МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Российский государственный гуманитарный университет»

(РГГУ)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профили) подготовки
№ 2 Организация и технология защиты информации,
№ 3 Комплексная защита объектов информатизации
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2017

Криптографические методы защиты информации
Рабочая программа дисциплины
Составитель:
Кандидат технических наук, доцент кафедры КЗИ А.С. Моляков

Ответственный редактор
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 6 от 24.01.2017 г.

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины: получение основных знаний об использовании криптографических методов для защиты информации при ее хранении, обработке и дистанционной передаче электронных данных.

Задачи дисциплины: овладение студентами основными понятиями, математическими моделями и методами современной криптографии, умение студентами: решать типовые криптографические задачи; работать со специальной математической литературой, использовать математический аппарат для решения прикладных криптографических задач защиты информации в различных сферах человеческой деятельности.

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине

Коды компетенции	**Содержание компетенций**	**Перечень планируемых результатов обучения по дисциплине**
ОПК-2	способностью применять соответствующий математический аппарат для решения профессиональных задач	Знать: основные положения математического аппарата, методы кодирования информации; основные модели, методы и средства криптографической защиты информации Уметь: решать типовые криптографические задачи защиты информации; Владеть: методами синтеза и анализа криптографических систем и протоколов, способами решения криптографических задач защиты информации в различных сферах человеческой деятельности.
ОПК-4	способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Знать: математические модели кодирования систем информации; Уметь: применять информационные технологии для поиска и обработки информации; Владеть: навыками эксплуатации криптографических протоколов и схем, получивших широкое применение в качестве инструментария в системах электронных платежей и систем электронного документооборота
ОПК-5	способностью использовать нормативные правовые акты в профессиональной деятельности	Знать: нормативно-правовые требования в области разработки и применения СКЗИ Уметь: применять теоретические знания при разработке ОРД Владеть: навыками поиска нужной информации в нормативных базах и источниках

1.3. Место дисциплины в структуре основной образовательной программы

Дисциплина «Криптографические методы защиты информации» относится к базовой части блока дисциплин учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации.

Для освоения дисциплины необходимы компетенции, сформированные в ходе изучения следующих дисциплин: «Теория информации», «Математические основы защиты информации», «Техническое регулирование в области защиты информации».

В результате освоения дисциплины формируются компетенции, необходимые для изучения следующих дисциплин и прохождения практик: «Комплексное обеспечение безопасности объекта информатизации», «Защита информационных процессов в автоматизированных системах», «Организация виртуальных частных сетей», «Практика по получению профессиональных умений и опыта профессиональной деятельности по технической защите информации, «Преддипломная практика».

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоемкость дисциплины – 3 з.е., 108 часов, в том числе контактная работа обучающихся с преподавателем 42 ч., промежуточная аттестация 18 ч., самостоятельная работа обучающихся 48 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Введение в дисциплину	6	2					2	Опрос
2	История криптографии	6	2		4			4	Оценка выполнения практических заданий
3	Базовые криптографические методы и схемы криптографической защиты информации	6	4		4			14	Оценка выполнения практических и внеаудиторных заданий
4	Криптографические протоколы	6	4		4			8	Оценка выполнения практических и внеаудиторных заданий
5	Нормативные акты, регламентирующие деятельность в области криптографической защиты информации	6	4		4			10	Оценка выполнения практических и внеаудиторных заданий
6	Средства и услуги в области криптографической защиты информации, представленные отечественном рынке	6	4		6			10	Оценка выполнения практических заданий
7	Экзамен	6					18		Экзамен по билетам / итоговая
	Итого:		**20**		**22**		**18**	**48**	

