Частное образовательное учреждение
высшего образования
«Брянский институт управления и бизнеса»

УТВЕРЖДАЮ
Заведующий кафедрой информатики и
программного обеспечение
_____ Т.М. Хвостенко
«27» августа 2020 г.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Укрупненная группа направлений и специальностей	090000 Информатика и вычислительная техника
Направление подготовки:	09.03.03.62 Прикладная информатика
Профиль:	Прикладная информатика (в экономике)

Разработал: Ионан Ю.Э.

Брянск 2020

1. ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ ПО ФГОС ВО

В соответствии с учебным планом направления подготовки, разработанным на основе Федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика, утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017г. № 922, дисциплина «Информационная безопасность» входит в обязательную часть. Эта дисциплина, в соответствии с учебным планом, является обязательной для изучения.

2. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность» включает 19 тем. Темы объединены в четыре дидактические единицы: «Концепция информационной безопасности», «Угрозы информации», «Виды возможных нарушений информационной системы», «Информационная безопасность информационных систем».

Цель изучения дисциплины заключается в ознакомлении с комплексом проблем информационной безопасности предпринимательских структур различных типов и направлений деятельности, построения и функционирования совокупности правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сферах охраны интеллектуальной собственности предпринимателей и сохранности их информационных ресурсов.

Основными **задачами** изучения дисциплины являются:

1. овладение способностью осуществлять инсталляцию и настройку параметров программного обеспечения информационных систем;
2. овладение способностью принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью;
3. изучение основных направлений обеспечения информационной безопасности, меры законодательного, административного, процедурного и программно-технического уровней при работе на вычислительной технике и в каналах связи;
4. приобретение теоретических и практических навыков по использованию современных методов защиты информации в компьютерных системах;
5. формирование практических навыков и способностей осуществления мероприятий по обеспечению информационной безопасности функционирования информационной системы при взаимодействии с информационными рынками по сетям или с использованием иных методов обмена данными.

3. ТРЕБОВАНИЯ К УРОВНЮ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Информационная безопасность» направлено на формирование следующих планируемых результатов обучения студентов по дисциплине. Планируемые результаты обучения (ПРО) студентов по этой дисциплине являются составной частью планируемых результатов освоения образовательной программы и определяют следующие требования. После освоения дисциплины студенты должны:

Овладеть компетенциями:

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической

культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно- исследовательской работе с учетом требований информационной безопасности.

ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью**.**

Знать: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.

Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.

Владеть: навыками составления технической документации на различных этапах жизненного цикла информационной системы.

4. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Для изучения дисциплины, необходимы знания и умения из дисциплин, изучаемых ранее по учебному плану:

1. Операционные системы
2. Базы данных

Согласно учебному плану дисциплина «Информационная безопасность» изучается в 4 семестре 2 курса при очной форме обучения, в 8 семестре 4 курса при заочной форме обучения (4 г. 6 мес.), в 10 семестре 5 курса при заочной форме обучения (5 лет).

Компетенции, знания и умения, приобретаемые студентами после изучения дисциплины, будут использоваться ими в ходе осуществления профессиональной деятельности.

5. ВИДЫ УЧЕБНОЙ РАБОТЫ И ИХ ТРУДОЕМКОСТЬ

очная форма обучения

Вид учебной работы	Всего зачетных единиц (академических часов – ак. ч.)	Семестр
		4
Общая трудоемкость дисциплины	3 (108)	3 (108)
Аудиторные занятия (контактная работа обучающихся с преподавателем), из них:	60	60
- лекции (Л)	30	30
- семинарские занятия (СЗ)		
- практические занятия (ПЗ)	30	30
- лабораторные занятия (ЛЗ)		
Самостоятельная работа студента (СРС), в том числе:	48	48
- курсовая работа (проект)		
- контрольная работа		
- доклад (реферат)		
- расчетно-графическая работа		
Вид промежуточной аттестации	Зачет с оценкой	Зачет с оценкой

заочная форма обучения (5 лет)

Вид учебной работы	Всего зачетных единиц (академических часов – ак. ч.)	Семестр
		10
Общая трудоемкость дисциплины	3 (108)	3 (108)
Аудиторные занятия (контактная работа обучающихся с преподавателем), из них:	36	36
- лекции (Л)	16	16
- семинарские занятия (СЗ)		
- практические занятия (ПЗ)	20	20
- лабораторные занятия (ЛЗ)		
Самостоятельная работа студента (СРС), в том числе:	72	72
- курсовая работа (проект)		
- контрольная работа	9	9
- доклад (реферат)		
- расчетно-графическая работа		
Вид промежуточной аттестации	Зачет с оценкой	Зачет с оценкой

заочная форма обучения (4 г. 6 мес.)

