Федеральное государственное бюджетное образовательное учреждение
высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
Среднерусский институт управления - филиал
ФАКУЛЬТЕТ «ГОСУДАРСТВЕННОЕ, МУНИЦИПАЛЬНОЕ УПРАВЛЕНИЕ И ЭКОНОМИКА НАРОДНОГО ХОЗЯЙСТВА»
КАФЕДРА «Социология и информационные технологии»

Меркулов Павел Александрович

Подписан: Меркулов Павел Александрович
DN: C=RU, S=Орловская область, L=гор. Орел, T=Директор, OU="СРЕДНЕРУССКИЙ ИНСТИТУТ УПРАВЛЕНИЯ - ФИЛИАЛ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ ""РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ""", O="ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "" РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ""", СНИЛС=00482216008, ИНН=575206486423, E=it@orel.ranepa.ru, G=Павел Александрович, SN=Меркулов, CN=Меркулов Павел Александрович
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: Среднерусский институт управления

УТВЕРЖДЕНА
кафедрой «Социология и информационные технологии»
Протокол № 1 от "27" августа 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.35.05 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки (специальность) 38.05.01 «Экономическая безопасность»
Специализация: «Экономико-правовое обеспечение экономической безопасности»
Квалификация (степень) выпускника: экономист
Форма обучения: очная
Год набора: 2020

Орел, 2019 г.

Автор-составитель:
канд. техн. наук, доцент кафедры
«Социология и информационные технологии» В.В. Николаев

Заведующая кафедрой
«Социология и информационные технологии»
доктор социологических наук, доцент Н.В. Проказина

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы 4
2. Объем и место дисциплины в структуре образовательной программы 5
3. Содержание и структура дисциплины 6
4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине 7
5. Методические указания для обучающихся по освоению дисциплины 21
6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине 22
6.1. Основная литература
6.2. Дополнительная литература
6.3. Учебно-методическое обеспечение самостоятельной работы
6.4. Нормативные правовые документы
6.5. Интернет-ресурсы
6.6. Иные источники
7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы 24

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

1.1. Дисциплина «Информационная безопасность» обеспечивает овладение следующими компетенциями:

ОПК ОС - 6 Способность применять инструменты и механизмы нейтрализации и предотвращения экономических угроз в деятельности хозяйствующих субъектов;

ПК - 48 Способностью проводить специальные исследования в целях определения потенциальных и реальных угроз экономической безопасности организации.

Этапы освоения компетенций

Таблица 1

Код компетенции	Наименование компетенции	Код этапа освоения компетенций	Наименование этапа компетенции
ОПК ОС-6	Способность применять инструменты и механизмы нейтрализации и предотвращения экономических угроз в деятельности хозяйствующих субъектов	ОПК ОС -6.1	способность выявлять реальные и потенциальные угрозы информационной безопасности хозяйствующих субъектов, использовать организационно-правовые и экономические инструменты и механизмы по их предотвращению и нейтрализации при разработке и реализации комплекса мер по обеспечению информационной безопасности организации
ПК-48	Способностью проводить специальные исследования в целях определения потенциальных и реальных угроз экономической безопасности организации	ПК - 48.1	способностью применять современные методы научных исследований для выявления потенциальных и реальных угроз экономической безопасности организации

1.2. В результате освоения дисциплины у студентов должны быть:

Таблица 2

Результаты освоения компетенций

Код этапа освоения компетенции	Результаты обучения

ОПК ОС -6	***сформированы знания:*** - об основных принципах формирования на основе научных подходов современных систем обеспечения информационной безопасности хозяйствующих субъектов, месте и роли деятельности по выявлению, предотвращению и нейтрализации угроз экономической безопасности организации в данных системах; ***сформированы умения:*** - применять современные организационно-правовые и экономические инструменты и механизмы по предотвращению и нейтрализации угроз экономической безопасности организации при разработке и реализации комплекса мер по обеспечению ее информационной безопасности; ***сформированы навыки:*** - выявления на основе научных подходов потенциальных и реальных информационных угроз безопасности организации;
ПК - 48	***сформированы знания:*** – методов и приемов определения при анализе деятельности организации возможных источников угроз ее внешней и внутренней безопасности; ***сформированы умения:*** – находить и оценивать источники информации, анализировать данные, необходимые для проведения экономических расчетов, мониторинга текущего экономического и финансового состояния хозяйствующих субъектов на предмет надежности ресурсного потенциала, стабильности и устойчивости их деятельности; ***сформированы навыки:*** – осуществления мониторинга экономических процессов, сбора, анализа и оценки информации, имеющей значение для выявления рисков и угроз экономической безопасности организаций.

2. Объем и место дисциплины в структуре образовательной программы

Таблица 3

Объем дисциплины

Вид учебных занятий и самостоятельной работы	**Объем дисциплины, час.**											
	Всего	**Семестр**										
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Очная форма обучения												
Контактная аудиторная работа обучающихся с преподавателем, в том числе:	48				48							
Лекционного типа (Л)	16				16							
Лабораторные работы (ЛР)												
Практического типа (ПЗ)	32				32							
Контролируемая самостоятельная работа обучающихся (КСР):												
Контактная внеаудиторная работа,												

в т.ч. проводимая в электронной информационно- образовательной среде													
Самостоятельная работа обучающихся (СР) (всего):		69				69							
Промежуточная аттестация	**Форма**	Экзамен				Экз							
	Час.	27				27							
Общая трудоемкость (час./з.е.)		144 /4				144 /4							

Место дисциплины в структуре ОП ВО

Дисциплина «Информационная безопасность» изучается на 3-ем курсе в 6-ом семестре, общая трудоемкость дисциплины 4 з.е.

Дисциплина «Информационная безопасность» относится к базовой части подготовки специалистов по направлению 38.05.01 «Экономическая безопасность» специализация «Экономико-правовое обеспечение экономической безопасности».

Освоение дисциплины опирается на приобретенные ранее умения и навыки использования персонального компьютера и системного и прикладного программного обеспечения.

Дисциплина «Информационная безопасность» является предшествующей для дисциплин «Информационные системы в экономике», «Экономико-математическое моделирование», «Экономическая безопасность».

Форма промежуточной аттестации в соответствии с учебным планом - экзамен.

