Частное образовательное учреждение высшего образования

«Курский институт менеджмента, экономики и бизнеса»

УТВЕРЖДАЮ:

Первый проректор - проректор по учебной работе и дистанционному обучению

_____ В.В. Закурдаева

«1» сентября 2019г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.02.01 «Защита информации в компьютерных системах и сетях»

Направление подготовки

09.04.03 Прикладная информатика

Профиль "Информационные системы в организационном управлении и бизнес-процессах"

Курск 2019

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО по направлению подготовки 09.04.03 Прикладная информатика, утвержденным приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 916.

Разработчики:

д.т.н., профессор	А.В. Филонович	
(занимаемая должность)	*(ФИО)*	*(подпись)*

ст. преподаватель МЭБИК	Шумаков А.Н,.	
(занимаемая должность)	*(ФИО)*	*(подпись)*

Рабочая программа дисциплины одобрена на заседании кафедры Прикладной информатики и математики
Протокол №1 от «30» августа 2019 г.

Заведующий кафедрой: к.ф-мат.н., доцент Федоров А.В. _____
(ученая степень, звание, Ф.И.О.) *(подпись)*

1. Цель и задачи освоения дисциплины

Цель дисциплины: формирование у обучающихся знаний и умений по защите компьютерных сетей с применением современных программно-аппаратных средств.

Задачи:

ознакомление студентов с:

- основными понятиями и определениями защиты информации;
- источниками, рисками и формами атак на информацию; угрозами, которым подвергается информация;
- вредоносными программами;
- защитой от компьютерных вирусов и других вредоносных программ; методами и средствами защиты информации;

2. Место дисциплины в структуре программы

Дисциплина Б1.В.ДВ.02.01 «Защита информации в компьютерных системах и сетях» входит в блок Б1 «Часть, формируемая участниками образовательных отношений» учебного плана.

Освоение дисциплины «Защита информации в компьютерных системах и сетях» опирается на знания и умения, приобретенные студентами при изучении следующих дисциплин программы:

- Математическое моделирование
- Информационное общество и проблемы прикладной информатики)
- Актуальные проблемы информационного права

Изучение дисциплины «Защита информации в компьютерных системах и сетях» необходимо для успешного освоения дисциплин:

- Современные технологии разработки программного обеспечения
- Производственная практика
- Выполнение и защита выпускной квалификационной работы

3. Требования к планируемым результатам освоения дисциплины:

3.1 Обучающийся должен:

знать:

- виды угроз КС и методы обеспечения защиты информации;
- основные задачи и понятия криптографии;
- модели шифров и математические методы их исследования;

уметь:

- использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки;
- пользоваться научно технической литературой в области защиты информации

владеть:

- навыками использования ПЭВМ в анализе простейших шифров;
- навыками использования типовых криптографических алгоритмов

3.2 В результате изучения дисциплины обучающийся должен освоить:

обобщенную трудовую функцию: управление работами по сопровождению и проектами создания (модификации) ИС, автоматизирующих задачи организационного управления и бизнес-процессы

трудовые функции:

- разработка инструментов и методов документирования существующих бизнес-процессов организации заказчика (реверс-инжиниринга бизнес-процессов организации);
- разработка инструментов и методов проектирования бизнес-процессов заказчика;
- экспертная поддержка разработки прототипов ИС;

трудовые действия:

- разработка и выбор инструментов и методов описания бизнес-процессов;
- разработка инструментов и методов сбора исходных данных у заказчика;
- разработка и выбор инструментов и методов проектирования бизнес-процессов;
- разработка и выбор инструментов и методов моделирования бизнес-процессов в ИС;
- выработка вариантов реализации прототипов ИС на основе накопленного опыта;

профессиональную компетенцию

Код	Наименование компетенции	наименование показателя достижения компетенции
ПК-3	Способен формировать стратегию информатизации прикладных процессов и создания прикладных ИС в соответствии со стратегией развития предприятий	Знает основы инновационного и стратегического управления организацией; основы информационного менеджмента; основы инжиниринга и реинжиниринга информационных и бизнес-процессов организации; основы информационной безопасности.