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	**Введение в дисциплину**	Общие положения криптологии. Базовые криптографические термины, понятия и определения. Классическая и математическая криптография. Стойкость криптографических схем (неформальное введение).
2	**История криптографии**	Эра донаучной криптографии. Шифр «Сциталь», шифры Цезаря, Полибия, Тритемия, Кардано, Порты, Виженера, большой и малый шифр Наполеона. Формы византийской тайнописи. Древнерусские шифры «Пермская азбука», «Простая и мудрая литорея», «Фиоть и Хвиоть», «Уголки», «Тарабарщина». Шифр Вернама. Шифровальные машины «Lorenz» и «Enigma».
3	**Базовые криптографические методы и схемы криптографической защиты информации**	Криптосистемы с секретным ключом, атаки на криптосистемы с секретным ключом. Криптосистемы с открытым ключом, открытое распределение ключей Диффи-Хеллмана, атаки на криптосистемы с открытым ключом. Теоретическая и практическая стойкость криптосистем. Схемы электронной подписи. Криптографически стойкие хэш-функции. Методы поиска коллизий. Элементы теории вычислительной сложности. Односторонние функции и функции с секретом. Псевдослучайные генераторы. Интерактивные системы доказательств и интерактивные системы доказательств с нулевым разглашением. Схемы с сокрытием свидетельства и с неразличимыми свидетельствами. Схемы вероятностного шифрования. Разновидности схем электронной подписи. Схемы конфиденциальной подписи. Схемы групповой подписи. Схемы мультиподписи. Схемы затемненной подписи. Схемы подписи для интеллектуальных карточек. Схемы подписи вида «офф-лайн/он-лайн». (n,t)-пороговые схемы подписи. Процедуры арбитража в схемах электронной подписи. Практические схемы интерактивной аутентификации.
4	**Криптографические протоколы**	Основы теории криптографических протоколов. Свойства и основные параметры криптографических протоколов. Классификация основных видов атак на криптографические протоколы. Протоколы аутентификации. Требования к протоколам аутентификации. Парольная аутентифи-

		кация (протоколы с фиксированными паролями, протоколы с одноразовыми паролями). Протоколы типа «запрос – ответ» (односторонняя аутентификация, основанная на метке времени, односторонняя аутентификация с использованием случайных чисел, протоколы с использованием асимметричных криптосистем, протоколы с использованием электронной подписи). Протоколы аутентификации, основанные на использовании интерактивных систем доказательств с нулевым разглашением знания. Протоколы распределения ключей. Сферы применения протоколов распределения ключей. Классификация протоколов распределения ключей. Протоколы, основанные на криптосистемах с секретным ключом. Протоколы распределения ключей, основанных на криптосистемах с открытым ключом. Протоколы образования защищенных каналов передачи данных. Основные используемые на практике методы организации защищенных каналов передачи данных. Гибридные схемы шифрования. Протоколы, одновременно обеспечивающие конфиденциальность и аутентичность информации. Банковские криптографические протоколы. Электронные монеты и переводимые электронные монеты. Электронный бумажник. Электронные платежи. Протоколы конфиденциальных вычислений и конфиденциального вычисления функции.
5	**Нормативные акты, регламентирующие деятельность в области криптографической защиты информации**	Федеральные законы «Об информации, информационных технологиях и о защите информации», «О персональных данных», «Об электронной подписи», «О техническом регулировании». Постановление Правительства Российской Федерации от 23 сентября 2002 года №691 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами». Положение о разработке, производ-стве, реализации и эксплуатации шифровальных (криптографических) средств защиты ин-формации (Положение ПКЗ-2005), утв. Приказом Директора ФСБ России от 09 февраля 2005 года №66. Отечественные (криптографические) ГОСТЫ: ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.

6	**Средства и услуги в области криптографической защиты информации, представленные на отечественном рынке**	Организации, осуществляющие деятельность в области криптографической защиты информации. Линейка продуктов «КриптоПро». Линейка продуктов «Secret Disk». Защищенный абонентский пункт системы «Атлас» (изделие М-468Р). Решения ФГУП «НТЦ «Атлас» по созданию защищенных (до класса АК3) автоматизированных систем на платформе Майкрософт. СКЗИ «Крипто БД». Другие продукты и услуги в области криптографической защиты информации.

4. Образовательные технологии

При реализации рабочей программы дисциплины «Криптографические методы защиты информации» используются следующие образовательные технологии:

Образовательные технологии

№ п/п	Наименование темы	Виды учебных занятий	Образовательные технологии
1	*Введение в дисциплину*	*Лекция.*	*Традиционная с использованием презентаций*
2	*История криптографии*	*Лекция.* *Практическое занятие 1.*	*Лекция-дискуссия* *Традиционная*
3	*Базовые криптографические методы и схемы криптографической защиты информации*	*Лекция.* *Практическое занятие 2.*	*Лекция-дискуссия* *Традиционная*
4	*Криптографические протоколы*	*Лекция.* *Практические занятия 3.*	*Проблемная лекция* *Традиционная с использованием презентаций*
5	*Нормативные акты, регламентирующие деятельность в области криптографической защиты информации*	*Лекция.* *Практическое занятие 4.*	*Лекция с разбором конкретных ситуаций* *Традиционная*
6	*Средства и услуги в области криптографической защиты информации, представленные на отечественном рынке*	*Лекция.* *Практическое занятие 5.*	*Лекция-дискуссия* *Традиционная*

