. Проблемы “ванильной” реализации RSA.

18) El Gamal. Доказательство корректности, использование для шифрования и электронной подписи.

19) Цифровые подписи. Цели, основные принципы получения и использования. Конкретные примеры использования цифровых подписей в современных информационных системах.

20) Стандарт ГОСТ Р 34.10-2012 (ГОСТ 34.10-2015).

21) Контейнеры ключей на примере стандартов PKCS#12, PKCS#15.

22) Протоколы аутентификации и идентификации сторон на основе систем симметричного шифрования. Построение, плюсы и минусы, криптографическая стойкость на примере протокола Yahalom или Нидхема-Шрёдера.

23) Протоколы аутентификации и идентификации сторон на основе систем асимметричного шифрования. Построение, плюсы и минусы, криптографическая стойкость на примере протокола DASS, Деннинга-Сакко или Ву-Лама.

23) Протоколы распространения ключей. Протокол Диффи-Хеллмана и один на выбор: MTI, STS, Жиро.

24) Разделение секрета. Пороговые схемы разделения секрета Шамира и Блэкли (подробно).

25) Протокол распространения ключей на схеме Блома.

26) Атака на переполнение буфера. Причины и последствия. Детальное описание (без примера на ассемблере), программные и аппаратные способы защиты: безопасные функции, security cookies, DEP, ASLR, etc.

27) Атаки на плохие указатели. Причины и последствия. Детальное описание (без примера на ассемблере).

28) Атаки на ошибки контроля данных, примеры с printf, HTML+HTTP+SQL, HTTP+HTML+JavaScript. Directory traversal, альтернативные имена файлов в NTFS. Атаки из OWASP TOP 20.

29) Атаки на некорректное применение криптоалгоритмов и нестрогое следование стандартам. Примеры с вектором инициализации в CBC, с многоразовыми блокнотами, с проверкой длины хеша.

30) Атаки на плохие генераторы псевдослучайной последовательности. Примеры с Netscape SSL, WinZIP, PHP.

31) Протокол Kerberos. Математическое описание, описание реализации (v4 или v5 на выбор).

32) Протокол IPsec (подробно).

33) Порядок разработки средств защиты информации для технических и криптографических средств защиты информации в РФ.

34) Порядок разработки наложенных систем защиты информации по ISO2700x.

35) Китайская теорема об остатках. Доказательство, использование для защиты информации.

36) “Длинная” модульная арифметика, использование в криптографии. Сложение, умножение, возведение в степень, расширенный алгоритм Евклида.

37) Тесты проверки чисел на простоту. Свойства отдельных алгоритмов, возможность их использования в криптографии. (Только сравнение, но все тесты, включая тест на эллиптических кривых и AKS).

38) Проверка чисел на простоту с использованием тестов Ферма, Миллера, Миллера-Рабина (подробно).

39) Группы вычетов, подгруппы, генераторы. Построение, операции, свойства, использование в криптографии.

40) Поля Галуа вида GF(p) и GF(2n). Построение, операции, свойства, использование в криптографии.

41) Группы точек эллиптической кривой над множеством рациональных чисел и над конечными полями. Построение, операции, свойства. Теорема Хассе. Использование в криптографии.

42) Протоколы квантового распределения ключей BB84, BB92, Lo05, E91

43) Системы частичного и полностью гомоморфного шифрования.

Примеры билетов для проведения устного экзамена:

Билет №1.

1) Цели, задачи и методы защиты информации. Примеры выполнения целей по защите информации без использования криптографических средств.

2) Группы точек эллиптической кривой над множеством рациональных чисел и над конечными полями. Построение, операции, свойства. Теорема Хассе. Использование в криптографии.

Билет №2.

1) Криптология, криптоанализ, криптография. Криптографические примитивы. Основные определения и примеры использования. Код, шифр, ключ, хеш-функция, криптографический протокол, цифровая подпись, etc. Принцип Керкгоффса.

2) Поля Галуа вида GF(p) и GF(2n). Построение, операции, свойства, использование в криптографии.

Критерии оценивания

Для промежуточного оценивания успеваемости студентов по курсу «Защита информации» применяется балльно-рейтинговая система (БРС). Настоящая программа, в части методики оценивания, является дополнением к «Положению о текущем контроле успеваемости и промежуточной аттестации обучающихся в МФТИ» №1191-1 от 30.12.2016

№	Вид занятий	Сумма баллов
1	Контрольная работа № 1	0-10
2	Контрольная работа № 2	0-10
3	Контрольная работа № 3	0-10
4	Курсовая работа (эссе)	0-15(без учета дополнительных баллов за качество работы)
5	Курсовой проект	0-15 (без учета дополнительных баллов за качество работы)
6	Итого за работу в семестре:	0-60
	Ответ на экзамене	0-40
	Итого	0-100

Критерии оценивания ответа по одному билету на экзамене:

40 баллов выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины, проявляющему интерес к данной предметной области, продемонстрировавшему умение уверенно и творчески применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

36 баллов выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

32 балла выставляется студенту, показавшему систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, правильное обоснование принятых решений, с некоторыми недочетами.

28 баллов выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но недостаточно грамотно обосновывает полученные результаты.

24 балла выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности.

20 баллов выставляется студенту, если он в основном знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач достаточно большое количество неточностей.

16 баллов выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он освоил основные разделы учебной программы, необходимые для дальнейшего обучения, и может применять полученные знания по образцу в стандартной ситуации.

12 баллов выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, допускающему ошибки в формулировках базовых понятий, нарушения логической последовательности в изложении программного материала, слабо владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и с трудом применяет полученные знания даже в стандартной ситуации.

8 баллов выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных принципов и не умеет использовать полученные знания при решении типовых задач.

4 балла выставляется студенту, который не знает основного содержания учебной программы дисциплины, допускает грубейшие ошибки в формулировках базовых понятий дисциплины и вообще не имеет навыков решения типовых практических задач.

Баллы за эссе и курсовой проект выше 15 считаются дополнительными. В случае, получения балла БРС 50 и выше, за счет дополнительных баллов оценки работы на семинаре, студенту может быть предложено автоматически выставить оценку «отлично» за экзамен.

Соответствие баллов БРС оценкам итоговой академической успеваемости выставляемым обучающимся в качестве оценки за экзамен.

Баллы БРС	Оценки
80-100	10 отлично
65-79	9 отлично
50-64	8 отлично
43-49	7 хорошо
37-42	6 хорошо
30-36	5 хорошо
23-29	4 удовлетворительно
15-22	3 удовлетворительно
2-14	2 неудовлетворительно
0-1	1 неудовлетворительно

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Промежуточная аттестация в виде зачета и экзамена проводится в устной форме или в устной и письменной форме.

Зачет не дифференцированный, выставляется по факту сдачи курсового проекта и курсовой работы.

Оценка за экзамен складывается из результатов работы в семестре и оценок за каждый ответ.

Ответ по одному билету оценивается от 0 до 20 баллов.

При проведении устного экзамена обучающемуся предоставляется 1 час на подготовку. Опрос обучающегося по билету на устном экзамене не должен превышать двух астрономических часов.

Во время проведения экзамена обучающиеся могут пользоваться программой дисциплины.