3. Содержание и структура дисциплины

Таблица 4

Структура дисциплины

№ п/п	Наименование тем (разделов)	Форма текущего контроля успеваемости / промежуточной аттестации						Форма текущего контроля успеваемости, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР, в том числе КВР	
			Л	ЛР	ПЗ	КСР		
Очная форма обучения								
1	Теоретические основы информационной безопасности	40	6		10		24	О1, Т1
2	Система обеспечения информационной безопасности	40	6		10		24	О2, Т2
3	Технологии защиты информации	37	4		12		21	О3, Т3

№ п/п	Наименование тем (разделов)	Форма текущего контроля успеваемости / промежуточной аттестации						Форма текущего контроля успеваемости, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР, в том числе КВР	
			Л	ЛР	ПЗ	КСР		
Промежуточная аттестация		**27**						**Экзамен**
Всего:		**144**	**16**		**32**		**69**	

Примечание. Форма текущего контроля успеваемости: опрос (О), тестирование (Т).

Содержание дисциплины

Тема 1. Теоретические основы информационной безопасности

Информационная безопасность: содержание и структура понятия. Законодательный уровень информационной безопасности. Стандарты информационной безопасности. Административный уровень информационной безопасности. Процедурный уровень информационной безопасности

Тема 2. Система обеспечения информационной безопасности

Организационный уровень информационной безопасности. Программно-технический уровень информационной безопасности. Методы и средства защиты информации. Оценка уровня защищенности ИС. Оценка рисков. Классификация угроз информационной безопасности. Построение модели угроз и модели нарушителя.

Тема 3. Технологии защиты информации

Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Основные алгоритмы и стандарты симметричного шифрования. Асимметричные криптосистемы шифрования. Алгоритмы асимметричного шифрования. Функция хэширования. Электронная цифровая подпись. Алгоритмы и стандарты ЭЦП. Проблемы обеспечения безопасности операционных систем. Функции межсетевых экранов. Концепция построения виртуальных защищенных сетей VPN. Компьютерные вирусы и проблемы антивирусной защиты. Обзор современных систем управления сетевой защитой.

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости и промежуточной аттестации.

4.1.1. В ходе реализации дисциплины «Информационная безопасность» используются следующие методы текущего контроля успеваемости обучающихся:

4.1.1. В ходе реализации дисциплины используются следующие методы текущего контроля успеваемости обучающихся:

- при проведении занятий лекционного типа: опрос;
- при проведении практических занятий: опрос, тестирование, практические задания.

4.1.2. Промежуточная аттестация проводится с применением следующих методов (средств):

Промежуточная аттестация по дисциплине проводится в виде устного экзамена. Экзаменационный билет включает два теоретических вопроса и (или) тестирование.

4.2. Материалы текущего контроля успеваемости

Типовые оценочные материалы по теме

Вопросы для подготовки к опросу

Тема 1. Теоретические основы информационной безопасности

1.Предмет и объект изучения дисциплины.

2.Базовые свойства информации с точки зрения информационной безопасности.

3.Основные международные стандарты в области ИБ.

4.Конфиденциальность, доступность, целостность информации как грани информационной безопасности.

5.Характеристика классов безопасности согласно «Оранжевой книге».

6.Основные этапы управления рисками.

7.Организационная зрелость предприятия с точки зрения информационной безопасности.

8.Механизм принудительного (мандатного) управления доступом.

9.Классификация информационных активов.

10.Идентификация, аутентификация и авторизация пользователя.

11.Базовые признаки классификации угроз.

12.Модель нарушителя.

Тема 2. Система обеспечения информационной безопасности

1.Классификация нормативно-правовых актов, регламентирующих сферу информационной безопасности.

2.Доктрина информационной безопасности Российской Федерации.

3.Основные законодательные акты, определяющие в целом юридические аспекты защиты информации.

4.Отношения, регулируемые законом от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации»

5.Российские стандарты, регулирующие ИБ.

6.Стандарт ГОСТ Р ИСО/МЭК 27001-2006 «Системы менеджмента информационной безопасности».

7.Характеристика стандарта ГОСТ Р ИСО/МЭК 15408 «Критерии оценки безопасности информационных технологий».

8.Административный уровень информационной безопасности.

Тема 3. Технологии защиты информации

1.Типичная схема ЛВС организации.

2.Сетевые протоколы TCP/IP.

3.Основные функции подсистемы защиты операционной системы.

4.Классификация криптосистем.

5.Симметричные криптосистемы.

6.Режимы работы блочных и поточных шифров.

7.Обобщенная схема асимметричной криптосистемы. Алгоритм шифрования RSA.

8.Классификация компьютерных вирусов. Антивирусные программы

9.Функции межсетевых экранов.

10.Основные режимы работы блочного симметричного алгоритма.

11.Концепция построения виртуальных частных сетей VPN.

12.Виды резервного копирования.

Материалы текущего контроля успеваемости

Тема 1. Теоретические основы информационной безопасности

Практическое занятие по теме 1. Исследование точности и сходимости математических моделей.

Методика выполнения:

1. Изучить теоретическую часть практического занятия и ответить на контрольные вопросы.

2. Выбрать задание в соответствии с порядковым номером студента в журнале группы.

3. Выполнить построение математической модели по заданным исходным данным.

4. Провести анализ точности и сходимости расчета.

5. Оформить отчет в соответствии с принятыми стандартами оформления документов и направить его преподавателю.

Тема 2. Система обеспечения информационной безопасности

Практическое занятие по теме 2. Исследование устойчивости сложных систем

Методика выполнения:

1. Изучить теоретическую часть практического занятия и ответить на контрольные вопросы.

2. Выбрать задание в соответствии с порядковым номером студента в журнале группы.

3. Выполнить построение математической модели по заданным исходным данным.

4. Провести анализ точности, сходимости и устойчивости расчета.

5. Оформить отчет в соответствии с принятыми стандартами оформления документов и направить его преподавателю.

Тема 3. Технологии защиты информации

Практическое занятие 2 по теме 3. Исследование методов ассиметричной криптографии Диффи-Хеллмана и RSA

Методика выполнения:

1. Изучить теоретическую часть практического занятия и ответить на контрольные вопросы.

2. Выбрать задание в соответствии с порядковым номером студента в журнале группы.

3. Выполнить построение математической модели по заданным исходным данным.

4. Провести анализ требований при использовании DH и RSA.