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *- опрос (темы 1-6)* *- участие в дискуссии на семинаре* *- практические задания (темы 2-3)* *- практические задания (темы 4-6)*	 *5 баллов* *5 баллов* *10 баллов* *10 баллов*	 *30 баллов* *10 баллов* *20 баллов* *30 баллов*
Промежуточная аттестация *Экзамен*		*40 баллов*
Итого за семестр *Экзамен*		*100 баллов*

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2.Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
		Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетвори-тельно)»/ «зачтено»	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности - проверка сформированности компетенций ОПК-2, ОПК-4,ОПК-5

1. Каковы основные свойства криптографической системы и криптографического протокола? Приведите примеры процедур обмена сообщениями, которые являются раундами и шагами криптографических протоколов.

2. В чем заключаются свойства полноты и корректности интерактивного доказательства?

3. В чем отличие интерактивных систем доказательства с нулевым разглашением знания от интерактивных систем доказательства? Сохраняется ли свойство нулевого разглашения при последовательном и параллельном выполнении протоколов?

4. Что понимается под компрометацией криптографического протокола? Приведите примеры:

атаки по известным ключам;

словарной атаки.

5. Имеется схема открытого шифрования RSA. d – секретный ключ участника P, e – открытый ключ, соответствующий этому секретному ключу, n – модуль схемы шифрования. P имеет шифртекст C. P хочет доказать V знание секретного ключа d, но так, чтобы V не узнал этот ключ, и чтобы он не смог расшифровать какой-либо шифртекст (в том числе и C). Как это можно сделать? (Предложите протокол доказательства с нулевым разглашением знания.) Вычислительные возможности P и V в процессе обмена полиномиально ограничены.

6. Известна формула Андерсена определения длины пароля:

$$S_t = \frac{1}{2} N^x \cdot \frac{L}{T},$$

где S_t – время безопасности (раскрытия) пароля (в течение этого времени пароль сохраняет тайну);

T – скорость ввода пароля, симв./мин.;

x – длина пароля, симв.;

N – мощность алфавита;

L – число вводимых символов и др. знаков, необходимых для инициализации опознания (может быть больше длины пароля).

Постройте графики зависимости времени безопасности:

а) PIN-кода;

б) цифро-алфавитного пароля (русский алфавит)

от длины пароля при условии:

ручного ввода символов на клавиатуре (T=120);

автоматизированного подбора паролей (T=1200),

считая, что число попыток ввода пароля не ограничено, а для ввода пароля необходимо набрать его на клавиатуре и нажать клавишу <Enter>.

7. Проведите сравнение протоколов аутентификации, основанных на доказательствах с нулевым разглашением знания (Фиата – Шамира, Гийю-Кискатера, Шнорра), по следующим параметрам: вычислительной сложности протокола для доказывающего и проверяющего, количеству передаваемых байтов данных, дополнительной памяти, необходимой P и V. Сделайте вывод о сравнительной эффективности протоколов. (Необходимые параметры выберите самостоятельно.)

8. Как преобразовать протокол аутентификации Шнорра в схему электронной подписи?

9. Предположим, что к данным, предназначенным для передачи в канал связи, согласно техническим условиям, отправителю необходимо применить: алгоритм блочного шифрования (шифр считать идеальным), алгоритм помехоустойчивого кодирования, алгоритм сжатия. В каком порядке следует применять эти алгоритмы и почему? На каком этапе в случае необходимости нужно сгенерировать электронную подпись отправителя? Имеет ли эта задача однозначное решение?

10. Поясните, в каких случаях для обеспечения подлинности сообщений необходимо применять электронную подпись, а в каких – хэш-функции с ключом? В чем преимущества и недостатки каждого метода?

11. Приведите основные положения Федерального закона «Об электронной подписи», ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012. Расскажите об принципах использования, видах и средствах электронных подписей, об удостоверяющих центрах и сертификатах ключей проверки электронной подписи.