Вид учебной работы	Всего зачетных единиц (академических часов – ак. ч.)	Семестр
		8
Общая трудоемкость дисциплины	3 (108)	3 (108)
Аудиторные занятия (контактная работа обучающихся с преподавателем), из них:	12	12
- лекции (Л)	4	4
- семинарские занятия (СЗ)		
- практические занятия (ПЗ)	8	8
- лабораторные занятия (ЛЗ)		
Самостоятельная работа студента (СРС), в том числе:	96	96
- курсовая работа (проект)		
- контрольная работа	9	9
- доклад (реферат)		
- расчетно-графическая работа		
Вид промежуточной аттестации	Зачет с оценкой	Зачет с оценкой

6. тематическая структура дисциплины

№ п.п	**Наименование модуля**	**№ п.п.**	**Тема**	**Перечень планируемых результатов обучения (ПРО)**
1	Концепция информационной безопасности.	1	Актуальность информационной безопасности.	ОПК-3 ОПК-4
		2	Пользователи и	

			злоумышленники в Интернет	
		3	Лицензирование и сертификация в области защиты информации.	
		4	Основные нормативные руководящие документы	
2	Угрозы информации.	5	Виды угроз информационной безопасности РФ	ОПК-3 ОПК-4
		6	Информационная безопасность сетей.	
		7	Способы совершения компьютерных преступлений.	
		8	Уязвимость сети Интернет.	
		9	Обеспечение информационной безопасности.	
3	Виды возможных нарушений информационной системы.	10	Компьютерные преступления.	ОПК-3 ОПК-4
		11	Вредоносные программы.	
		12	Вирусы.	
		13	Признаки заражения компьютера	
		14	Антивирусное программное обеспечение.	
4	Информационная безопасность информационных систем.	15	Теория информационной безопасности информационных систем.	ОПК-3 ОПК-4
		16	Криптографические способы защиты информации.	
		17	Организация информационной безопасности компании.	
		18	Угрозы информационной безопасности для автоматизированной системы обработки информации	
		19	Контроль доступа к информации	

7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

очная форма обучения

№ п.п.	Темы дисциплины	Трудоемкость	Лекции	ПЗ	СРС
1	Актуальность информационной	6	2	1,5	2,5

	безопасности.				
2	Пользователи и злоумышленники в Интернет	6	1,5	2	2,5
3	Лицензирование и сертификация в области защиты информации.	6	1,5	1,5	3
4	Основные нормативные руководящие документы	5,5	1,5	1,5	2,5
5	Виды угроз информационной безопасности РФ	5,5	1,5	1,5	2,5
6	Информационная безопасность сетей.	5,5	1,5	1,5	2,5
7	Способы совершения компьютерных преступлений.	5,5	1,5	1,5	2,5
8	Уязвимость сети Интернет.	6	1,5	2	2,5
9	Обеспечение информационной безопасности.	5,5	1,5	1,5	2,5
10	Компьютерные преступления.	5,5	1,5	1,5	2,5
11	Вредоносные программы.	5,5	1,5	1,5	2,5
12	Вирусы.	5,5	1,5	1,5	2,5
13	Признаки заражения компьютера	6	2	1,5	2,5
14	Антивирусное программное обеспечение.	5,5	1,5	1,5	2,5
15	Теория информационной безопасности информационных систем.	5,5	1,5	1,5	2,5
16	Криптографические способы защиты информации.	5,5	1,5	1,5	2,5
17	Организация информационной безопасности компании.	5,5	1,5	1,5	2,5
18	Угрозы информационной безопасности для автоматизированной системы обработки информации	6	2	1,5	2,5
19	Контроль доступа к информации	6	1,5	2	2,5
Итого:		**108**	**30**	**30**	**48**

заочная форма обучения (5 лет)

№ п.п.	**Темы дисциплины**	**Трудоемкость**	**Лекции**	**ПЗ**	**СРС**
1	Актуальность информационной безопасности.	4			4
2	Пользователи и злоумышленники в Интернет	5		2	3
3	Лицензирование и сертификация в области защиты информации.	6	2		4
4	Основные нормативные руководящие документы	6	2		4
5	Виды угроз информационной безопасности РФ	5		2	3
6	Информационная безопасность сетей.	5		2	3
7	Способы совершения компьютерных преступлений.	5		2	3
8	Уязвимость сети Интернет.	7	2	1	4

9	Обеспечение информационной безопасности.	5		1	4
10	Компьютерные преступления.	7	2	1	4
11	Вредоносные программы.	5		1	4
12	Вирусы.	5		1	4
13	Признаки заражения компьютера	5		1	4
14	Антивирусное программное обеспечение.	7	2	1	4
15	Теория информационной безопасности информационных систем.	5		1	4
16	Криптографические способы защиты информации.	7	2	1	4
17	Организация информационной безопасности компании.	7	2	1	4
18	Угрозы информационной безопасности для автоматизированной системы обработки информации	5		1	4
19	Контроль доступа к информации	7	2	1	4
Итого:		**108**	**16**	**8**	**72**

заочная форма обучения (4 г. 6 мес.)

№ п.п.	Темы дисциплины	Трудоемкость	Лекции	ПЗ	СРС
1	Актуальность информационной безопасности.	6			6
2	Пользователи и злоумышленники в Интернет	5,5		0,5	5
3	Лицензирование и сертификация в области защиты информации.	5,5	0,5		5
4	Основные нормативные руководящие документы	5,5	0,5		5
5	Виды угроз информационной безопасности РФ	5,5		0,5	5
6	Информационная безопасность сетей.	5,5		0,5	5
7	Способы совершения компьютерных преступлений.	5,5		0,5	5
8	Уязвимость сети Интернет.	6	0,5	0,5	5
9	Обеспечение информационной безопасности.	5,5		0,5	5
10	Компьютерные преступления.	6	0,5	0,5	5
11	Вредоносные программы.	5,5		0,5	5
12	Вирусы.	5,5		0,5	5
13	Признаки заражения компьютера	5,5		0,5	5
14	Антивирусное программное обеспечение.	6	0,5	0,5	5
15	Теория информационной безопасности информационных систем.	5,5		0,5	5
16	Криптографические способы защиты информации.	6	0,5	0,5	5

17	Организация информационной безопасности компании.	6	0,5	0,5	5
18	Угрозы информационной безопасности для автоматизированной системы обработки информации	5,5		0,5	5
19	Контроль доступа к информации	6	0,5	0,5	5
Итого:		**108**	**4**	**8**	**96**

8. СЕМИНАРСКИЕ ЗАНЯТИЯ

Учебным планом не предусмотрены.

9. ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

Учебным планом предусмотрено проведение практических занятий по дисциплине.

Рекомендуемые темы для проведения практических занятий:

при очной форме обучения:

1. Актуальность информационной безопасности.
2. Пользователи и злоумышленники в Интернет
3. Лицензирование и сертификация в области защиты информации.
4. Основные нормативные руководящие документы
5. Виды угроз информационной безопасности РФ
6. Информационная безопасность сетей.
7. Способы совершения компьютерных преступлений.
8. Уязвимость сети Интернет.
9. Обеспечение информационной безопасности.
10. Компьютерные преступления.
11. Вредоносные программы.
12. Вирусы.
13. Признаки заражения компьютера
14. Антивирусное программное обеспечение.
15. Теория информационной безопасности информационных систем
16. Криптографические способы защиты информации.
17. Организация информационной безопасности компании.
18. Угрозы информационной безопасности для автоматизированной системы обработки информации
19. Контроль доступа к информации

при заочной форме обучения:

1. Пользователи и злоумышленники в Интернет
2. Виды угроз информационной безопасности РФ
3. Информационная безопасность сетей.
4. Способы совершения компьютерных преступлений.
5. Уязвимость сети Интернет.
6. Обеспечение информационной безопасности.
7. Компьютерные преступления.
8. Вредоносные программы.
9. Вирусы.
10. Признаки заражения компьютера
11. Антивирусное программное обеспечение.
12. Теория информационной безопасности информационных систем.
13. Криптографические способы защиты информации.
14. Организация информационной безопасности компании.
15. Угрозы информационной безопасности для автоматизированной системы

обработки информации
16. Контроль доступа к информации

10. ЛАБОРАТОРНЫЕ РАБОТЫ

Учебным планом не предусмотрены.

11. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

11.1. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Рекомендуются следующие виды самостоятельной работы:

- выполнение контрольной работы
- изучение теоретического материала с использованием курса лекций и рекомендованной литературы;
- подготовка к зачету с оценкой в соответствии с перечнем контрольных вопросов для аттестации;
- дидактическое тестирование.

В комплект учебно-методического обеспечения самостоятельной работы обучающихся входят:

- методические указания для выполнения контрольной работы
- рабочая программа дисциплины;
- оценочные материалы.

11.2. КУРСОВАЯ РАБОТА (ПРОЕКТ)

Учебным планом не предусмотрено.

11.3. КОНТРОЛЬНАЯ РАБОТА

Учебным планом предусмотрено написания контрольной работы. Требования к написанию контрольных работ находятся в методических указаниях по написанию контрольных работ.

12. ОЦЕНОЧНЫЕ МАТЕРИАДЫ

12.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

№ п п	Компетенция	Виды оценочных средств используемых для оценки компетенций по дисциплине		
		Вопросы для зачета с оценкой	Контрольная работа	Тестирование
1	ОПК-3	+ (1-38 вопросы)	+	+
2	ОПК-4	+ (1-38 вопросы)	+	+

12.2. Описание критериев и показателей оценивания компетенций и описание шкал оценивания при использовании различных видов оценочных средств

12.2.1. Вопросы для зачета с оценкой

При оценке знаний на экзамене учитывается:

1. Уровень сформированности компетенций.
2. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
3. Уровень знания фактического материала в объеме программы.

4. Логика, структура и грамотность изложения вопроса.
5. Умение связать теорию с практикой.
6. Умение делать обобщения, выводы.

№ пп	Оценка	Шкала
1	Отлично	Студент должен: - продемонстрировать глубокое и прочное усвоение знаний программного материала; - исчерпывающе, последовательно, грамотно и логически стройно изложить теоретический материал; - правильно формулировать определения; - продемонстрировать умения самостоятельной работы с литературой; - уметь сделать выводы по излагаемому материалу.
2	Хорошо	Студент должен: - продемонстрировать достаточно полное знание программного материала; - продемонстрировать знание основных теоретических понятий; достаточно последовательно, грамотно и логически стройно излагать материал; - продемонстрировать умение ориентироваться в литературе; - уметь сделать достаточно обоснованные выводы по излагаемому материалу.
3	Удовлетворительно	Студент должен: - продемонстрировать общее знание изучаемого материала; - показать общее владение понятийным аппаратом дисциплины; - уметь строить ответ в соответствии со структурой излагаемого вопроса; - знать основную рекомендуемую программой учебную литературу.
4	Неудовлетворительно	Студент демонстрирует: - незнание значительной части программного материала; - не владение понятийным аппаратом дисциплины; - существенные ошибки при изложении учебного материала; - неумение строить ответ в соответствии со структурой излагаемого вопроса; - неумение делать выводы по излагаемому материалу.