5. Оформить отчет в соответствии с принятыми стандартами оформления документов и направить его преподавателю.

Типовые тестовые задания по темам

Тема 1. Теоретические основы информационной безопасности

1. Концепция национальной безопасности Российской Федерации учитывает интересы:

а) личности и общества;
б) общества и государства;
в) личности, общества и государства;
г) избирателя, партий и органов законодательной власти

2. Основы государственной политики Российской Федерации в области международной информационной безопасности действуют до:

а) 2015 г.;
б) 2020 г.;
в) 2030 г.;
г) не являются действующим документом

3. Объект защиты информации - это:

а) служебные данные;
б) информация или носитель информации или информационный процесс;
в) носитель информации;
г) персонал

4. Несанкционированный доступ к информации - это:
а) доступ к информации с нарушением установленных правил доступа;
б) изменение или уничтожение данных;
в) доступ к информации без разрешения руководства;
г) копирование данных с нарушением установленных правил доступа
5. Стандарт ГОСТ Р ИСО/МЭК 27001-2006 определяет информационную безопасность как:
а) сохранение конфиденциальности, целостности и достоверности информации;
б) сохранение подлинности, целостности и доступности информации;
в) сохранение конфиденциальности, целостности и доступности информации;
г) сохранение подлинности, целостности и достоверности информации;
6. Первым этапом разработки и внедрения системы управления информационной безопасностью является:
а) вовлеченность руководства предприятия в процесс управления ИБ;
б) оценка информационных рисков;
в) оценка защищенности информационной системы;
г) инвентаризация активов
7. Принятие информационных рисков осуществляется в случае:
а) полного устранения источника риска;
б) если уровень рисков признается приемлемым;
в) перенесения ответственности за риск за страховые компании;
г) внедрения мер по снижению вероятности ущерба
8. Стандарт ГОСТ Р ИСО/МЭК 27002-2012 к защищаемым активам предприятия <u>не относит:</u>
а) информационные ресурсы;
б) программное обеспечение;
в) финансовые активы;
г) персонал, его квалификация, навыки и опыт
9. Стандарт TCSEC ("Оранжевая книга") к компьютерным системам с минимальной безопасностью относит группу:
а) A;
б) B;
в) C;
г) D
10. Первым этапом процедуры распознавания информационной системой пользователя является:
а) идентификация;
б) авторизация;
в) аутентификация;
г) верификация
11. В соответствии с Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации» обладатель информации <u>не обязан</u>:
а) соблюдать права и законные интересы иных лиц;
б) принимать меры к защите информации;
в) всегда проверять достоверность размещаемой общедоступной информации;
г) ограничивать доступ к информации, если это установлено федеральными законами
12. Защита информации в соответствии с Федеральным законом №149-ФЗ «Об информации, информационных технологиях и о защите информации» <u>не включает</u>:
а) обеспечение достоверности;
б) соблюдение конфиденциальности;
в) реализацию доступности;
г) оценку рисков

13. Владелец сайта обязан обеспечить соблюдение законодательства РФ, если число пользователей в сутки составляет:
а) 5000;
б) 3000;
в) 2000;
г) 1000
14. Среда для хранения и обработки данных пользователя, предоставляемая в виде онлайн-сервиса:
а) Всемирная паутина;
б) облачные технологии;
в) социальная сеть;
г) распределенные базы данных
15. Репликация данных - это:
а) проверка прав доступа к данным;
б) уничтожение данных;
в) проверка целостности;
г) копирование данных

Тема 2. Система обеспечения информационной безопасности
16. Стандарт ГОСТ Р ИСО/МЭК 27001-2006 называется:
а) Системы менеджмента информационной безопасности;
б) “Оранжевая книга”;
в) Критерии оценки безопасности информационных технологий;
г) Защита информации. Основные термины и определения
17. Стандарт ГОСТ Р ИСО/МЭК 27001-2006 определяет информационную безопасность как:
а) сохранение конфиденциальности, целостности и достоверности информации;
б) сохранение подлинности, целостности и доступности информации;
в) сохранение конфиденциальности, целостности и доступности информации;
г) защиту интересов личности, общества и государства
18. Стандарт ГОСТ Р ИСО/МЭК 27002-2012 относит к активам:
а) информационные ресурсы;
б) всё, что имеет ценность для организации;
в) программно-техническое обеспечение;
г) персонал, его квалификацию, навыки и опыт
19. Вторым этапом разработки и внедрения системы управления информационной безопасностью является:
а) инвентаризация активов;
б) оценка информационных рисков;
в) оценка защищенности информационной системы;
г) категорирование активов
20. Уклонение от информационных рисков осуществляется в случае:
а) полного устранения источника риска;
б) если уровень рисков признается приемлемым;
в) перенесения ответственности за риск за страховые компании;
г) внедрению мер по снижению вероятности ущерба
21. Вовлеченность руководства предприятия в процесс управления информационной безопасностью предполагает:
а) личный контроль и выполнение руководством требований ИБ;
б) личный контроль;
в) выполнение руководством требований ИБ;
г) постановку задач по обеспечению ИБ

22. Стандарт ГОСТ Р ИСО/МЭК 15408 называется:
а) об информации, информационных технологиях и защите информации;
б) система менеджмента информационной безопасности;
в) методы и средства обеспечения безопасности;
г) критерии оценки безопасности информационных технологий
23. Стандарт TCSEC ("Оранжевая книга") к компьютерным системам с максимальной безопасностью относит группу:
а) A;
б) B;
в) C;
г) D
24. Процедура предоставления законному пользователю соответствующих полномочий называется:
а) идентификация;
б) авторизация;
в) аутентификация;
г) верификация
25. Контроль за созданием средств защиты информации обеспечивается посредством:
а) обязательного лицензирования деятельности;
б) обязательного лицензирования деятельности и сертификацией средств защиты;
в) сертификацией средств защиты;
г) проведением единой технической политики
26. Максимальную скорость передачи данных обеспечивают:
а) беспроводная передача данных;
б) проводные линии связи;
в) оптоволоконные линии связи;
г) сотовые технологии
27. С точки зрения защиты информации наиболее уязвимы:
а) беспроводная передача данных;
б) проводные линии связи;
в) оптоволоконные линии связи;
г) бумажные технологии
28. Криптосистема с использованием разных ключей для зашифрования и расшифрования называется:
а) неоднородной;
б) симметричной;
в) асимметричной;
г) сложной
29. Инфраструктура открытых ключей называется:
а) PKI;
б) VPN;
в) ISP;
г) DNS
30. Попытка прочесть зашифрованный текст без знания ключа называется:
а) гаммирование;
б) расшифрование;
в) зашифрование;
г) дешифрование