Промежуточная аттестация (контрольные вопросы) - проверка сформированности компетенций ОПК-2, ОПК-4,ОПК-5

1. Пусть (E,D) – схема симметричного шифрования, MAC – криптографическая хэш-функция с ключом. Пусть A и B имеют общие ключи: K_1 – для шифрования, K_2 – для хэш-функции. Они хотят передать сообщение m таким образом, чтобы была обеспечена секретность, целостность и подлинность сообщения. Им предложены следующие способы выполнения протокола:

а) $M, MAC_{K_2}(E_{K_1}(M))$;

б) $E_{K_1}(M), MAC_{K_2}(M)$;

в) $E_{K_1}(M), MAC_{K_2}(M)$;

г) $E_{K_1}(M), E_{K_1}(MAC_{K_2}(M))$;

д) $E_{K_1}(M), MAC_{K_2}(E_{K_1}(M))$;

е) $E_{K_1}(MAC_{K_2}(M)), MAC_{K_2}(E_{K_1}(M))$;

ж) $E_{K_1}(M, MAC_{K_2}(M)), MAC_{K_2}(M)$;

и) $E_{K_1}(M, A)$, где A – идентификатор отправителя (B расшифровывает шифртекст и проверяет, что вторая часть открытого текста совпадает с идентификатором отправителя).

Для каждого способа объясните, обеспечивает ли он требуемые свойства (секретности, целостности, подлинности)? Какие из этих способов предпочтительнее? Какие не пригодны для использования? Почему?

2. Назовите известные Вам режимы работы блочных шифров, позволяющие обеспечить:

только секретность сообщений;

только подлинность сообщений;

одновременно секретность и подлинность сообщений.

Какие из этих режимов считаются лучшими по соотношению «стойкость/скорость»?

3. Какие режимы алгоритмов шифрования ГОСТ 28147-89 и DES предпочтительнее использовать для шифрования полей базы данных автоматизированной банковской системы с интеллектуальной карточкой, содержащей сведения о клиентах (идентификаторы, открытые ключи, номера интеллектуальных карточек, состояние счета, отметка о включении интеллектуальных карточек в стоп-лист и т.д.), доступ к которой осуществляется в режиме реального времени, и почему?

4. Рассматривается схема электронной подписи с восстановлением сообщения из стандарта ISO/IEC 9796. Какой максимальной длины (в байтах) может быть сообщение, если требуется, чтобы подпись имела длину 512 битов?

5. Какие функции может выполнять центр доверия в протоколах распределения ключей? Приведите примеры.

6. В чем разница между понятиями: способы распространения ключей и протоколы распределения ключей?

7. Опишите схему Д. Чома со следующими параметрами: банкноты имеют разное достоинство, сумма, оплачиваемая продавцу, составляет 7 рублей, максимальная сумма, оплачиваемая покупателем, составляет 21 рубль.

8. Приведите протокол конфиденциально реализуемой операции умножения переменной на константу с использованием (t,n)-пороговой схемы Шамира.

9. Приведите примеры реализации систем защищенного электронного документооборота и защищенной электронной почты.

10. Приведите примеры реализации систем дистанционного банковского обслуживания и системы платежей по банковским картам. Расскажите об основных положениях Стандарта Банка России СТО БР ИББС 1.0.

Примерные задания для тестирования- проверка сформированности компетенций ОПК-2, ОПК-4,ОПК-5

1. Длина ключа алгоритма DES:

а) 56 бит.

б) 48 бит.

в) 512 бит.

2. Криптостойкость — это:

а) устойчивость к внешним излучениям..

б). способность криптографического алгоритма противостоять криптоанализу

в) устойчивость к деформациям.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники

основные

1. *Федеральный закон* от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]: Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.
2. *Федеральный закон* от 27 июля 2006 г. №152-ФЗ «О персональных данных» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.
3. *Федеральный закон* от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_112701/, свободный. – Загл. с экрана.
4. *Федеральный закон* от 27 декабря 2002 г. №184-ФЗ «О техническом регулировании» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_40241/, свободный. – Загл. с экрана.

Литература

основная

1. Методы и средства защиты программного обеспечения [Электронный ресурс] : учеб.-метод. комплекс : для бакалавриата по направлению подготовки 090900 Информационная безопасность : по профилям: Организация и технология защиты информации, Комплексная защита объектов информатизации / Минобрнауки России, Федер. гос. бюджетное образоват. учреждение высш. проф. образования "Рос. гос. гуманитарный ун-т" (РГГУ), Ин-т информац. наук и технологий безопасности, Фак. информац. систем и безопасности, Каф. компьютерной безопасности ; [сост.: Казарин О. В. ; отв. ред. А.

А. Тарасов]. - Электрон. дан. - Москва: РГГУ, 2013. - 30 с. - Режим доступа: http://elib.lib.rsuh.ru/elib/000009341. - Загл. с экрана. - ISBN 978-5-7281-1789-6.

