МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

_Б1.В.ДВ.01.01_
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность корпоративных информационных систем
(наименование дисциплины)

по направлению подготовки (специальности)

09.04.03 Прикладная информатика
(код и наименование направления подготовки, специальности в соответствии с ФГОС ВПО/ФГОС ВО)

Информационные системы и технологии корпоративного управления
(направленность (профиль))

Форма обучения: _очная_

Год набора: _2019_

Общая трудоемкость: _7_ **ЗЕ**

Распределение часов дисциплины по семестрам

Семестр	**3**	**Итого**
Форма контроля / **Вид занятий**	зачет	
Лекции	**34**	**34**
Лабораторные	**8**	**8**
Практические	**50**	**50**
Руководство: курсовые работы (проекты) / РГР		
Промежуточная аттестация		
Контактная работа	**92**	**92**
Самостоятельная работа	**160**	**160**
Контроль		
Итого	**252**	**252**

Рабочую программу составил(и):
доцент кафедры «Прикладная математика и информатика» доцент к.т.н. Кузьмичев А.Б.

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:

☐ Отсутствует

☐ Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа составлена на основании ФГОС ВО и учебного плана направления подготовки (специальности)

09.04.03 Прикладная информатика

(код и наименование направления подготовки, специальности в соответствии с ФГОС ВПО)

Срок действия рабочей программы дисциплины до «31» августа 2021 г.

УТВЕРЖДЕНО

На заседании кафедры «Прикладная математика и информатика»

(протокол заседания № 1 от «30» 08 2018 г.).

1. Цель освоения дисциплины

Цель – развитие у обучающихся знаний и получении навыков по разработке и реализации защиты информации на основе современных методов криптографии в области построения и эксплуатации корпоративных информационных систем.

Задачи:

1. Сформировать у обучающихся продвинутые знания в области криптографических методов защиты информации.
2. Развить у обучающихся практические навыки в области проектирования и реализации криптосистем.
3. Выработать у обучающихся способность разрабатывать политику информационной безопасности с заданным уровнем защиты информации.

2. Место дисциплины (учебного курса) в структуре ОПОП ВО

Данная дисциплина (учебный курс) относится к Б1 "Дисциплины (модули)" (Дисциплины по выбору).

Дисциплины, учебные курсы, на освоении которых базируется данная дисциплина (учебный курс) – .

Дисциплины, учебные курсы, для которых необходимы знания, умения, навыки, приобретаемые в результате изучения данной дисциплины (учебного курса) – .

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
ПК-4: Способен управлять информационными ресурсами и ИС		Знать: – основные руководящие документы по реализации защиты информации, применительно к корпоративной информационной системе, – основы проведения политики безопасности – Хэш-функций, – базовые технологии защиты информации: идентификация и аутентификация, авторизация, аудит и шифрование.
		Уметь: – разрабатывать криптографическую систему на основе российских стандартов.
		Владеть: – навыками разработки системы реализации электронной цифровой подписи, – навыками разработки политики безопасности при внедрении и эксплуатации корпоративной информационной системы.
ПК-5: Способен управлять проектами по информатизации прикладных задач и созданию ИС предприятий и организаций		Знать: – Российские стандарты для криптографической защиты информации, применительно к корпоративной информационной системы – основы реализации электронной цифровой подписи – криптографические алгоритмы шифрования

		Уметь: – разрабатывать систему реализации электронной цифровой подписи – проводить анализ степени защиты корпоративной информационной системы методом сверху -вниз
		Владеть: – навыками разработки криптографической системы на основе современной среды программирования, применительно к корпоративной информационной системе.

4. Структура и содержание дисциплины Безопасность корпоративных информационных систем