4. Объем дисциплины и виды учебной работы

Очная форма обучения

Вид учебной работы	Всего часов	Семестр(ы)		
		3		
Контактная работа (всего)	24.3	24.3		
В том числе:				
Лекционные занятия	12	12		
Практические занятия	12	12		
Контактная работа на промежуточной аттестации	0.3	0.3		
Самостоятельная работа	83.7	83.7		
ИТОГО:	**108**	**108**		
з.е.	**3**	**3**		

Заочная форма обучения

Вид учебной работы	Всего часов	Семестр(ы)		
		4		
Контактная работа (всего)	4.3	4.3		
В том числе:				
Лекционные занятия	2	2		
Практические занятия	2	2		
Контактная работа на промежуточной аттестации	0.3	0.3		
Самостоятельная работа	100	100		
Часы на контроль	3.7	3.7		
ИТОГО:	**108**	**108**		
з.е.	**3**	**3**		

5. Структура и содержание дисциплины

5.1. Разделы/темы дисциплины и виды занятий

Очная форма обучения

№ п/п	Наименование разделов/тем дисциплины	Лекции	Прак. занятия	СРС	Катт	Контроль
1.	Угрозы безопасности компьютерным системам	1		10		
2.	КС и их компоненты как объекты защиты	1		10		
3.	Методика построения защищенных КС	1		10		
4.	Организационные меры и средства ЗИ в КС	1	3	10		
5.	Технические СЗИ в КС	2	3	10		
6.	Технические средства контроля доступа к	2	3	10		

	компонентам КС					
7.	Методы и средства уничтожения компьютерной информации	2	3	10		
8.	Технические средства защиты компьютерных коммуникаций	2		13.7		
	ИТОГО:	**12**	**12**	**83.7**	**0.3**	

Форма обучения Заочная

№ п/п	**Наименование разделов/тем дисциплины**	**Лекции**	**Прак. занятия**	**СРС**	**Катт**	**Контроль**
1.	Угрозы безопасности компьютерным системам	0,5		12		
2.	КС и их компоненты как объекты защиты	0,5		12		
3.	Методика построения защищенных КС		0,5	12		
4.	Организационные меры и средства ЗИ в КС	0,5		12		
5.	Технические СЗИ в КС		0,5	12		
6.	Технические средства контроля доступа к компонентам КС	0,5		12		
7.	Методы и средства уничтожения компьютерной информации		0,5	14		
8.	Технические средства защиты компьютерных коммуникаций		0,5	14		
	ИТОГО:	**2**	**2**	**100**	**0.3**	**3.7**

5.2. Содержание разделов/тем дисциплины

№ п/п	Наименование раздела/темы дисциплины	Содержание раздела/темы
1.	Угрозы безопасности компьютерным системам	Основные понятия информационной безопасности; Классификации угроз безопасности КС; Каналы, способы и средства воздействия угроз
2.	КС и их компоненты как объекты защиты	Объекты защиты в КС; Классификация КС и характеристика классов
3.	Методика построения защищенных КС	Разработка системы организационных и физических мер защиты КС; Разработка системы программно-технических мер защиты КС
4.	Организационные меры и средства ЗИ в КС	Характеристика организационных мер и средств защиты КС; Документирование мероприятий по ЗИ
5.	Технические СЗИ в КС	Технические средства защиты КС от НСД; Технические методы и средства защиты целостности и бесперебойности функционирования компонентов КС
6.	Технические средства контроля доступа к компонентам КС	Классификация систем контроля доступа (СКД); СКД на основе считывания ключевой информации; Системы с использованием смарт-карт; СКД на основе считывания биометрических признаков; Исполняющие подсистемы СКД
7.	Методы и средства уничтожения компьютерной информации	Особенности хранения компьютерной информации на физических носителях; Методы уничтожения информации без разрушения носителя.
8.	Технические средства защиты компьютерных коммуникаций	Использование активного коммуникационного оборудования; Серверы доступа и модемы DSL; Маршрутизаторы (routers); Аппаратные криптосистемы

6. Компетенции обучающегося, формируемые в процессе освоения дисциплины

Наименование раздела/темы дисциплины	Формируемые компетенции
Угрозы безопасности компьютерным системам	ПК-3
КС и их компоненты как объекты защиты	ПК-3
Методика построения защищенных КС	ПК-3
Организационные меры и средства ЗИ в КС	ПК-3
Технические СЗИ в КС	ПК-3
Технические средства контроля доступа к компонен-	ПК-3

там КС	
Методы и средства уничтожения компьютерной информации	ПК-3
Технические средства защиты компьютерных коммуникаций	ПК-3

7. Методические рекомендации преподавателям по дисциплине[1]

Аудиторная работа проводится в виде традиционных лекционно-практических занятий, проблемно-поисковых технологий по реинжинирингу бизнес-процессов. По дисциплине разработаны индивидуальные задания (см.ФОМы), направленные на реализацию компетентностно-орентированного бакалавра по реинжинирингу бизнес-процессов.