12.2.2. Тестирование

№ пп	Оценка	Шкала
1	Отлично	Количество верных ответов в интервале: 71-100%
2	Хорошо	Количество верных ответов в интервале: 56-70%
3	Удовлетворительно	Количество верных ответов в интервале: 41-55%
4	Неудовлетворительно	Количество верных ответов в интервале: 0-40%

12.2.3 .Контрольная работа

Выполняется в письменной форме. При оценке контрольной работы учитывается:
1. Правильность оформления контрольной работы.
2. Уровень сформированности компетенций.
3. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
4. Уровень знания фактического материала в объеме программы.
5. Логика, структура и грамотность изложения письменной работы.
6. Умение связать теорию с практикой.
7. Умение делать обобщения, выводы.

№ пп	Оценка	Шкала
1	Отлично	Студент должен: - продемонстрировать глубокое и прочное усвоение знаний программного материала; - исчерпывающе, последовательно, грамотно и логически стройно изложить теоретический материал; - правильно формулировать определения; - продемонстрировать умения самостоятельной работы с литературой; - уметь сделать выводы по излагаемому материалу.
2	Хорошо	Студент должен: - продемонстрировать достаточно полное знание программного материала; - продемонстрировать знание основных теоретических понятий; достаточно последовательно, грамотно и логически стройно излагать материал; - продемонстрировать умение ориентироваться в литературе; - уметь сделать достаточно обоснованные выводы по излагаемому материалу.
3	Удовлетворительно	Студент должен: - продемонстрировать общее знание изучаемого материала; - показать общее владение понятийным аппаратом дисциплины; - уметь строить ответ в соответствии со структурой излагаемого вопроса; - знать основную рекомендуемую программой учебную литературу.
4	Неудовлетворительно	Студент демонстрирует: - незнание значительной части программного материала; - не владение понятийным аппаратом дисциплины; - существенные ошибки при изложении учебного материала; - неумение строить ответ в соответствии со структурой излагаемого вопроса; - неумение делать выводы по излагаемому материалу.
5	Зачтено	Выставляется при соответствии параметрам экзаменационной шкалы на уровнях «отлично», «хорошо», «удовлетворительно».
6	Не зачтено	Выставляется при соответствии параметрам экзаменационной шкалы на уровне

		«неудовлетворительно».

12.3. Типовые контрольные задания необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

12.3.1. Вопросы для зачета с оценкой

1. Необходимость защиты информации
2. Сохранность защищаемой информации: сущность и основные виды. Сущность понятия "защищаемая информация"
3. Разновидность защищаемой информации и ее носителей.
4. Компьютерные вирусы и их классификация
5. Характеристика антивирусного программного обеспечения
6. Способы ограничение доступа к информации
7. Методы взлома компьютерных систем. Атаки на уровне систем управления базами данных
8. Методы взлома компьютерных систем. Атаки на уровне операционной системы
9. Методы взлома компьютерных систем. Атаки на уровне сетевого программного обеспечения.
10. Методы взлома компьютерных систем. Защита системы от взлома.
11. Характеристика троянских программ. Возникновение троянских программ.
12. Характеристика троянских программ. Распознавание троянской программы.
13. Программные закладки и их классификация
14. Модели воздействия программных закладок на компьютеры
15. Защита системы от программных закладок. Разновидность ПЗ (имитаторы, фильтры и заместители).
16. Парольные взломщики. Защита системы от клавиатурных шпионов. Парольная защита операционных систем.
17. Взлом парольной защиты ОС UNIX
18. Взлом парольной защиты ОС Windows
19. Информационная безопасность компьютерной сети. Характеристика и назначение сканеров.
20. Информационная безопасность компьютерной сети. Защита от анализаторов протоколов.
21. Значение и современные методы шифрования информации в информационном обществе
22. Методологические основы технологии шифрования программными средствами.
23. Применение и проблемы стандартизации криптографических алгоритмов.
24. Средства безопасности ОС Windows. Понятия и термины защиты данных. Характеристики безопасности.
25. Средства безопасности ОС Windows. Применение шифрования с открытым и закрытым ключами.
26. Средства безопасности ОС Windows. Протокол аутентификации Kerberos. Основы применения протокола Kerberos.
27. Средства безопасности ОС Windows. Характеристика протоколов обмена сообщениями.
28. Аутентификация протокола Kerberos в доменах ОС Windows.
29. Средства безопасности ОС Windows. Применение EPS в ОС Windows.
30. Средства безопасности ОС Windows. Шифрование файлов и каталогов. Копирование, перемещение, переименование и уничтожение зашифрованных файлов и папок.

31. Средства безопасности ОС Windows. Архивация и восстановление зашифрованных файлов на другом компьютере

32. Средства безопасности ОС Windows. Восстановление данных зашифрованных с помощью неизвестного личного ключа.

33. Протокол безопасности IP в ОС Windows. Характеристика средств безопасности протокола IP.

34. Архитектура протокола безопасности IP в ОС Windows.

35. Администрирование безопасности в ОС Windows.

36. Использование сертификатов для обеспечения безопасности в ОС Windows. Хранилища сертификатов безопасности.

37. Планирование мероприятий по защите информации

38. Применение средства криптографической защиты информации Pretty good Privacy (PGP).