2. *Комплексная защита* информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/546679
3. *Шаньгин В.Ф.* Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В. Ф. Шаньгин. - М.: ДМК Пресс, 2010. - 544 с.: ил. - ISBN 978-5-94074-518-1. - Режим доступа: http://znanium.com/catalog/product/408107

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимый для освоения дисциплины

Адреса ресурсов Интернет

1. Анохин М. И. Конспект лекций курса. Введение в математическую криптографию / Математическая криптография [Электронный ресурс] // Режим доступа: http://cryptography.ru/wp-content/uploads/2016/04/math_crypto_lecture_ notes.pdf.

2. Варновский Н.П. Курс лекций по математической криптографии [Электронный ресурс]. – Режим доступа: http://cryptography.ru/wp-content/uploads/2014/11/varn_lectures_long.pdf

3. Введение в криптографию/ Под общ. ред. В.В. Ященко. [Электронный ресурс]. – Режим доступа: http://nature.web.ru/db/msg.html?mid=1157083&uri=book.html

4. Goldreich O. Foundations of cryptography. [Электронный ресурс]. – Режим доступа: http://www.twirpx.com/file/493751/

6.3. Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Компьютерные справочные правовые системы Консультант Плюс, Гарант

7. Материально-техническое обеспечение дисциплины

Для проведения занятий необходимо следующее материально-техническое обеспечение:

1) лекционный класс с видеопроектором и компьютером, на котором должны быть установлены:

– лицензионное ПО MS Windows 7 и старше;

– лицензионное ПО MS Office 2010 (с обязательным наличием MS PowerPoint) и старше

2) компьютерный класс, оборудованный современными персональными компьютерами для каждого студента с выходом в интернет. На компьютере должны быть установлены:

– лицензионное ПО MS Windows 7 и старше;

– лицензионное ПО MS Office 2010 и старше;

– программный гипервизор Vmware Player;

– демо-дистрибутивы СКЗИ с сайта компании «КриптоПро».

Перечень ПО

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 7 Pro	Microsoft	лицензионное
3	Microsoft Share Point 2010	Microsoft	лицензионное
4	Microsoft Office 2013	Microsoft	лицензионное
5	Windows 10 Pro	Microsoft	лицензионное
6	Kaspersky Endpoint Security	Kaspersky	Лицензионное
7	Secret Net Studio 8.4	Код безопасности	Свободное ПО, Режим доступа: https://securitycode.ru Демо-версия
8	Dallas Lock 8.0	Конфидент	Свободное ПО, Режим доступа: https://dallaslock.ru/ Демо-версия
9	Vmware Player 15.5	VMWare	Свободное ПО, Режим доступа: https://www.vmware.com/products/ Демо-версия
10	демо-дистрибутивы СКЗИ «Крипто-Про».	Крипто-Про	Свободное ПО, Режим доступа: https://www.cryptopro.ru/user?destination=node%2F148 Демо-версия

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

– лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

– письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;

– обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

– для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;

– письменные задания оформляются увеличенным шрифтом;

– экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

– лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;

– письменные задания выполняются на компьютере в письменной форме;

– экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

– лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

– письменные задания выполняются на компьютере со специализированным программным обеспечением;

– экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

– в печатной форме увеличенным шрифтом;

– в форме электронного документа;

– в форме аудиофайла.

- для глухих и слабослышащих:

– в печатной форме;

– в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

– в печатной форме;

– в форме электронного документа;

– в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:

– устройством для сканирования и чтения с камерой SARA CE;

– дисплеем Брайля PAC Mate 20;

– принтером Брайля EmBraille ViewPlus;

- для глухих и слабослышащих:

– автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;

– акустический усилитель и колонки;

- для обучающихся с нарушениями опорно-двигательного аппарата:

– передвижными, регулируемыми эргономическими партами СИ-1;

– компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий. Методические указания по организации и проведению - *проверка сформированности компетенций ОПК-2, ОПК-4,ОПК-5*

Практическое занятие 1 (4 часа). История криптографии. Основные положения криптографии (*проверка сформированности компетенций ОПК-5)*

Вопросы для изучения и обсуждения:

Криптосинтез и криптоанализ. Криптографическая система (подсистемы шифрования, идентификации, имитозащиты, электронной подписи). Криптографический протокол. Криптографический примитив.

Криптоаналитик (противник). Криптоаналитик активный и пассивный.

Теоретико-информационная стойкость (совершенная криптографическая стойкость, безусловная стойкость, шенноновская стойкость). Теоретико-сложностная стойкость.

Электронная подпись. Шифр, ключ, Шифрование/дешифрование. Шифртекст (криптограмма). Криптографическая система с секретным ключом. Блочная криптосистема. Поточная криптосистема. Криптографическая система с открытым ключом. Имитозащита. Стеганография.