8. Методические рекомендации для преподавателей для проведения текущего контроля успеваемости/промежуточной аттестации по дисциплине

Текущий контроль успеваемости в рамках дисциплины проводятся с целью определения степени освоения обучающимися образовательной программы.

Текущий контроль успеваемости обучающийся проводится по каждой теме учебной дисциплины и включает контроль знаний на аудиторных и внеаудиторных занятиях в ходе выполнения самостоятельной работы.

Промежуточная аттестация обучающихся проводится в форме сдачи **зачета** в 3 семестре.

Зачет сдается согласно расписанию и служит формой проверки учебных достижений обучающихся по всей программе учебной дисциплины и преследуют цель оценить учебные достижения за академический период. Обучающийся может быть освобожден от сдачи промежуточной аттестации в случае успешного прохождения заданий из ФОМ.

Вопросы к зачету для студентов ОФО и ЗФО

1. Понятия безопасности и уязвимости автоматизированной системы.
2. Виды доступа к информации.
3. Понятия конфиденциальности, целостности и доступности.
4. Понятие политики безопасности. Обеспечение безопасности автоматизированной системы.
5. Основные угрозы безопасности автоматизированной системе.
6. Принципы криптографической защиты информации.
7. Понятие симметричной криптосистемы.
8. Шифрующие таблицы.
9. Системы шифрования Цезаря.
10. Шифрующие таблицы Трисемуса.
11. Биграммный шифр Плейфейра.
12. Система шифрования Вижинера.

13. Шифр "двойной квадрат" Уитстона
14. Одноразовая система шифрования.
15. Шифрование методом Вернама.
16. Шифрование методом гаммирования.
17. Методы генерации псевдослучайных последовательностей чисел.
18. Стандарт шифрования данных DES.
19. Алгоритм шифрования данных IDEA.
20. ГОСТ 28147-89.
21. Понятие блочных и поточных шифров.
22. Понятие асимметричной криптосистемы.
23. Однонаправленные функции.
24. Криптосистема шифрования данных RSA.
25. Схема шифрования Полига-Хеллмана.
26. Схема шифрования Эль-Гамаля.
27. Принципы идентификации и проверки подлинности.
28. Типовые схемы идентификации и аутентификации.
29. Понятие электронной цифровой подписи.
30. Алгоритмы электронной цифровой подписи.
31. Уязвимости основных сетевых протоколов.
32. Особенности политики сетевой безопасности.
33. Фильтрующие маршрутизаторы.
34. Шлюзы сетевого уровня.
35. Шлюзы прикладного уровня.
36. Понятие усиленной аутентификации.
37. Основные схемы сетевой защиты на базе межсетевых экранов.
38. Аппаратно-программные средства криптографической защиты информации и системы защиты информации от несанкционированного доступа.
39. Стандарты в области защиты информации.
40. Законодательство в области защиты информации.

9. Методические рекомендации обучающимся по освоению дисциплины, в том числе для самостоятельной работы обучающихся

9.1. Работа над понятиями

1. Знать термин.
2. Выделить главное в понятии.
3. Выучить определение.

4. Уметь использовать понятие в различных формах ответа.

9.2. Запись лекции

1. Настроиться на запись лекции (состояние внутренней готовности, установка).
2. Соблюдать единый орфографический режим:
а) записать дату, тему, план, рекомендованную литературу;
б) вести запись с полями;
в) выделять главное, существенное (подчеркивая, абзацы, цвет, пометки на полях и т.д.).
3. Запись вести сжато, но без искажения содержания.
4. Выделять основные понятия, определения, схемы, факты, сведения, статистические данные.

9.3. Работа с источником информации:

1. Познакомиться в целом с содержанием источника информации:
а) чтение аннотации источника;
б) чтение вступительной статьи;
в) просматривание оглавления;
г) чтение источника с выделением основных проблем и выводов;
д) работа со словарем с целью выяснения значений понятий.
2. Составить план темы:
а) выделить логически законченные части;
б) выделить в них главное, существенное;
в) сформулировать вопросы или пункты плана;
г) ставить вопросы по прочитанному.

9.4. Конспектирование:

1.Определить цель конспектирования.
2.Составить план.
3. Законспектировать источник:
а) указать автора статьи, ее название, место и год написания, страницы;
б) составить конспект по следующим формам (по указанию преподавателя или выбору студента): 1. Цитатный план. 2. Тезисный план.