12.3.2. Примерное содержание тестовых материалов

Задание 1

В каком году в России появились первые преступления с использованием компьютерной техники (были похищены 125,5 тыс. долл. США во Внешэкономбанке)?

1988;
1991;
1994;
1997;
2002.

Задание 2.

Сколько уголовных дела по ст. ст. 272 и 165 УК РФ было возбуждено в 2003 г. в России?

6;
60;
160;
600;
1600.

Задание 3.

В стандарте США «Оранжевая книга» фундаментальное требование, которое относится к группе Стратегия:

индивидуальные субъекты должны идентифицироваться;

контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность;

необходимо иметь явную и хорошо определенную систему обеспечения безопасности;

вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;

гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

Задание 4.

Сертификации подлежат:

средства криптографической защиты информации;
средства выявления закладных устройств и программных закладок;
защищенные технические средства обработки информации;
защищенные информационные системы и комплексы телекоммуникаций;

Задание 5.

Первый по времени открытый правовой нормативный акт, который регулировал вопросы оборота средств криптографической защиты информации, был принят в …

1989 г.

1991 г.

1993 г.

1995 г.

1997 г.

Задание 6.

Естественные угрозы безопасности информации вызваны:

деятельностью человека;

ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;

корыстными устремлениями злоумышленников;

ошибками при действиях персонала.

Задание 7.

Искусственные угрозы безопасности информации вызваны:

деятельностью человека;

ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;

корыстными устремлениями злоумышленников;

ошибками при действиях персонала.

Задание 8.

К основным непреднамеренным искусственным угрозам АСОИ относится:

физическое разрушение системы путем взрыва, поджога и т.п.;

неправомерное отключение оборудования или изменение режимов работы устройств и программ;

изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

Задание 9.

К основным непреднамеренным искусственным угрозам АСОИ относится:

физическое разрушение системы путем взрыва, поджога и т.п.;

чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

нелегальное внедрение и использование неучтенных программ игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения служебных обязанностей;

перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

Задание 10.

Активный перехват информации это – перехват, который:

заключается в установке подслушивающего устройства в аппаратуру средств

обработки информации;
основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
неправомерно использует технологические отходы информационного процесса;
осуществляется путем использования оптической техники;
осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

Задание 11.

Пассивный перехват информации это – перехват, который:

заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
неправомерно использует технологические отходы информационного процесса;
осуществляется путем использования оптической техники;
осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

Задание 12.

Хакер – это:

лицо, которое взламывает интрасеть в познавательных целях;
мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;
лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
плохой игрок в гольф, дилетант;
мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

Задание 13.

Фракер – это:

лицо, которое взламывает интрасеть в познавательных целях;
мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;
лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО;
плохой игрок в гольф, дилетант;
мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

Задание 14.

Кодификатор Генерального Секретариата Интерпола был интегрирован в автоматизированную систему поиска в …

1989 г.
1991 г.
1993 г.
1995 г.
1997 г.

Задание 15.

Преступление, обозначенное кодом QR , означает, что это …

несанкционированный доступ и перехват;
изменение компьютерных данных;
компьютерное мошенничество;
незаконное копирование;
компьютерный саботаж;
прочие компьютерные преступления.

Задание 16.

Спам, который распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

черный пиар;

фишинг;

нигерийские письма;

источник слухов;

пустые письма.

Задание 17.

Для взаимной проверки подлинности пользователей используются:

Механизм запроса-ответа

Механизм аутентификации

Механизм отметки времени ("временной штемпель")

Механизм регистрации

Алгоритмы шифрования

Задание 18.

Для исследования программы в статическом режиме используются:

Отладчики

Компиляторы

Дизассемблеры

Мониторы отладки

Задание 19.

Перечислите какие из перечисленных программ не являются отладчиками?

SoftIce

AFD

IDA

Turbo Debugger

DiskEdit

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

1. Методические указания по выполнению контрольной работы (доступны в библиотеке и профильной кафедре вуза, на сайте вуза).

2. Демонстрационные варианты компьютерного тестирования (доступны во внутренней информационной сети вуза в учебных кабинетах с компьютерной техникой

13. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ И РЕСУРСОВ СЕТИ ИНТЕРНЕТ

13.1. ОСНОВНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

1. Суворова Г.М. Информационная безопасность [Электронный ресурс]: учебное пособие/ Суворова Г.М.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2019.— 214 c.— Режим доступа: http://www.iprbookshop.ru/86938.html.— ЭБС «IPRbooks»

13.2. ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

1. Бахаров Л.Е. Информационная безопасность и защита информации (разделы криптография и стеганография) [Электронный ресурс]: практикум/ Бахаров Л.Е.— Электрон. текстовые данные.— Москва: Издательский Дом МИСиС, 2019.— 59 c.— Режим доступа: http://www.iprbookshop.ru/98171.html.— ЭБС «IPRbooks»

2. Информационная безопасность [Электронный ресурс]: лабораторный практикум/ — Электрон. текстовые данные.— Пермь: Пермский государственный гуманитарно-педагогический университет, 2018.— 86 с.— Режим доступа: http://www.iprbookshop.ru/86357.html.— ЭБС «IPRbooks»