Тема 3. Технологии защиты информации

31. Компонент ОС, позволяющий создать виртуальную машину, называется :

а) планировщик;
б) браузер;
в) реестр;
г) гипервизор

32. Криптосистема с использованием одного и того же ключа для зашифрования и расшифрования называется:
а) однородной;
б) симметричной;
в) асимметричной;
г) простой

33. Система криптографии с открытыми ключами называется:
а) однородной;
б) симметричной;
в) асимметричной;
г) сложной

34. Шифрование с использованием некоторой ключевой последовательности (гаммы) используется:
а) в блочных шифрах;
б) в поточных шифрах;
в) не используется;
г) в подстановочных криптограммах

35. Число уровней в модели взаимодействия открытых систем, предложенной ISO:
а) 7;
б) 6;
в) 5;
г) 4

36. В стеке протоколов TCP/IP к уровню приложений относится протокол:
а) HTTP;
б) IP;
в) TCP;
г) ARP

37. Протокол сетевого уровня в стеке протоколов TCP/IP:
а) HTTP;
б) TCP;
в) IP;
г) FTP

38. DNS-сервер предназначен для:
а) преобразования доменных имен компьютеров в IP-адреса;
б) обеспечения доступа компьютеров ЛВС в Интернет;
в) авторизации пользователей;
г) репликации данных

39. Прокси-сервер предназначен для:
а) резервного копирования информации;
б) обеспечения доступа компьютеров ЛВС в Интернет;
в) авторизации пользователей;
г) защиты от компьютерных вирусов

40. Межсетевой экран также называют:
а) прокси-сервер;
б) firewall и брандмауэр;
в) хаб;
г) маршрутизатор

41. Технология VPN:

а) обеспечивает защищенную связь поверх публичной сети;
б) обеспечивает резервное копирование данных;
в) используется только внутри ЛВС;
г) используется только в глобальных сетях

42. Задача центра сертификации в криптографии:
а) подтвердить наличие документированных процедур;
б) сертифицировать предоставляемые услуги;
в) подтвердить подлинность ключей шифрования;
г) обеспечить передачу зашифрованных данных

43. К функциям электронной цифровой подписи не относится:
а) удостоверение авторства;
б) невозможность отказа от авторства;
в) гарантирование целостности данных;
г) восстановление исходного текста документа

44. Компьютерный вирус, маскирующийся под легальное программное обеспечение, называется:
а) червь;
б) троян;
в) бот;
г) эксплойт

45. Дисковый массив RAID, обеспечивающий распределенное хранение данных и кодов четности:
а) RAID 0;
б) RAID 1;
в) RAID 5;
г) JBOD

Ответы на типовые тестовые задания

№ вопроса	ОТВЕТ
Тема 1	
1	В
2	Б
3	Б
4	А
5	В
6	Г
7	Б
8	В
9	Г
10	А
11	В
12	Г
13	В
14	Б
15	Г
Тема 2	
16	А
17	В
18	Б
19	Г
20	В
21	А
22	В
23	А
24	Б
25	Б

26	В
27	А
28	В
29	А
30	Г
Тема 3	
31	Г
32	Б
33	В
34	Б
35	А
36	А
37	В
38	А
39	Б
40	Б
41	А
42	В
43	Г
44	Г
45	В

Вопросы для контроля самостоятельной работы

1.Предмет и объект изучения дисциплины.

2.Организационная зрелость предприятия с точки зрения информационной безопасности.

3.Сущность объектно-ориентированного подхода применительно к проблемам информационной безопасности.

4.Базовые свойства информации с точки зрения информационной безопасности.

5.Основные международные стандарты в области ИБ.

6.Базовые признаки классификации угроз.

7.Основные законодательные акты, определяющие в целом юридические аспекты защиты информации.

8.Стандарт ГОСТ Р ИСО/МЭК 27001-2006 «Системы менеджмента информационной безопасности».

9.Конфиденциальность, доступность, целостность информации как грани информационной безопасности.

10.Отношения, регулируемые законом от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации»

11.«Оранжевая книга», как стандарт ИБ. Краткая характеристика.

12.Классификация нормативно-правовых актов, регламентирующих сферу информационной безопасности.

13.Характеристика классов безопасности согласно «Оранжевой книге».

14.Механизм принудительного (мандатного) управления доступом.

15.Административный уровень информационной безопасности.

16.Характеристика стандарта ГОСТ Р ИСО/МЭК 15408 «Критерии оценки безопасности информационных технологий».

17.Основные этапы управления рисками.

18.Российские стандарты, регулирующие ИБ.

19.Доктрина информационной безопасности Российской Федерации.

20.Классификация криптосистем.

21.Основные функции подсистемы защиты операционной системы.

22.Режимы работы блочных шифров.

23.Режим блочного симметричного алгоритма «Сцепление блоков».

24.Понятие «Профиль защиты»

25.Режим блочного симметричного алгоритма «Обратная связь по выходу».
26.Обобщенная схема асимметричной криптосистемы. Алгоритм шифрования RSA.
27.Режим блочного симметричного алгоритма «Обратная связь по шифротексту».
28.Идентификация, аутентификация и авторизация субъекта доступа.
29.Российские стандарты шифрования.
30.Блочные и поточные шифры.
31.Распределение криптографических ключей.
32.Межсетевые экраны.
33.Основные режимы работы блочного симметричного алгоритма.
34.Концепция построения VPN.
35.Виды резервного копирования.

4.3 Оценочные средства для промежуточной аттестации

Фонд оценочных средств по дисциплине утвержден и хранится на выпускающей кафедре.