9.5. Выполнение практических работ

1. Ознакомиться с методичекими рекомендациями по выполнению практической работы
2. Выполнить практическую работу

10. Перечень информационных технологий

При осуществлении образовательного процесса студентами и профессорско-преподавательским составом используются следующее:	
Оборудование:	**Проектор;** **Интерактивная доска;** **Ноутбук;** **Экран на треноге;** **ПК;** **Колонки.**
Программное обеспечение и информационно справочные системы:	ЭБС Znanium; Консультант плюс; WindowsXPProfessionalSP3; Windows 7; MicrosoftOffice 2007; MicrosoftOffice 2010; Антивирус DoctorWeb; Gimp 2; CorelDrawGraphicsSuiteX4;

	1С Предприятие 8. Комплект для обучения в высших и средних учебных заведениях

11. Учебно-методическое и информационное обеспечение дисциплины:

а) основная литература

1. Защита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М. : РИОР : ИНФРА-М, 2018. - 392 с. - (Высшее образование: Бакалавриат; Магистратура). — https://doi.org/10.12737/4868. - Режим доступа: http://znanium.com/catalog/product/937469

б) дополнительная литература

1. Шаньгин В.Ф. Информационная безопасность. Издательство ДМК-Пресс, 2014г
2. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Издательство: ДМК Пресс, 2012 г
3. Мельников В.В. Безопасность информации в автоматизированных системах. М.: Финансы и статистика, 2003. – 368 с.
4. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий.. 2-е изд. СПб.: БХВ-Петенрбург, 2003. – 368 с.: ил.
5. ГОСТ 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
6. Аверченков В.И., Рытов М.Ю. Организационная защита информации: учебное пособие для вузов. – Издательство: ФЛИНТА, 2011 г.
7. Аверченков В.И., Рытов М.Ю., Кувыклин А.В., Гайнулин Т.Р. Разработка системы технической защиты информации: учебное пособие.– Издательство: ФЛИНТА, 2011 г.

в) Интернет-ресурсы:

1. ЭБС http://znanium.com
2. http://www.intuit.ru
3. http://www.networkdoc.ru
4. http://www.interface.ru
5. http://mrybakov.ru/order/business/business_processes
6. http://www.wikipro.ru
7. http://quality.eup.ru/MATERIALY/deming.htm

12. Материально-техническое обеспечение дисциплины:

Наименование оборудованных учебных кабинетов, лабораторий	**№ аудитории**	**Перечень оборудования и технических средств обучения**
Учебные аудитории для проведения занятий лекционного типа. Кабинеты, оснащенные мультимедийным оборудованием	№001, №002, №215, №309, №406	Средства звуковоспроизведения с мультимедийными комплексами для презентаций, интерактивная доска. Ноутбук, комплект мультимедиа, экран, техническое и программное обеспечение, подключение к Internet, доска фломастерная, флип-чат.
Учебные аудитории для проведения занятий семинарского типа/практических занятий. Учебные аудитории для групповых и индивидуальных консультаций. Учебные аудитории для текущего контроля и промежуточной аттестации.	№202, №107, №110, №207	Учебные рабочие места • Компьютер Cel 3 ГГц, 512Мб, 120Гб, FDD, • КомпьютерIntel Pentium Dual CPU 1,8 ГГц, 2048 Мб • Компьютер Intel Core i3 CPU 3,4 ГГц, 4 Гб • Компьютер Intel Core i5 CPU 3,2 ГГц, 4 Гб • Лицензионное программное обеспечение - Windows XP Professional SP3, Windows 7 • Microsoft Office 2007, 2010 • 1С Предприятие 8. Комплект для обучения в высших и средних учебных заведениях • Антивирус Doctor Web • Консультант Плюс • Corel Draw Graphics Suite X4 • Adobe Connect 9 (вебинар)
Помещение для самостоятельной работы	№102	столы компьютерные 13 шт., столы с дополнительным расширением для инвалидов и лиц с ОВЗ 2 шт., стулья 6 шт., компьютеры benq 17” lcd/cel 3мгц /512 mb/80 gb9 шт. доска фломастерная 2-х сторонняя передвижная 1 шт., сплит-система LG1 шт., жалюзи (пластик) 4 шт., кресло 9 шт., огнетушитель 1 шт.
Библиотека	№004	Каталожная система библиотеки – для обучения студентов умению пользоваться системой поиска литературы
Читальный зал библиотеки	№003	Рабочие места с ПК – для обучения работе с индексирующими поисковыми системами в Internet

Наименование оборудованных учебных кабинетов, лабораторий	**№ аудитории**	**Перечень оборудования и технических средств обучения**
Аудитория для хранения учебного оборудования	№111	