3. Ревнивых А.В. Информационная безопасность в организациях [Электронный ресурс]: учебное пособие/ Ревнивых А.В.— Электрон. текстовые данные.— Новосибирск: Новосибирский государственный университет экономики и управления «НИНХ», 2018.— 84 с.— Режим доступа: http://www.iprbookshop.ru/95200.html.— ЭБС «IPRbooks»

13.3. РЕСУРСЫ СЕТИ ИНТЕРНЕТ

1. Электронно-библиотечная система «IPRbooks» - http://www.iprbookshop.ru
2. Научная электронная библиотека elibrary.ru - http://elibrary.ru/project_authors.asp?
3. Сайты, обнаруживаемые в поисковых системах Yandex, Google и Rambler по запросам:

– "Информационная безопасность»
– "Защита информации";
– "Спам";
– "Вирусы".
– "Антивирусное ПО".

14. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Освоение дисциплины «Информационная безопасность» для студентов, обучающихся по направлению подготовки 09.03.03 Прикладная информатика, осуществляется в виде лекционных и практических занятий, в ходе самостоятельной работы. В ходе самостоятельной работы студенты должны изучить лекционные материалы и другие источники (учебники и учебно-методические пособия), подготовиться к ответам на контрольные вопросы и выполнить тестовые задания.

Дисциплина «Информационная безопасность» включает 19 тем.

Для проведения лекционных занятий предлагается следующая тематика, в соответствии с 7 разделом рабочей программы дисциплины:

очная форма обучения

1. Актуальность информационной безопасности.
2. Пользователи и злоумышленники в Интернет
3. Лицензирование и сертификация в области защиты информации.
4. Основные нормативные руководящие документы
5. Виды угроз информационной безопасности РФ
6. Информационная безопасность сетей.
7. Способы совершения компьютерных преступлений.
8. Уязвимость сети Интернет.
9. Обеспечение информационной безопасности.
10. Компьютерные преступления.
11. Вредоносные программы.
12. Вирусы.
13. Признаки заражения компьютера
14. Антивирусное программное обеспечение.
15. Теория информационной безопасности информационных систем.
16. Криптографические способы защиты информации.
17. Организация информационной безопасности компании.
18. Угрозы информационной безопасности для автоматизированной системы

обработки информации

19. Контроль доступа к информации

заочная форма обучения

1. Лицензирование и сертификация в области защиты информации.
2. Основные нормативные руководящие документы
3. Уязвимость сети Интернет.
4. Компьютерные преступления.
5. Антивирусное программное обеспечение
6. Криптографические способы защиты информации.
7. Организация информационной безопасности компании.
8. Контроль доступа к информации

Лекция – форма обучения студентов, при которой преподаватель последовательно излагает основной материал темы учебной дисциплины. Лекция – это важный источник информации по каждой учебной дисциплине. Она ориентирует студента в основных проблемах изучаемого курса, направляет самостоятельную работу над ним. Для лекций по каждому предмету должна быть отдельная тетрадь для лекций. Прежде всего, запишите имя, отчество и фамилию лектора, оставьте место для списка рекомендованной литературы, пособий, справочников.

Будьте внимательны, когда лектор объявляет тему лекции, объясняет Вам место, которое занимает новый предмет в Вашей подготовке и чему новому Вы сможете научиться. Опытный студент знает, что, как правило, на первой лекции преподаватель обосновывает свои требования, раскрывает особенности чтения курса и способы сдачи зачета или экзамена.

Отступите поля, которые понадобятся для различных пометок, замечаний и вопросов.

Запись содержания лекций очень индивидуальна, именно поэтому трудно пользоваться чужими конспектами.

Не стесняйтесь задавать вопросы преподавателю! Чем больше у Вас будет информации, тем свободнее и увереннее Вы будете себя чувствовать!

Базовые рекомендации:

- не старайтесь дословно конспектировать лекции, выделяйте основные положения, старайтесь понять логику лектора;
- точно записывайте определения, законы, понятия, формулы, теоремы и т.д.;
- передавайте излагаемый материал лектором своими словами;
- наиболее важные положения лекции выделяйте подчеркиванием;
- создайте свою систему сокращения слов;
- привыкайте просматривать, перечитывать перед новой лекцией предыдущую информацию;
- дополняйте материал лекции информацией;
- задавайте вопросы лектору;
- обязательно вовремя пополняйте возникшие пробелы.

Правила тактичного поведения и эффективного слушания на лекциях:

- Слушать (и слышать) другого человека - это настоящее искусство, которое очень пригодится в будущей профессиональной деятельности.
- Если преподаватель «скучный», но Вы чувствуете, что он действительно владеет материалом, то скука - это уже Ваша личная проблема (стоит вообще спросить себя, а настоящий ли Вы студент, если Вам не интересна лекция специалиста?).

Существует очень полезный прием, позволяющий студенту оставаться в творческом напряжении даже на лекциях заведомо «неинтересных» преподавателях. Представьте, что перед Вами клиент, который что-то знает, но ему трудно это сказать. Очень многое здесь зависит от того, поможет ли слушающий говорящему лучше изложить свои мысли (или сообщить свои знания). Но как может помочь «скучному»

преподавателю студент, да еще в большой аудитории, когда даже вопросы задавать неприлично?