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Криптографические алгоритмы защиты информации в корпоративных информационных системах	лекция	Симметричная криптографическая система	3	8		-	Собеседование (устный опрос)
	практ. занятие	Разработка программы по реализации блочного симметричного алгоритма шифрования	3	10	10	-	Отчет по практической работе (защита)
	практ. занятие	Разработка программы шифрования и дешифрирования произвольного файла по алгоритму создания цепочек OFB	3	8	8	-	Отчет по практической работе (защита)
	практ. занятие	Разработка программы реализации алгоритма хеширования для создания ключа на основе пароля	3	8	8	-	Отчет по практической работе (защита)
	практ. занятие	Разработка подсистемы шифрования для симметричной криптосистемы	3	8	8	-	Отчет по практической работе (защита)
	практ. занятие	Разработка подсистемы дешифрирования для симметричной криптосистемы	3	8	8	-	Отчет по практической работе (защита)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	3	26		-	
	лекция	Асимметричная криптографическая система	3	4		-	Собеседование (устный опрос)
	лабор. работа	Разработка программы сжатия данных с целью уменьшения энтропии информации по алгоритму RLE или LZW	3	4	4	-	Отчет по практической работе
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	3	28		-	
Стандарты информа-	лекция	Стандарты информационной безопасности	3	6		-	Собеседование (устный опрос)

ционной безопасности и модели безопасности информационных систем	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	3	20		-	
	лекция	Базовые технологии защиты информации в вычислительных сетях	3	4		-	Собеседование (устный опрос)
	лабор. работа	Разработка программы, реализующую симметричную криптосистему	3	4	4	-	Отчет по практической работе
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	3	26		-	
	лекция	Модели безопасности информационных систем	3	4		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	3	18		-	
Политика информационной безопасности	лекция	Анализ безопасности информации в корпоративной ин-формационной системе	3	4		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	3	18		-	
	лекция	Основы разработки политики информационной безопасности	3	4		-	Собеседование (устный опрос)
	практ. занятие	Разработка политики информационной безопасности организации	3	8	8	-	Отчет по практической работе (защита)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	3	24		-	
			3			-	
Итого				252	100		

Схема расчета итогового балла: текущий рейтинг (все занятия и промежуточные тесты) + Результат итогового теста, полученная сумма делится на 2

5. Образовательные технологии

В рамках изучения дисциплины предусмотрено использование следующих образовательных технологий:

- технология традиционного обучения;
- интерактивные технологии: учебные дискуссии (применяются во всех модулях по итогам выполнения работ).

Технологии традиционного обучения - организация учебного процесса в вузе, основанная на лекционных и практических формах обучения: объяснительно-иллюстративное обучение. Данная технология применяется во всех модулях курса.

Технология интерактивного обучения - организация учебного процесса, которая предполагает максимальную активность студентов в процессе формирования ключевых компетенций. На учебной дискуссии студенты представляют результат выполнения заданной работы. Проводится дискуссия по применённым решениям, обсуждается эффективность и архитектура программного кода.

6. Методические указания по освоению дисциплины

6.1 Рекомендации по подготовке к практическим занятиям

Студентам следует:

- при подготовке к занятиям обязательно использовать не только учебную литературу, но и другие источники;
- в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения;
- на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание путей решения поставленных задач и освоения выданных знаний, в случае затруднений обращаться к преподавателю.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения задачи, то нужно сравнить их и выбрать самый рациональный. Полезно до начала решения задачи составить краткий план решения задачи. Решение проблемных задач или примеров следует излагать подробно, отделяя вспомогательные пути решения от основных. Решения при необходимости нужно сопровождать комментариями, схемами, алгоритмами.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

6.2 Рекомендации по подготовке к итоговой сдаче дисциплины

Подготовка к итоговой сдаче предмета способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к ней, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На итоговой сдаче студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине.

Необходимо ориентировать студентов на систематическую подготовку к занятиям в течение семестра, что позволит использовать время экзаменационной сессии для систематизации знаний.

7. Оценочные средства

7.1Паспорт оценочных средств зачету

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
3	ПК-4	Тестовые задания по лекционному материалу. Вопросы по сдаче дисциплины. Отчеты по практическим занятиям.
3	ПК-5	Тестовые задания по лекционному материалу. Вопросы по сдаче дисциплины. Отчеты по практическим занятиям.