4.3.1 Формируемые компетенции

Таблица 5

Код компетенции	**Наименование компетенции**	**Код этапа освоения компетенций**	**Наименование этапа компетенции**
ОПК ОС-6	способность применять инструменты и механизмы нейтрализации и предотвращения экономических угроз в деятельности хозяйствующих субъектов	ОПК ОС -6.1	способность выявлять реальные и потенциальные угрозы информационной безопасности хозяйствующих субъектов, использовать организационно-правовые и экономические инструменты и механизмы по их предотвращению и нейтрализации при разработке и реализации комплекса мер по обеспечению информационной безопасности организации
ПК-48	способность проводить специальные исследования в целях определения потенциальных и реальных угроз экономической безопасности организации	ПК - 48.1	способность определять и оценивать на основе научных подходов угрозы экономической безопасности при разработке и реализации комплекса мер по обеспечению информационной безопасности организации

Показатели и критерии оценивания компетенций с учетом этапа формирования установлены паспортами компетенций ОП ВО по направлению подготовки 38.05.01 «Экономическая безопасность» (приложение 1.2).

4.3.2 Типовые оценочные средства

Вопросы к экзамену

1.Понятие и предмет информационной безопасности.

2.Основные процессы преобразования информации. Информационная деятельность в модели архитектуры предприятия.

3.Базовые свойства информации с точки зрения информационной безопасности.

4.Законодательный уровень информационной безопасности.

5.Классификация нормативно-правовых актов, регламентирующих сферу информационной безопасности.

6.Основы государственной политики Российской Федерации в сфере информационной безопасности.

7.Основные законодательные акты РФ, определяющие в целом юридические аспекты защиты информации.

8.Основные российские и международные стандарты в области информационной безопасности.

9.Конфиденциальность, доступность, целостность информации как грани информационной безопасности.

10. Отношения, регулируемые законом от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации»

11. «Оранжевая книга», как стандарт ИБ. Краткая характеристика.

12. Уровни информационной безопасности

13. Административный уровень информационной безопасности.

14. Характеристика стандарта ГОСТ Р ИСО/МЭК 15408-1-2012. Методы и средства обеспечения безопасности.

15. Характеристика стандарта ГОСТ Р ИСО/МЭК 27001-2006. Системы менеджмента информационной безопасности.

16. Базовые признаки классификации угроз в сфере информационной безопасности.

17. Основные подходы к управлению рисками.

18. Классификация компьютерных вирусов.

19. Классификация сетевых атак на информационные системы.

20. Элементы информационной инфраструктуры.

21. Модель взаимодействия открытых систем ИСО.

22. Состав и характеристики стека протоколов TCP/IP.

23. Модель локальной вычислительной сети организации.

24. Способы идентификации компьютера в локальной вычислительной сети.

25. Назначение и функции прокси-сервера.

26. Функции межсетевых экранов в компьютерных сетях.

27. Концепция построения виртуальных частных сетей VPN.

28. Классификация криптографических методов защиты информации.

29. Обобщенная схема симметричной криптосистемы.

30. Блочные и поточные режимы шифрования.

31.Обобщенная схема асимметричной криптосистемы. Алгоритм шифрования RSA.

32. Хеширование. Электронная цифровая подпись.

33. Основные функции подсистемы защиты операционной системы.

34. Особенности численных методов расчета с точки зрения информационной безопасности.

35. Этапы разработки и внедрения системы менеджмента информационной безопасности.

36. Политика информационной безопасности организации

37. Цели, методы и средства обеспечения информационной безопасности.

38. Общие принципы при управлении персоналом с точки зрения ИБ.

39. Основные принципы управления средствами информационно-коммуникационных технологий (ИКТ).
40. Идентификация, аутентификация и авторизация субъекта доступа.
41. Принципы управления доступом к информационной системе.
42. Методы контроля целостности данных.
43. Виды резервного копирования данных.
44. Мониторинг и аудит системы обеспечения информационной безопасности.

Типовые тестовые задания для промежуточного контроля

1. Компонент ОС, позволяющий создать виртуальную машину, называется :
а) планировщик;
б) браузер;
в) реестр;
г) гипервизор

2. Криптосистема с использованием одного и того же ключа для зашифрования и расшифрования называется:
а) однородной;
б) симметричной;
в) асимметричной;
г) простой

3. Система криптографии с открытыми ключами называется:
а) однородной;
б) симметричной;
в) асимметричной;
г) сложной

4. Шифрование с использованием некоторой ключевой последовательности (гаммы) используется:
а) в блочных шифрах;
б) в поточных шифрах;
в) не используется;
г) в подстановочных криптограммах

5. Число уровней в модели взаимодействия открытых систем, предложенной ISO:
а) 7;
б) 6;
в) 5;
г) 4

6. В стеке протоколов TCP/IP к уровню приложений относится протокол:
а) HTTP;
б) IP;
в) TCP;
г) ARP

Описание показателей и критериев оценивания на различных этапах их формирования описание шкал оценивания

Промежуточная аттестация по дисциплине проводится в виде экзамена.

Шкала оценивания экзамена: отлично, хорошо, удовлетворительно, неудовлетворительно.

Таблица 6

Наименование темы	**Код компетенции**	**Критерии оценивания**	**Оценка**
1. Теоретические	ОПК ОС-6	Студент владеет знаниями, умениями и	Отлично

основы информационной безопасности		навыками в рамках дисциплины в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину; самостоятельно, в логической последовательности и исчерпывающе отвечает на все вопросы, подчеркивал при этом самое существенное, умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделять в нем главное: устанавливать причинно-следственные связи; четко формирует ответы, свободно читает результаты анализов и других исследований и решает ситуационные задачи повышенной сложности; хорошо знаком с основной литературой и методами исследования в объеме, необходимом для практической деятельности; увязывает теоретические аспекты предмета с практическими задачами; владеет знаниями основных принципов изучаемых наук. Студент владеет знаниями, умениями и навыками в рамках дисциплины почти в полном объеме программы (имеются пробелы знаний только в некоторых, особенно сложных разделах); самостоятельно и отчасти при наводящих вопросах дает полноценные ответы на вопросы; не всегда выделяет наиболее существенное, не допускает вместе с тем серьезных ошибок в ответах; умеет решать легкие и средней сложности ситуационные задачи; умеет трактовать лабораторные и инструментальные исследования в объеме, превышающем обязательный минимум. Студент владеет основным объемом знаний, умений и навыков в рамках дисциплины; проявляет затруднения в самостоятельных ответах, оперирует неточными формулировками; в процессе ответов допускаются ошибки по существу вопросов; способен решать лишь наиболее легкие задачи, владеет только обязательным минимумом методов исследований. Студент не освоил обязательного минимума знаний, умений и навыков в	
2. Система обеспечения информационной безопасности	ПК-48		Хорошо
3. Технологии защиты информации	ПК-48		Удовлетворительно Неудовле-

		рамках дисциплины, не способен ответить на вопросы даже при дополнительных наводящих вопросах	творительно

4.4. Методические материалы

Изучение дисциплины завершается устным экзаменом в 6 семестре, который проводится по всему содержанию дисциплины. В самом начале учебного курса желательно ознакомиться со следующей учебно-методической документацией:

- программой дисциплины;
- перечнем знаний и умений, которыми студент должен владеть;
- тематическими планами лекций, практических занятий;
- контрольными мероприятиями;
- учебником, учебными пособиями по дисциплине, а также электронными ресурсами;
- перечнем примерных вопросов к экзамену.