Прием прост – постарайтесь всем своим видом показать, что Вам «все-таки интересно» и Вы «все-таки верите», что преподаватель вот-вот скажет что-то очень важное. И если в аудитории найдутся хотя бы несколько таких студентов, внимательно и уважительно слушающих преподавателя, то может произойти «маленькое чудо», когда преподаватель «вдруг» заговорит с увлечением, начнет рассуждать смело и с озорством (иногда преподаватели сами ищут в аудитории внимательные и заинтересованные лица и начинают читать свои лекции, частенько поглядывая на таких студентов, как бы «вдохновляясь» их доброжелательным вниманием). Если это кажется невероятным (типа того, что «чудес не бывает»), просто вспомните себя в подобных ситуациях, когда с приятным собеседником-слушателем Вы вдруг обнаруживаете, что говорите намного увереннее и даже интереснее для самого себя. Но «маленького чуда» может и не произойти, и тогда главное - не обижаться на преподавателя (как не обижается на своего «так и не разговорившегося» клиента опытный психолог-консультант). Считайте, что Вам не удалось «заинтересовать» преподавателя своим вниманием (он просто не поверил в то, что Вам действительно интересно).

- Чтобы быть более «естественным» и чтобы преподаватель все-таки поверил в вашу заинтересованность его лекцией, можно использовать еще один прием. Постарайтесь молча к чему-то «придраться» в его высказываниях. И когда вы найдете слабое звено в рассуждениях преподавателя, попробуйте «про себя» поспорить с преподавателем или хотя бы послушайте, не станет ли сам преподаватель «опровергать себя» (иногда опытные преподаватели сначала подбрасывают провокационные идеи, а затем как бы сами с собой спорят). В любом случае, несогласие с преподавателем - это прекрасная основа для диалога (в данном случае - для «внутреннего диалога»), который уже после лекции, на семинаре может превратиться в диалог реальный. Естественно, не следует извращать данный прием и всем своим видом показывать преподавателю, что Вы его «презираете», что он «ничтожество» и т. п. Критика (особенно критика преподавателя) должна быть конструктивной и доброжелательной.

- Если Вы в чем-то не согласны (или не понимаете) с преподавателем, то совсем не обязательно тут же перебивать его и, тем более, высказывать свои представления, даже если они и кажутся Вам верными. Перебивание преподавателя на полуслове - это верный признак невоспитанности. А вопросы следует задавать либо после занятий (для этого их надо кратко записать, чтобы не забыть), либо выбрав момент, когда преподаватель сделал хотя бы небольшую паузу, и обязательно извинившись. Неужели не приятно самому почувствовать себя воспитанным человеком, да еще на глазах у целой аудитории?

Правила конспектирования на лекциях:

- Не следует пытаться записывать подряд все то, о чем говорит преподаватель. Даже если студент владеет стенографией, записывать все высказывания просто не имеет смысла: важно уловить главную мысль и основные факты.

- Желательно оставлять на страницах поля для своих заметок (и делать эти заметки либо во время самой лекции, либо при подготовке к семинарам и экзаменам).

- Естественно, желательно использовать при конспектировании сокращения, которые каждый может «разработать» для себя самостоятельно (лишь бы самому легко было потом разобраться с этими сокращениями).

- Стараться поменьше использовать на лекциях диктофоны, поскольку потом трудно будет «декодировать» неразборчивый голос преподавателя, все равно потом придется переписывать лекцию (а с голоса очень трудно готовиться к ответственным экзаменам), наконец, диктофоны часто отвлекают преподавателя тем, что студент ничего не делает на лекции (за него, якобы «работает» техника) и обычно просто сидит, глядя на преподавателя немигающими глазами (взглядом немного скучающего «удава»), а преподаватель чувствует себя неуютно и вместо того, чтобы свободно размышлять над

проблемой, читает лекцию намного хуже, чем он мог бы это сделать (и это не только наши личные впечатления: очень многие преподаватели рассказывают о подобных случаях).

Для проведения практических занятий предлагается следующая тематика, в соответствии с 9 разделом рабочей программы дисциплины:

при очной форме обучения:

1. Актуальность информационной безопасности.
2. Пользователи и злоумышленники в Интернет
3. Лицензирование и сертификация в области защиты информации.
4. Основные нормативные руководящие документы
5. Виды угроз информационной безопасности РФ
6. Информационная безопасность сетей.
7. Способы совершения компьютерных преступлений.
8. Уязвимость сети Интернет.
9. Обеспечение информационной безопасности.
10. Компьютерные преступления.
11. Вредоносные программы.
12. Вирусы.
13. Признаки заражения компьютера
14. Антивирусное программное обеспечение.
15. Теория информационной безопасности информационных систем
16. Криптографические способы защиты информации.
17. Организация информационной безопасности компании.
18. Угрозы информационной безопасности для автоматизированной системы обработки информации
19. Контроль доступа к информации

при заочной форме обучения:

1. Пользователи и злоумышленники в Интернет
2. Виды угроз информационной безопасности РФ
3. Информационная безопасность сетей.
4. Способы совершения компьютерных преступлений.
5. Уязвимость сети Интернет.
6. Обеспечение информационной безопасности.
7. Компьютерные преступления.
8. Вредоносные программы.
9. Вирусы.
10. Признаки заражения компьютера
11. Антивирусное программное обеспечение.
12. Теория информационной безопасности информационных систем.
13. Криптографические способы защиты информации.
14. Организация информационной безопасности компании.
15. Угрозы информационной безопасности для автоматизированной системы обработки информации
16. Контроль доступа к информации

Практическое занятие – это одна из форм учебной работы, которая ориентирована на закрепление изученного теоретического материала, его более глубокое усвоение и формирование умения применять теоретические знания в практических, прикладных целях.