7.2Типовые задания или иные материалы, необходимые для текущего контроля

7.2.1 Вопросы для собеседования по модулю

Типовые примеры заданий

Модуль 1. Криптографические алгоритмы защиты информации в корпоративных информационных системах

1. Перечислите свойства информации.
2. Назовите предмет и объект защиты информации.
3. Что такое безопасность информации в компьютерных системах?
4. Что такое система защиты информации?
5. Что такое угроза безопасности информации?
6. Что такое конфиденциальность информации?
7. Что такое целостность информации?
8. Что такое доступность информации?
9. Перечислите случайные угрозы безопасности информации.
10. Что такое нарушитель информации и злоумышленник?
11. Перечислите преднамеренные угрозы безопасности информации.
12. Что такое криптография, криптоанализ и криптология?
13. Что такое криптосистема?
14. Перечислите и охарактеризуйте методы криптографических преобразований.
15. Дайте классификацию криптоалгоритмов.
16. Дайте понятие основных операций, используемых в алгоритмах шифрования.
17. Дайте понятие потокового и блочного шифра.
18. Перечислите операции, используемые в алгоритмах блочных шифров.
19. Приведите схему шифрования и дешифрирования по сети Фейстеля.
20. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
21. Что такое режимы шифрования?
22. Раскройте принцип реализации режима шифрования обратная связь по выходу (OFB).
23. Раскройте принципы внесения случайности в сообщения при шифровании.
24. Приведите способы генерации случайных чисел.
25. Понятие и свойства Хеш-функции.

26. Приведите пример алгоритма приведения пароля пользователя к заданной длине ключа с помощью Хеш-функции.
27. Приведите общую схема симметричной криптосистемы.
28. Основная идея асимметричных криптоалгоритмов?
29. Приведите необходимые условия реализации асимметричной криптографии.
30. Приведите примеры асимметричных критоалгоритмов.
31. Общая схема асимметричной криптосистемы.
32. Первый этап алгоритма RSA по созданию пары ключей.
33. Этап передачи зашифрованного сообщения в алгоритме RSA.
34. Понятие и свойства Хеш-функции.
35. Приведите примеры использования и реализаций криптографических Хеш-функций.
36. Раскройте алгоритм Меркеля-Дамгарда по реализации хеш-функции.
37. Алгоритм вычисления хеш-функции согласно ГОСТ Р 34.11-2012.
38. Схема алгоритма Девиса и Майера для хеширования паролей.
39. Назначение и виды защиты от злоумышленных действий при использовании ЭЦП.
40. Алгоритм формирования и проверки ЭЦП.
41. Алгоритм формирования ЭЦП по ГОСТ Р 34.10-2012.

Модуль 2. Стандарты информационной безопасности и модели безопасности информационных систем

1. Контрольные функции в области государственной безопасности, возложенные на ФСТЭК России?
2. Основные законы Российской Федерации, связанные с защитой информации.
3. Указы Президента, связанные с защитой информации.
4. Приказы ФСТЭК России, связанные с защитой информации.
5. Методические и руководящие документы ФСТЭК, связанные с защитой информации.
6. Статья Кодекса Административных правонарушений, Гражданского и Уголовного кодекса
7. 7 уровней безопасности, определенные в Оранжевой книге.
8. 6 базовых требований безопасности, определенные в Оранжевой книге.
9. 10 классов безопасности информации, установленные в европейских стандартах.
10. Перечислите и дайте понятия базовых технологий защиты информации.
11. Дайте классификацию процессов аутентификации.
12. В чем заключается строгая аутентификация.
13. В чем заключается простая аутентификация.
14. Основы биометрической аутентификации.
15. Что такое Хеширование пароля?
16. Дайте характеристики криптографических хеш-функций.
17. Дайте характеристики методов простой и биометрической аутентификации.
18. Приведите алгоритм строгой аутентификации на основе симметричных алгоритмов.
19. Что такое Модель политики информационной безопасности?
20. Приведите классы модели политики информационной безопасности.
21. Раскройте дискреционную модель Харрисона-Рузо-Ульмана.
22. Что такое матричное разграничения доступа. Приведите пример реализации.
23. Что такое мандатное разграничение доступа. Приведите пример реализации.

Модуль 3. Политика информационной безопасности

1. Перечислите основные пути получения информации о системе защиты?
2. Дайте классификацию информационных объектов по требуемой степени безотказности.
3. Дайте классификацию информационных объектов по уровню конфиденциальности.