Непосредственная подготовка к экзамену осуществляется по вопросам, представленным в данной рабочей программе. Необходимо тщательно изучить формулировку каждого вопроса, вникнуть в его суть, желательно составить план ответа. Обычно план включает в себя:

- показ теоретической и практической значимости рассматриваемого вопроса;
- обзор освещения вопроса в истории;
- определение сущности рассматриваемого предмета;
- основные элементы содержания и структуры предмета рассмотрения;
- факторы, логику и перспективы эволюции предмета;
- показ роли и значения рассматриваемого материала для практической деятельности.

План ответа желательно развернуть, приложив к нему ссылки на первоисточники с характерными цитатами. Необходимо отметить для себя пробелы в знаниях, которые следует ликвидировать в ходе подготовки, для чего возможно обратиться за консультацией к преподавателю.

В данном курсе изучаются вопросы обеспечения информационной безопасности в Российской Федерации и организации.

В связи с этим студенты должны хорошо понимать сущность системы обеспечения информационной безопасности, включающей в себя методы и средства обеспечения безопасности и систему менеджмента информационной безопасности.

Студенты должны хорошо представлять себе роль и место информационные безопасности в системе менеджмента качества и обеспечения непрерывности бизнес-процессов.

Обучение по дисциплине «Информационная безопасность» предполагает изучение курса на аудиторных занятиях (лекционные, практические и лабораторные занятия), а также самостоятельной работы студентов. При изучении дисциплины «Информационная безопасность» рекомендуется пользоваться контрольными вопросами к каждой теме, программой курса, рекомендуемой основной и дополнительной литературой.

К каждой теме занятий студентам необходимо готовиться заранее. Существенным аспектом изучения курса является знакомство с компьютерными и информационными системами, в том числе на лабораторных и практических занятиях. Основным нормативно-правовым документом при изучении курса «Информационная безопасность» является Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 19.12.2016) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.01.2017).

В процессе подготовки к практическим занятиям студентам предлагается выполнить следующие домашние задания:

- ознакомиться с вопросами к теме, рассматриваемой на лекции и практическом занятии.
- выполнить тестовые задания по теме.

5. Методические указания для обучающихся по освоению дисциплины

Обучение по дисциплине «Информационная безопасность» предполагает изучение курса на аудиторных занятиях (лекции, практические занятия, лабораторные работы) и самостоятельной работы студентов.

Практические занятия дисциплины «Информационная безопасность» предполагают их проведение в различных формах с целью выявления полученных знаний, умений, навыков и компетенций с проведением контрольных мероприятий.

С целью обеспечения успешного обучения студент должен готовиться к лекции, она является важнейшей формой организации учебного процесса, поскольку:

–знакомит с новым учебным материалом;

–разъясняет учебные элементы, трудные для понимания;

–систематизирует учебный материал;

–ориентирует в учебном процессе.

Подготовка к лекции заключается в следующем:

–внимательно прочитайте материал предыдущей лекции;

–узнайте тему предстоящей лекции (по тематическому плану, по информации лектора);

–ознакомьтесь с учебным материалом по учебнику и учебным пособиям;

–постарайтесь уяснить место изучаемой темы в своей профессиональной подготовке;

–запишите возможные вопросы, которые вы зададите лектору на лекции.

Подготовка к практическим и лабораторным занятиям:

–внимательно прочитайте материал лекций относящихся к данному семинарскому занятию, ознакомьтесь с учебным материалом по учебнику и учебным пособиям;

–выпишите основные термины;

–ответьте на контрольные вопросы по семинарским занятиям, готовьтесь дать развернутый ответ на каждый из вопросов;

–уясните, какие учебные элементы остались для вас неясными и постарайтесь получить на них ответ заранее (до семинарского занятия) во время текущих консультаций преподавателя;

–готовиться можно индивидуально, парами или в составе малой группы, последние являются эффективными формами работы;

–рабочая программа дисциплины в части целей, перечню знаний, умений, терминов и учебных вопросов может быть использована вами в качестве ориентира в организации обучения.

Подготовка к экзамену. К экзамену необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить дисциплину в период зачётно-экзаменационной сессии, как правило, показывают не слишком удовлетворительные результаты. В самом начале учебного курса познакомьтесь со следующей учебно-методической документацией:

–программой дисциплины;

–перечнем знаний и умений, которыми студент должен владеть;

–тематическими планами лекций, семинарских занятий;

–контрольными мероприятиями;

–учебником, учебными пособиями по дисциплине, а также электронными ресурсами;

–перечнем вопросов к экзамену.

После этого у студента должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине.