Роль и место криптографических методов в защите современных информационных систем.

Контрольные вопросы:

1. Опишите взаимосвязь криптографии и криптологии и их основных составляющих дисциплин.

2. Приведите примеры криптографических систем с секретным ключом и криптографических систем с открытым ключом.

3. Опишите требования, которые должны быть предъявлены к криптографическим системам.

4. Выполните классификацию основных видов атак криптоаналитика (противника) на криптографические системы.

5. Дайте определения теоретической и практической стойкости криптографических систем и поясните их различия.

6. В чем отличие криптографии от стеганографии? Приведите примеры.

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение практического занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer

Практическое занятие 2 (4 часа). Базовые криптографические методы и схемы криптографической защиты информации (*проверка сформированности компетенций ОПК-4,ОПК-5)*

Вопросы для изучения и обсуждения:

1. Криптосистемы с секретным ключом, атаки на криптосистемы с секретным ключом. Криптосистемы с открытым ключом, открытое распределение ключей Диффи-Хеллмана, атаки на криптосистемы с открытым ключом. Формальное определение теоретической и практической стойкости криптографических систем.

2. Схемы электронной подписи. Атаки и угрозы для схем электронной подписи. Примеры схем электронной подписи: RSA, Эль-Гамаля, Фиата-Шамира, Шнорра, ГОСТ Р 34.10-2012.

3. Криптографически стойкие хэш-функции. Методы поиска коллизий. Методы защиты от поиска коллизий. Хэш-функции Р.Ривеста и МККТТ Х.509.

4. Элементы теории вычислительной сложности. Односторонние функции и функции с секретом. Псевдослучайные генераторы. Интерактивные системы доказательств и интерактивные системы доказательств с нулевым разглашением. Схемы с сокрытием свидетельства и с неразличимыми свидетельствами.

5. Схемы вероятностного шифрования. Схема Голдвассер-Микали.

6. Разновидности схем электронной подписи. Схемы конфиденциальной подписи. Схемы групповой подписи. Схемы мультиподписи. Схемы затемненной подписи. Схемы подписи для интеллектуальных карточек. Схемы подписи вида «офф-лайн/он-лайн». (*n*,*t*)-пороговые схемы подписи. Процедуры арбитража в схемах электронной подписи.

7. Прикладные схемы интерактивной аутентификации. Схемы Шнорра, Фиата-Шамира, Гийю-Кискатера.

Контрольные вопросы:

1. Математически опишите криптографические системы с секретным и открытым ключами, схемы электронной подписи.

2. Дайте формальные определения односторонней функции и функции с секретом.

3. Дайте формальное определение псевдослучайному генератору.

4. Опишите свойства полноты, корректности и нулевого разглашения для интерактивных систем доказательств с нулевым разглашением.

5. Почему схема интерактивной аутентификации Шнорра является схемой с сокрытием свидетельства, а не системой доказательства с нулевым разглашением?

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение практического занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer

Практическое занятие 3 (4 часа). Криптографические протоколы (*проверка сформированности компетенций ОПК-2, ОПК-4)*

Вопросы для изучения и обсуждения:

1. Основы теории криптографических протоколов. Свойства и основные параметры криптографических протоколов.

2. Классификация основных видов атак на криптографические протоколы.

3. Протоколы аутентификации. Требования к протоколам аутентификации. Парольная аутентификация (протоколы с фиксированными паролями, протоколы с одноразовыми паролями). Протоколы типа «запрос – ответ» (односторонняя аутентификация, основанная на метке времени, односторонняя аутентификация с использованием случайных чисел, протоколы с использованием асимметричных криптосистем, протоколы с использованием электронной подписи). Протоколы аутентификации, основанные на использовании интерактивных систем доказательств с нулевым разглашением знания.

4. Протоколы распределения ключей. Сферы применения протоколов распределения ключей. Классификация протоколов распределения ключей. Протоколы, основанные на криптосистемах с секретным ключом. Протоколы распределения ключей, основанных на криптосистемах с открытым ключом.

5. Банковские криптографические протоколы. Электронные монеты и переводимые электронные монеты. Электронный бумажник. Электронные платежи.

Контрольные вопросы:

1. Каковы основные свойства криптографической системы и криптографического протокола? Что такое шаг, раунд и сеанс в криптографическом протоколе?

2. В чем заключаются свойства полноты и корректности интерактивного доказательства?