Особое внимание на практических занятиях уделяется выработке учебных или профессиональных навыков. Такие навыки формируются в процессе выполнения конкретных заданий – упражнений, задач и т.п. – под руководством и контролем преподавателя.

Готовясь к практическому занятию, тема которого всегда заранее известна, студент

должен освежить в памяти теоретические сведения, полученные на лекциях и в процессе самостоятельной работы, подобрать необходимую учебную и справочную литературу. Только это обеспечит высокую эффективность учебных занятий.

Отличительной особенностью практических занятий является активное участие самих студентов в объяснении вынесенных на рассмотрение проблем, вопросов; преподаватель, давая студентам возможность свободно высказаться по обсуждаемому вопросу, только помогает им правильно построить обсуждение. Такая учебная цель занятия требует, чтобы учащиеся были хорошо подготовлены к нему. В противном случае занятие не будет действенным и может превратиться в скучный обмен вопросами и ответами между преподавателем и студентами.

При подготовке к практическому занятию:

- проанализируйте тему занятия, подумайте о цели и основных проблемах, вынесенных на обсуждение;
- внимательно прочитайте материал, данный преподавателем по этой теме на лекции;
- изучите рекомендованную литературу, делая при этом конспекты прочитанного или выписки, которые понадобятся при обсуждении на занятии;
- постарайтесь сформулировать свое мнение по каждому вопросу и аргументирование его обосновать;
- запишите возникшие во время самостоятельной работы с учебниками и научной литературой вопросы, чтобы затем на семинарском занятии получить на них ответы.

В процессе работы на практическом занятии:

- внимательно слушайте выступления других участников занятия, старайтесь соотнести, сопоставить их высказывания со своим мнением;
- активно участвуйте в обсуждении рассматриваемых вопросов, не бойтесь высказывать свое мнение, но старайтесь, чтобы оно было подкреплено убедительными доводами;
- если вы не согласны с чьим-то мнением, смело критикуйте его, но помните, что критика должна быть обоснованной и конструктивной, т.е. нести в себе какое-то конкретное предложение в качестве альтернативы;
- после семинарского занятия кратко сформулируйте окончательный правильный ответ на вопросы, которые были рассмотрены.

Практическое занятие помогает студентам глубоко овладеть предметом, способствует развитию у них умения самостоятельно работать с учебной литературой и первоисточниками, освоению ими методов научной работы и приобретению навыков научной аргументации, научного мышления. Преподавателю же работа студента на практическом занятии позволяет судить о том, насколько успешно и с каким желанием он осваивает материал курса.

Методические указания и рекомендации по другим видам учебной работы - по написанию контрольной работы, представлены в соответствующих изданиях. При выполнении контрольной работы следует руководствоваться специальными методическими указаниями. Эти методические указания находятся на профильной кафедре вуза.

15. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

15.1. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Реализация образовательного процесса по дисциплине «Информационная безопасность» осуществляется в следующих аудиториях:

1. Занятия **лекционного типа** - аудитория №503: 40 мест (20 столов, 40 стульев), 1 доска, 5 стендов, 1 стол преподавателя, 1 кафедра, вешалка напольная – 2 шт.

2. Для проведения **практических занятий** используется лаборатория для проведения практических занятий №404: 44 места (22 стола, 44 стула), 1 доска, 5 стендов,

1 кафедра, вешалка напольная – 1 шт, 12 ПЭВМ с выходом в Интернет, принтер – 1

3. Для **самостоятельной работы** студентов используется аудитория №506: 22 места (11 столов, 22 стула), 1 доска, 4 стенда, 1 кафедра, вешалка напольная – 1 шт, 10 ПЭВМ с выходом в Интернет, принтер - 1

4. Для **проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации** используется аудитория для текущего контроля и промежуточной аттестации №503: 40 мест (20 столов, 40 стульев), 1 доска, 5 стендов, 1 стол преподавателя, 1 кафедра, вешалка напольная – 2 шт.

15.2 ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ), ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

Для осуществления образовательного процесса по дисциплине необходимы следующие программное обеспечение и информационные справочные системы:

1. Информационно-правовая система Гарант http://www.garant.ru/
2. Справочная правовая система Консультант Плюс http://www.consultant.ru/
3. Электронно-библиотечная система «IPRbooks» - http://www.iprbookshop.ru
4. Научная электронная библиотека elibrary.ru - http://elibrary.ru/project_authors.asp

На рабочих местах используется операционная система Microsoft Windiws 7 Professional, пакет Microsoft Office 2007 Russian, Антивирусное ПО, а также другое специализированное программное обеспечение.

Рабочую программу дисциплины составил:
Ионан Юрий Эдуардович, к.т.н., доцент кафедры информатики и программного обеспечения Брянского института управления и бизнеса

Рабочая программа дисциплины рассмотрена и утверждена на заседании кафедры «Информатика и программное обеспечение»:
протокол № _1_ от «17» августа 2020 г.
Заведующий кафедрой _____ /Т.М. Хвостенко