Систематическое выполнение учебной работы на лекциях и практических занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи экзамена.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Основная литература

Таблица 7

Основная литература

Данные об издании					Печатная форма (кол-во в библио-теке)	Ссылка на ЭБС
№ п/п	Автор	Название	Издатель-ство	Год изда-ния		
1	Нестеров С.А.	Информационная безопасность. Учебник и практикум для академического бакалавриата	М.: - Юрай	2018	-	https://biblio-online.ru/viewer/836C32FD-678E-4B11-8BFC-F16354A8AFC7/informacionnaya-bezopasnost#page/1
2	Полякова Т.А. - отв. ред., Стрельцов А.А. - отв. ред.	Организационное и правовое обеспечение информационной безопасности. Учебник и практикум для бакалавриата и магистратуры	М.: - Юрай	2018	-	https://biblio-online.ru/viewer/D056DF3D-E22B-4A93-8B66-EBBAEF354847/organiza

						cionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti#/
3	В.Ю. Рогозин [и др.].	Основы информационной безопасности	М.: ЮНИТИ-ДАНА	2017		http://www.iprbookshop.ru/72444.html.
4	Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов	Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры	М.: - Юрайт	2019		https://biblio-online.ru/book/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-432966
5	С. А. Нестеров	Информационная безопасность: учебник и практикум для академического бакалавриата	М.: - Юрайт	2019		https://biblio-online.ru/book/informacionnaya-bezopasnost-434171

6.2. Дополнительная литература

Таблица 8

Дополнительная литература

Данные об издании					Печатная форма (кол-во в библиотеке)	Ссылка на ЭБС
№ п/п	Автор	Название	Издательство	Год издания		
1	Мельников В.П., Клейменов С.А.	Информационная безопасность и защита информации	Академия	2010	3	
2	Аверченков В.И.	Аудит информационной безопасности	ФЛИНТА	2011		http://e.lanbook.com/books/element.php?pl1_id=44799
3	Коваленко Ю.И.	Правовой режим лицензирования и сертификации в сфере информационной безопасности	Горячая линия-Телеком	2012		http://e.lanbook.com/books/element.php?pl1_id=5163
4	Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.	Основы управления информационной безопасностью	Горячая линия-Телеком	2012		http://e.lanbook.com/books/element.php?pl1_id=5178

5	О. В. Казарин, И. Б. Шубинский	Надежность и безопасность программного обеспечения: учебное пособие для бакалавриата и магистратуры	М.: - Юрайт	2019		https://biblio-online.ru/book/nadezhnost-i-bezopasnost-programmnogo-obespecheniya-441287

6.3. Учебно-методическое обеспечение самостоятельной работы

1. Николаев В.В. Основы информационной безопасности: Учебно-методическое пособие. – Орел: Изд-во СИУ РАНХиГС, 2017.

6.4. Нормативные правовые документы

1. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 19.12.2016) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.01.2017). URL: http://consultant.ru.
2. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных". URL: http://consultant.ru.
3. Указ Президента РФ от 5 декабря 2016 г. N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" / Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru/.

6.5. Интернет-ресурсы

1. Официальный портал ОФ РАНХиГС. URL: orel.ranepa.ru.
2. Корпоративный облачный сервис «Битрикс24». URL: www.bitrix24.ru.
3. Облачный сервис для совместной работы над документами “GoogleDocs”. URL: www.docs.google.com/?hl=ru.
4. Облачный сервис для совместной работы над документами “MSOneDrive”. URL: https://onedrive.live.com.

6.6. Иные источники

1.Николаев В.В. Особенности реализации домена с тонкими клиентами на базе Microsoft Windows Server 2012 R2 // Технические науки - от теории к практике: Сб. ст. по материалам LVII междунар. науч.-практ. конф. №4(52). - Новосибирск: Изд. АНС “СибАК”, 2016.- С.70-77

2.Николаев В.В. Информационная система мониторинга защищенности образовательных учреждений // Наука вчера, сегодня, завтра: Сб. статей по материалам XXXVI Междунар. науч.-практ. конф. №7(29).- Новосибирск: Изд. АНС «СибАК», 2016.- С. 13-19

7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Таблица 9

Материально-техническая база

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа

Учебная аудитория для проведения занятий лекционного типа, семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации 302001, Орловская область, г.Орёл, ул. Панчука, д.1, Литер А1	Столы ученические, стулья, аудиторная доска трехстворчатая меловая, видеопроектор acer m342, экран с эл. приводом Screen Media Champion 229x305.	ГК 035410000801-4000043-0010007- 43-0010007-01 от 30.01.2015
Учебная аудитория для проведения занятий семинарского типа, лабораторных занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации 302001, Орловская область, г.Орёл, ул. Панчука, д.1, Литер А1	Столы, стулья, кафедра настольная, аудиторная доска меловая, трехстворчатая, шкаф металлический, двухстворчатый Ноутбуки Lenovo g505 в составе: Процессор AMD E1-2100 APU 1GHz, ОЗУ 4 Gb, Жесткий диск 500Gb, ОС windows 8.1. Лицензии на програмное обеспечение: Microsoft Windows 8.1 Professional - OPEN License № 62760494 от 03.12.2013 Office Std 2013 - OPEN License №62760467 от 03.12.2013 Office Professional Plus 2007 - OPEN License №47729487 от 25.11.2010 Kaspersky Endpoint Security 10 для Windows - Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition. 250-499 Node 2 year Educational Renewal License до 03.01.2018, лицензии GNU LGPL license	ГК 030-0010007-01 от 20.12.2014
Компьютерный класс (аудитория для выполнения самостоятельной работы) /Учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации 302001, Орловская об-	Столы компьютерные, столы ученические, стулья для компьютеров, стулья, кафедра настольная, аудиторная доска трехстворчатая меловая. компьютеры в составе: системный блок: процессор AMD A4-6300 3.7 GHz, ОЗУ 8Gb, жесткий диск 500Gb, монитор ViewSonic VA2261-2, ОС windows 8.1 ОС windows 8.1 профессиональная. Лицензии на програмное обеспечение: Microsoft Windows 8.1 Professional - OPEN License № 62760494 от 03.12.2013 Office Professional Plus	ГК 0354100008016000010-0010007- 01 от 22.08.2016.

ласть, г.Орёл, ул. Панчука, д.1, Литер А1	2007 - OPEN License №47729487 от 25.11.2010 Kaspersky Endpoint Security 10 для Windows - Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition. 250-499 Node 2 year Educational Renewal License до 03.01.2018, лицензии GNU LGPL license	
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения оборудования.	