4. Что такое риск информационной безопасности и как он вычисляется.
5. Перечислите уровни ущерба от реализации рисков.
6. Приведите пример формирования оценки вероятности атак на информацию.
7. Дайте алгоритм расчета риска информационной безопасности
8. Что такое политика информационной безопасности?
9. Перечислите требования к системе безопасности.
10. Раскройте принципа доступа к информационным ресурсам организации.
11. Опишите основные направления разработки политики безопасности.
12. Перечислите этапы разработки политики информационной безопасности

Критерии оценки:

Раскрытие 90-100% ответа на вопрос - 20 баллов; раскрытие 80-89% ответа на вопрос - 18 баллов; раскрытие 66-79% ответа на вопрос - от 15 баллов; раскрытие 50-65% ответа на вопрос - от 12 баллов; раскрытие менее 50% ответа на вопрос - от 0 до 11 баллов.

7.2.2 Комплект отчетов по практическим работам (примеры)

Типовые примеры заданий

Практическое занятие №1 «Разработка программы по реализации блочного симметричного алгоритма шифрования»

Форма отчета по практическому занятию №1
- титульный лист;
- задание;
- результат выполнения задания;
- результат эксперимента (таблицы и графики);
- выводы по работе.

Практическое занятие №2 «Разработка программы шифрования и дешифрирования произвольного файла по алгоритму создания цепочек OFB»

Форма отчета по практическому занятию №2
- титульный лист;
- задание;
- результат выполнения задания;
- результат эксперимента (таблицы и графики);
- выводы по работе.

Практическое занятие №3 «Разработка программы реализации алгоритма хеширования для создания ключа на основе пароля»

Форма отчета по практическому занятию №3
- титульный лист;
- задание;
- результат выполнения задания;
- результат эксперимента (таблицы и графики);
- выводы по работе.

Практическое занятие №4 «Разработка подсистемы шифрования для симметричной криптосистемы»

Форма отчета по практическому занятию №4
- титульный лист;
- задание;

- результат выполнения задания;
- результат эксперимента (таблицы и графики);
- выводы по работе.

Практическое занятие №5 «Разработка подсистемы дешифрирования для симметричной криптосистемы»

Форма отчета по практическому занятию №5
- титульный лист;
- задание;
- результат выполнения задания;
- результат эксперимента (таблицы и графики);
- выводы по работе.

Практическое занятие №6 «Разработка политики информационной безопасности организации»

Форма отчета по практическому занятию №6
- титульный лист;
- задание;
- результат выполнения задания;
- результат эксперимента (таблицы и графики);
- выводы по работе.

Требования к оформлению

Отчет должен содержать подробное описание (включая иллюстративный материл) последовательности действий проделанных студентом для выполнения заданий. Оформление отчета должно соответствовать методическому указанию рекомендациям, изложенным учебно-методическом пособии [Очеповский А.В. Общие требования по выполнению и оформлению контрольных, курсовых и выпускных квалификационный работ : Учебно-методическое пособие. – Тольятти : ТГУ, 2015. 78 с.].

Процедура оценивания

Оценка выполненной работы проводится по критериям:
1. Наличие всей существенной информации по работе
2. Точность и полнота предоставляемых сведений
3. Непротиворечивость приводимой информации
4. Правильность интерпретаций и выводов, которые сделаны по результатам работы
5. Степень достижения студентом поставленной цели
6. Обоснованность применяемого решения
7. Грамотность (содержательная) используемых формулировок

Критерии оценки за отчеты по практическим работам:

Полностью выполненное и вовремя защищенный отчет – максимальный балл. За каждое невыполненное задание снимаются баллы в соответствии с заданием на практическое занятие. Просрочка на 1 неделю - коэффициент 0,75, за две - 0,5, за три - 0,25, за четыре и более - 0 (учитывается факт сдачи).

7.3Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1 Вопросы к промежуточной аттестации

1. Методы защиты информации от несанкционированного изменения структуры систем
2. Источники, риски и формы атак на информацию