3. В чем отличие интерактивных систем доказательства с нулевым разглашением знания от интерактивных систем доказательства? Сохраняется ли свойство нулевого разглашения при последовательном и параллельном выполнении протоколов?

4. Что понимается под компрометацией криптографического протокола? Приведите примеры:

атаки по известным ключам;

словарной атаки.

5. Проведите сравнение протоколов аутентификации, основанных на доказательствах с нулевым разглашением знания (Фиата – Шамира, Гийю-Кискатера, Шнорра), по следующим параметрам: вычислительной сложности протокола для доказывающего и проверяющего, количеству передаваемых байтов данных, дополнительной памяти, необходимой *P* и *V*. Сделайте вывод о сравнительной эффективности протоколов. (Необходимые параметры выберите самостоятельно.)

6. Как преобразовать протокол аутентификации Шнорра в схему цифровой подписи?

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение практического занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer

Практическое занятие 4 (4 часа). Нормативные акты, регламентирующие деятельность в области криптографической защиты информации (*проверка сформированности компетенций ОПК-5)*

Вопросы для изучения и обсуждения:

1. Федеральные законы РФ «Об информации, информационных технологиях и о защите информации», «О персональных данных», «Об электронной подписи», «О техническом регулировании».

2. Постановление Правительства Российской Федерации от 23 сентября 2002 года №691 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами».

3. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утв. Приказом Директора ФСБ России от 09 февраля 2005 года №66.

4. Отечественные (криптографические) ГОСТы: ГОСТ 28147-89, ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015.

Выполнение задания:

В ходе практической работы имитируется процесс сертификации и эксплуатации средств криптографической защиты информации (СКЗИ), реализованных в соответствии с ГОСТ ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015 и рассматривается пакет документов, необходимый для сертификации и эксплуатации СКЗИ и собственно сертификат соответствия СКЗИ нормативным документам и/или ТУ.

Контрольные вопросы:

1. Приведите основные положения Федеральных законов РФ «Об информации, информационных технологиях и о защите информации», «О персональных данных», «Об электронной подписи», «О техническом регулировании» в части криптографической защиты информации.

2. Опишите структуру и основные функции Удостоверяющего центра в соответствии положениями Федерального закона «Об электронной подписи».

3. Расскажите об основных типах электронной подписи, назначении, структуре и полях сертификатов открытых ключей в соответствии положениями Федерального закона «Об электронной подписи».

4. Опишите основные этапы сертификации и эксплуатации СКЗИ в соответствии с положением ПКЗ-2005.

5. Опишите основные поля сертификата соответствия на СКЗИ, реализованные в соответствии ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015.

Список литературы:
Приведён в п. 6 данной РПД

Материально-техническое обеспечение практического занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer.

Практическое занятие 5 (6 часов). Средства и услуги в области криптографической защиты информации, представленные на отечественном рынке (*проверка сформированности компетенций ОПК-2, ОПК-5)*

Вопросы для изучения и обсуждения:

1. Российские организации, осуществляющие деятельность в области криптографической защиты информации.

2. Линейка продуктов «КриптоПро», линейка продуктов «Secret Disk», «TrueCrypt»

3. Защищенный абонентский пункт системы «Атлас» (изделие М-468Р). Решения ФГУП «НТЦ «Атлас» по созданию защищенных (до класса АК3) автоматизированных систем на платформе Майкрософт.

4. СКЗИ «Крипто БД».

5. Другие продукты и услуги в области криптографической защиты информации.

Выполнение задания:

В ходе практической работы осуществляется получение демо-дистрибутива СКЗИ с сайта компаний «КриптоПро», выполнение установки и реализация основных функций СКЗИ.

Контрольные вопросы:

1. Назовите основные функции существующих СКЗИ, представленных на отечественном рынке продукции и услуг в области криптографической защиты информации.

2. Какие функции безопасности реализуются существующими СКЗИ:

- обеспечение конфиденциальности;
- обеспечение целостности;
- аутентификация информации;
- аутентификация пользователей.

3. Найти в сети Интернет СКЗИ, не представленные в вышеуказанном списке СКЗИ, описать его назначение и основные функции.

Адреса ресурсов Интернет:

1. Информация и программное обеспечение с сайтов компаний ООО «КриптоПро», ЗАО НИП «Информзащита» и др..

Список литературы:
Приведён в п. 6 данной РПД

Материально-техническое обеспечение практического занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer, демо-дистрибутивы СКЗИ «Крипто-Про».

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Криптографические методы защиты информации» реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации.

Цель дисциплины: получение основных знаний об использовании криптографических методов для защиты информации при ее хранении, обработке и дистанционной передаче электронных данных.