Таблица 10

Перечень программного обеспечения, необходимого для реализации дисциплины

Наименование программного обеспечения	**Назначение и тип лицензии программного обеспечения**
ИПС «КонсультантПлюс» URL: http://www.consultant.ru/	Информационно-поисковая система, позволяющая работать с нормативно-правовыми актами, учебной и научной литературой. Лицензионная версия
7-Zip	Архиватор с высокой степенью сжатия Свободная лицензия
Adobe reader – Russian	Просмотр, печать и внесение аннотаций в документы PDF. Свободная лицензия
Adobe Acrobat Reader DC– Russian	Чтение, печать и рецензирование файлов PDF. Свободная лицензия
AgroUML 0.34	Средство UML моделирования. ArgoUML является открытым программным обеспечением и распространяется под лицензией EPL.
AnyLogic 7.3.5 Personnel Learning edition	программное обеспечение для имитационного моделирования. Any Logic доступен бесплатно для обучения студентов и самообразования. Свободная лицензия
Deductor Academic	Deductor — платформа для создания законченных аналитических решений. В платформу встроены современные методы извлечения, визуализации данных и анализа данных. Свободная лицензия
DIA	Свободный кросс платформенный редактор диаграмм, часть GNOME Office. Свободная лицензия
Expert Decide (собственная разработка)	Система авторами отнесена к классу систем поддержки принятия решений (СППР) и. Свободная лицензия
Google Chrome	Браузер Свободная лицензия
Java	Представляет собой язык программирования и платформу вычислений Свободная лицензия

Microsoft SQL Server 2008 Express	Является бесплатным выпуском SQL Server и представляет собой платформу данных для обучения и создания небольших серверных приложений, которые могут распространяться независимыми поставщиками программного обеспечения. Свободная лицензия
Microsoft Visual C++ 2005 redistributable Microsoft Visual C++ 2008 redistributable - x64 9.0.30729.6161 Microsoft Visual C++ 2008 redistributable - x64 9.0.60729.4148 Microsoft Visual C++ 2008 redistributable – x86 9.0.30729 Microsoft Visual C++ 2008 redistributable – x86 9.0.30729.4148 Microsoft Visual C++ 2008 redistributable – x86 9.0.30729.6161 MicrosoftVisualC++ 2008, экспресс-выпуск – пакет обновления 1(SP1) – Rus Microsoft Visual C++ 2010 x64 redistributable – 10.0.40219 Microsoft Visual C++ 2010 x86 redistributable – 10.0.40219 Microsoft Visual C++ 2010 x86 redistributable – 10.0.40219 Microsoft Visual C++ 2012 redistributable (x64) – 11.0.51106 Microsoft Visual C++ 2013 redistributable (x64) – 12.0.30501	Интегрированная среда разработки приложений на языке C++. Свободная лицензия
Mozilla FireFox	Браузер. Свободная лицензия
MySQL Workbench 6.3 CE	Инструмент для визуального проектирования баз данных, интегрирующий проектирование, моделирование, создание и эксплуатацию БД в единое бесшовное окружение для системы баз данных MySQL. Версия Community Edition — распространяется по свободной лицензией GNU GPL.
NetBeans IDE 6.7.1	Свободная интегрированная среда разработки приложений (IDE) на языках программирования Java, Python, PHP, JavaScript, C, C++, Ада и ряда других Свободная лицензия
Opera	Браузер. Свободная лицензия

Oracle VM VirtualBox	Программный продукт виртуализации для операционных систем MicrosoftWindows, Linux, FreeBSD, Mac OS X, Solaris/OpenSolaris, ReactOS, DOS и других. Свободная лицензия
Ramus Educational	Может быть использован для создания диаграмм в формате IDEF0 и DFD. Ramus Education использует формат файлов полностью совместимый с форматом файла коммерческой версии Ramus. Свободная лицензия
Word Tabulator	Предназначена для анализа текстов в среде MS Windows. Свободная лицензия
Yandex Браузер	Браузер Свободная лицензия
Декларация 2009 Декларация 2011 Декларация 2012 Декларация 2013 Декларация 2014	Свободно распространяемая программа для автоматически формирования налоговых деклараций по формам 3-НДФЛ и 4-НДФЛ. Распространяется через сайт ФНС Свободная лицензия
Налогоплательщик ЮЛ	Программа предназначена для автоматизации процесса подготовки юридическими и физическими лицами документов налоговой и бухгалтерской отчётности, расчета страховых взносов, справок о доходах физических лиц (форма №2-НДФЛ), специальных деклараций (декларирование активов и счетов), документов по регистрации ККТ и других. Распространяется через сайт ФНС. Свободная лицензия
ТС-Обмен НП	Программа подготовки заявлений налогоплательщика при импорте товаров и уплате косвенных налогов в рамках соглашения о Таможенном союзе. Распространяется через сайт ФНС. Свободная лицензия
Apache Open Office	Свободный пакет офисных приложений. Свободная лицензия
SPSS Statistics 22 for Windows	Компьютерная программа для статистической обработки данных, предназначенных для проведения прикладных исследований в социальных науках. Лицензированная версия
Kaspersky Endpoint Security 10 для Windows	Антивирус - Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition. 250499 Node 2 year Educational Renewal License – лицензия до 2018-01-03 Лицензированная версия
Windows XP Professional Windows 7 Professional Windows 8 Pro Windows 8.1 Pro	Операционные системы. Лицензированная версия
WindowsServer 2003 R2 WindowsServer 2008 Std/Ent Windows Server Enterprise 2008 R2 Windows Server 2012	Серверные операционные системы. Лицензированная версия

Essentials WindowsServer 2012 Standard	
Office Professional Plus 2007 (Access 2007, Communicator 2007, Excel 2007, InfoPath 2007, Outlook 2007, PowerPoint 2007, Publisher 2007, Word 2007) Office Professional Plus 2010 (Microsoft Excel 2010, Microsoft Outlook 2010, Microsoft PowerPoint 2010, Microsoft Word 2010, Microsoft Access 2010, Microsoft InfoPath 2010, Microsoft Communicator, Microsoft Publisher 2010, Microsoft OneNote 2010, Microsoft SharePoint Workspace 2010) Office Standard 2007 Word 2007, Excel 2007, PowerPoint 2007, Outlook 2007) Office Standard 2010 Word 2010, Excel 2010, PowerPoint 2010, OneNote 2010, Outlook 2010, Publisher 2010) Office Standard 2013 (Microsoft Office Word 2013, Microsoft Excel 2013, Microsoft PowerPoint 2013, Microsoft OneNote 2013, Microsoft Publisher 2013, Microsoft Outlook 2013)	Пакет офисных приложений. Лицензированная версия
“ДЕЛО-предприятие” под СУБД MS SQL Server	Система электронного документооборота (СЭД). Версия для учебных заведений
eDocLib под СУБД MS SQL Server	Web-ориентированная ECM система для управления бизнес-процессами. Версия для учебных заведений