3. Организационные методы защиты информации.
4. Блочный шифр ГОСТ 28147-89
5. Алгоритмы архивации Хаффмана.
6. Алгоритмы архивации Лемпеля-Зива
7. Алгоритмы архивации RLE
8. Транспортное кодирование.
9. Хеширование паролей.
10. Общая схема симметричной криптосистемы
11. Общая схема асимметричной криптосистемы.
12. Алгоритм вычисления хеш-функции согласно ГОСТ Р 34.11-2012
13. ЭЦП с дополнительными свойствами.
14. Классификация процессов аутентификации.
15. Основы биометрической аутентификации и идентификации
16. Основы администрирования вычислительных сетей
17. Расчет рисков информационной безопасности
18. Методы внесения случайности в сообщения
19. Асимметричный алгоритм шифрования RSA
20. Основная законодательная база в области информационных технологий
21. Международные стандарты информационной безопасности
22. Основы хеширование и хранения паролей
23. Дискреционная модель Харрисона-Рузо-Ульмана
24. Реализация системы разграничения доступа в операционных системах
25. Основные пути получения информации о системе защиты информации
26. Понятие политики информационной безопасности
27. Режимы шифрования
28. Требования защищенности средств вычислительной техники от несанкционированного доступа к информации
29. Алгоритм Меркеля-Дамгарда по реализации хеш-функции
30. Алгоритм формирования ЭЦП по ГОСТ Р 34.10-2012
31. Основные понятия и определения безопасности информации.
32. Классификация угроз безопасности информации
33. Классификация методов противодействия угрозам безопасности информации.
34. Правовые методы защиты информации
35. Методы защиты информации от случайных угроз.
36. Методы защиты информации от шпионажа и диверсий.
37. Методы защиты информации от электромагнитных излучений и наводок.
38. Методы защиты информации от несанкционированного доступа.
39. Концепции построения систем разграничения доступа.
40. Криптографические методы защиты
41. Основы симметричных криптоалгоритмов.
42. Криптоалгоритм на основе сети Файстеля.
43. Блочный шифр DES
44. Алгоритмы создания цепочек.
45. Методы рандомизации сообщений.
46. Классификация алгоритмов архивации данных
47. Хеш-функция и её реализация
48. Понятие симметричной криптосистемы и ее функции
49. Асимметричные криптоалгоритмы
50. Асимметричный алгоритм шифрования RSA.
51. Электронная цифровая подпись
52. Основные понятия идентификации и аутентификации
53. Простая аутентификация

54. Методы строгой аутентификации.
55. Стандарты информационной безопасности.
56. Базовые технологии защиты информации в вычислительных сетях.
57. Модели безопасности операционных систем
58. Классификация информационных объектов по категориям информационной безопасности
59. Требования к системам защиты информации.
60. Порядок разработки политики информационной безопасности.
61. Многоуровневая защита систем обработки информации.

7.3.2 Критерии и нормы оценки

Семестр[i]	**Форма проведения промежуточной аттестации**[ii]	**Критерии и нормы оценки**[iii]	
3	Зачет (по накопительному рейтингу)	зачтено	От 40 до 100 баллов
		незачтено	'Менее 40 баллов.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1 Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС[iv]

8.2 Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1		Баранова Е. К. Информационная безопасность и защита информации [Электронный ресурс] : учеб. пособие / Е. К. Баранова, А. В. Бабаш. - 3-е изд., перераб. и доп. - Москва : РИОР : ИНФРА-М, 2017. - 322 с. : ил. - (Высшее образование). - ISBN 978-5-369-01450-	Учебное пособие	2017	ЭБС «Znanium.com»
2		Горюхина Е. Ю. Информационная безопасность [Электронный ресурс] : учеб. пособие / Е. Ю. Горюхина, Л. И. Литвинова, Н. В. Ткачева ; Воронеж. гос. аграр. ун-т им. Императора Петра I. -	Учебное пособие	2015	ЭБС «IPRbooks»

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
		Воронеж : ВГАУ им. Петра I, 2015. - 220 с.			
3		Джонс К. Д. Инструментальные средства обеспечения безопасности [Электронный ресурс] : [курс лекций] / К. Д. Джонс, М. Шема, Б. С. Джонсон. - 2-е изд., испр. - Москва : ИНТУИТ, 2016. - 915 с. : ил.	Учебное пособие	2016	ЭБС «IPRbooks»
4		Кукина Е. Г.Введение в криптографию [Электронный ресурс] : сборник задач и упражнений / Е. Г. Кукина, В. А. Романьков. - Омск : ОмГУ, 2013. - 91 с. - ISBN 978-5-7779-1588-7.	Учебное пособие	2013	ЭБС «IPRbooks»
5		Никифоров С. Н. Защита информации [Электронный ресурс] : учеб. пособие / С. Н. Никифоров. - Санкт-Петербург : СПбГАСУ, 2015. - 383 с. : ил. - ISBN 978-5-9227-0585-1.	Учебное пособие	2015	ЭБС «IPRbooks»
6		Спицын В. Г. Информационная безопасность вычислительной техники [Электронный ресурс] : учебное пособие / В. Г. Спицын. - Томск : Эль Контент, 2011. - 148 с. - ISBN 978-5-4332-0020-3.	Учебное пособие	2011	ЭБС «IPRbooks»
7		Технологии защиты информации в компьютерных сетях [Электронный ресурс] / Н. А. Руденков [и др.]. - 2-е изд., испр. - Москва : ИНТУИТ, 2016. - 369 с. : ил.	Учебное пособие	2016	ЭБС «IPRbooks»
8		Федин Ф. О. Информационная безопасность [Электронный ресурс] : учебное пособие / Ф. О. Федин, В. П. Офицеров, Ф. Ф. Федин ; [под ред. В. А. Дикарева]. - Москва : МГПУ, 2011. - 260 с.	Учебное пособие	2011	ЭБС «IPRbooks»