Задачи: овладение студентами основными криптографическими понятиями, умение студентами: решать типовые криптографические задачи, востребованные практикой; работать со специальной криптографической литературой и нормативными документами; использовать полученные знания для решения прикладных задач современной криптографии.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2 – способностью применять соответствующий математический аппарат для решения профессиональных задач;

ОПК-4 – способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ОПК-5 – способностью использовать нормативные правовые акты в профессиональной деятельности.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

знать:

математические модели кодирования систем информации;

основные модели, методы и средства криптографической защиты информации;

уметь:

решать типовые криптографические задачи защиты информации;

применять информационные технологии для поиска и обработки информации;

владеть:

навыками поиска нужной информации в нормативных базах и источниках;

навыками эксплуатации криптографических протоколов и схем, получивших широкое применение в качестве инструментария в системах электронных платежей и систем электронного документооборота;

методами синтеза и анализа криптографических систем и протоколов, способами решения криптографических задач защиты информации в различных сферах человеческой деятельности.

Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, контрольной работы, реферата, тестирования, промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы, 108 часов.

Приложение 2

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*29.06.2017 г.*	***10***
2	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*26.06.2018 г.*	***11***
3	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*29.08.2019 г.*	***1***
4	*Обновлена структура дисциплины (модуля) для очной формы обучения (2020 г.)*	*23.06.2020 г*	***14***
5	*Обновлена основная и дополнительная литература*	*23.06.2020 г*	***14***
6	*Обновлен раздел п.4 Образовательные технологии*	*23.06.2020 г*	***14***
7	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*23.06.2020 г*	***14***

Приложение 1
к листу изменений

1. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2017 г.)

Перечень ПО

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	MicrosoftOffice 2013	Microsoft	лицензионное
2	Windows XP	Microsoft	лицензионное
3	KasperskyEndpointSecurity	Kaspersky	лицензионное
4	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное

Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель: К.т.н, доцент, А.С. Моляков

Приложение 2
к листу изменений

2. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2018 г.)

Перечень ПО

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statisctics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statisctics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное

Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2018 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2018 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis Электронные издания издательства Springer
	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель: К.т.н, доцент, А.С. Моляков

Приложение 3
к листу изменений

3. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2019 г.)

Перечень ПО

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statisctics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statisctics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2019 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2019 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель: К.т.н, доцент, А.С. Моляков

Приложение 4
к листу изменений

4. Обновление структуры дисциплины (модуля) для очной формы обучения (2020 г.)

Структура дисциплины (модуля) для очной формы обучения

Общая трудоемкость дисциплины составляет 3 з. е., 114 ч., в том числе контактная работа обучающихся с преподавателем 42 ч., самостоятельная работа обучающихся 54 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Введение в дисциплину	**6**	**2**					**6**	Опрос
2	История криптографии	**6**	**2**		**4**			**8**	Оценка выполнения практических заданий
3	Базовые криптографические методы и схемы криптографической защиты информации	**6**	**4**		**4**			**10**	Оценка выполнения практических и внеаудиторных заданий
4	Криптографические протоколы	**6**	**4**		**4**			**10**	Оценка выполнения практических и внеаудиторных заданий
5	Нормативные акты, регламентирующие деятельность в области криптографической защиты информации	**6**	**4**		**4**			**10**	Оценка выполнения практических и внеаудиторных заданий
6	Средства и услуги в области криптографической защиты информации, представленные отечественном рынке	**6**	**4**		**6**			**10**	Оценка выполнения практических заданий
7	Экзамен	**6**					18		Экзамен по билетам / итоговая
	Итого:		**20**		**22**		**18**	**54**	

5. Обновление основной и дополнительной литературы (2020 г.)

В раздел **6. Учебно-методическое и информационное обеспечение дисциплины** вносятся следующие изменения:

Дополнить раздел Основная литература

Криптографические методы защиты информации: учебник для академического бакалавриата / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2019. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/433133

Дополнить раздел **Дополнительная литература**

Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — Москва : Издательство Юрайт, 2020. — 220 с. — (Высшее образование). — ISBN 978-5-9916-9244-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452871

6. В элемент рабочей программы **п.4 Образовательные технологии** вносятся следующие изменения:

В период временного приостановления посещения обучающимися помещений и территории РГГУ. для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции;

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

7. В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

Состав программного обеспечения (ПО)

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statisctics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statisctics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное
17	Zoom	Zoom	лицензионное

Составитель:
К.т.н, доцент, А.С. Моляков