8.3 Перечень профессиональных баз данных и информационных справочных систем[v]

1. Hacking Everything. Режим доступа: http://www.gomzin.com/crypto-gram.html, 2016-01-01.
2. The Tiny Encryption Algorithm (TEA). Режим доступа: http://143.53.36.235:8080/tea.htm, 2016-01-01.
3. Библиотека: Защита информации, криптография. Режим доступа: http://www.win-ni.narod.ru/biblio/cryptobib.htm, 2016-01-01.
4. ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ. Режим доступа: http://www.scrf.gov.ru/documents/5.html, 2016-01-01.
5. Режимы шифрования Олег Зензин. Режим доступа: http://citforum.ru/security/cryptography/rejim_shifrov/, 2016-01-01.
6. Сайт Брюса Шнайера. Schneier on Security. Режим доступа: https://www.schneier.com/, 2016-01-01.
7. Федеральная служба по техническому и экспортному контролю. Режим доступа: http://fstec.ru/, 2016-01-01.

8.4Перечень программного обеспечения

№ п/п	Наименование ПО	Количество лицензий	Реквизиты договора (дата, номер, срок действия)
1	Microsoft DreamSpark версия Premium	1	652/2014 от 07.07.2014
2	Microsoft Office Standart 2007 версия 2007	неограниченный	
3	Microsoft Windows 7 версия 7	30	Бесплатно для учебных организаций

8.5Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий	Перечень основного оборудования	Фактический адрес учебных кабинетов, лабораторий, мастерских и др.	Площадь, $м^2$	Количество посадочных мест
1	Компьютерный класс. Помещение для самостоятельной работы. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполне-	Столы ученические, стулья ученические, ПК с выходом в сеть Интернет	445667 Самарская область, г.Тольятти, Центральный р-н, ул. Белорус-ская, д.14, позиция по ТП №48, 4 этаж, Г-401	84,8	16

	ния курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации.				
2	Компьютерный класс. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для проведения лабораторных работ. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации.	Компьютер (монитор 19”, системный блок Pentium (R) Dual-Core E5500 2,8 GHz / 4 Gb / 500 Gb) , стол ученический, стол компьютерный, стол преподавательский, стулья, Доска аудиторная(меловая).	445667 Самарская область, г.Тольятти, Центральный р-н, ул. Белорусская, д.16В, позиция по ТП №31, 4 этаж, УЛК-401	49,5	24
3	Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации.	Стол ученический двухместный (моноблок), доска аудиторная 3-х секционная (меловая), стол преподавательский, стул, проектор Acer	445667 Самарская область, г.Тольятти, Центральный р-н, ул. Белорусская, д.16В, позиция по ТП №50, 4 этаж, УЛК-418	90,6	80

[i] *Если дисциплина реализуется несколько семестров, то семестры указываются в одной таблице по порядку.*

[ii] *Указывается форма контроля (зачет, зачет с оценкой, экзамен) и в скобках форма проведения (устно, письменно, по накопительному рейтингу (для дисциплин, реализуемых с БРС)).*

[iii] *Если форма контроля «зачет», то оставить только строки с отметками о зачете, если форма контроля – «зачет с оценкой» или «экзамен», то оставить только строки с оценками.*

[iv] *Указывается количество экз. для печатных изданий, для электронных изданий – наименование ЭБС.*

[v] *Базы данных и информационные справочные системы должны быть актуальны.*