Автономная некоммерческая организация высшего образования
«Волгоградский институт бизнеса»

Утверждаю
Проректор по учебной работе и управлению качеством
_____ Л.В. Шамрай-Курбатова
«12» мая 2022г.

Рабочая программа учебной дисциплины

Информационная безопасность
(Наименование дисциплины)

09.03.03 Прикладная информатика, направленность (профиль) «Менеджмент в области информационных технологий
(Направление подготовки / Профиль)

Бакалавр
(Квалификация)

Кафедра разработчик Экономики и управления
Год набора **2021, 2022**

Вид учебной деятельности	Трудоемкость (объем) дисциплины					
	Очная форма	Очно-заочная форма		Заочная форма		
	д	в	св	з	сз	вв
Зачетные единицы	**4**			**4**	**4**	**4**
Общее количество часов	144			144	144	144
Аудиторные часы контактной работы обучающегося с преподавателями:	36			10	10	8
– Лекционные (Л)						
– Практические (ПЗ)	36			10	10	8
– *В том числе в форме практической подготовки*	*36*			*10*	*10*	*8*
– Лабораторные (ЛЗ)						
– Семинарские (СЗ)						
Самостоятельная работа обучающихся (СРО)	72			125	125	127
К (Р-Г) Р (П) (+;-)						
Тестирование (+;-)						
ДКР (+;-)						
Зачет (+;-)						
Зачет с оценкой (+;- (Кол-во часов))						
Экзамен (+;- (Кол-во часов))	+(36)			+ (9)	+ (9)	+ (9)

Волгоград 2022

Содержание

Раздел 1. Организационно-методический раздел

1.1. Цели освоения дисциплины

Дисциплина **«Информационная безопасность»** входит в **часть, формируемую участниками образовательных отношений** по направлению подготовки **«09.03.03 Прикладная информатика», направленность (профиль) «Менеджмент в области информационных технологий.**

Целью дисциплины является формирование **компетенций** (*в соответствии с ФГОС ВО и требованиями к результатам освоения основной профессиональной образовательной программы высшего образования (ОПОП ВО)*):

Универсальных:

УК-8.1. Способен обеспечивать безопасность на рабочем месте в условиях воздействия опасных производственных факторов, готов принимать участие в оказании первой помощи при травмах и внезапных заболеваниях

Общепрофессиональных:

ОПК-3.1 - Способен решать задачи, связанные с обеспечением информационной безопасности

Перечисленные компетенции формируются в процессе достижения **индикаторов компетенций:**

Обобщенная трудовая функция/ трудовая функция	**Код и наименование дескриптора компетенций**	**Код и наименование индикатора достижения компетенций (из ПС)**
ПС 06.012 Менеджер продуктов в области информационных технологий **С Управление серией ИТ-продуктов и группой их менеджеров** **С/05.6** Командообразование и развитие персонала **С/09.6** Разработка предложений п приобретению и продаже технологических, продуктовых и прочих интеллектуальных активов и организаций	УК-8.1. Способен обеспечивать безопасность на рабочем месте в условиях воздействия опасных производственных факторов, готов принимать участие в оказании первой помощи при травмах и внезапных заболеваниях	*Знает* ИД-1 УК- 8.1 Основы защиты интеллектуальной собственности С/09.6 *Умеет* ИД-3 УК- 8.1 Проводить переговоры с командой менеджеров ИТ-продуктов С/05.6 *Имеет навыки и (или) опыт:* ИД-5 УК- 8.1 Наставничество и коучинг, включая организацию обучения персонала С/05.6
ПС 06.012 Менеджер продуктов в области информационных технологий **С Управление серией ИТ-продуктов и группой их менеджеров** **С/09.6** Разработка предложений п приобретению и продаже технологических, продуктовых и прочих интеллектуальных активов и организаций	ОПК-3.1 - Способен решать задачи, связанные с обеспечением информационной безопасности	*Знает:* ИД-1 ОПК- 3.1 Основы защиты интеллектуальной собственности С/09.6 *Умеет:* ИД-3 ОПК- 3.1 Проводить оценку ценности технологий, ИТ-продуктов и организаций как потенциальных активов для приобретения с целью развития серии ИТ-продуктов С/09.6 *Имеет навыки и (или) опыт:* ИД-5 ОПК- 3.1 Исследование существующих на рынке технологий, ИТ-продуктов и организаций как потенциальных активов для приобретения с целью

		развития серии ИТ-продуктов С/09.6

1.2. Место дисциплины в структуре ОПОП ВО направления подготовки «09.03.03 Прикладная информатика», направленность (профиль) «Менеджмент в области информационных технологий

№	Предшествующие дисциплины (дисциплины, изучаемые параллельно)	Последующие дисциплины
1	*2*	*3*
1	Введение в направление подготовки	ВКР
2	Информатика	
3	Правовые основы прикладной информатики	
4	Информационные системы и технологии	
5	Информационные технологии в менеджменте	
6	Базы данных	
7	Вычислительные системы, сети и телекоммуникации	
8	Проектный практикум	
9	Проектирование веб-сайтов	

Последовательность формирования компетенций в указанных дисциплинах может быть изменена в зависимости от формы и срока обучения, а также преподавания с использованием дистанционных технологий обучения.

1.3. Нормативная документация

Рабочая программа учебной дисциплины составлена на основе:

- Федерального государственного образовательного стандарта высшего образования по направлению подготовки **09.03.03 Прикладная информатика**;
- учебного плана направления подготовки **09.03.03 Прикладная информатика, направленность (профиль) «Менеджмент в области информационных технологий»** 2021, 2022 года набора;
- образца рабочей программы учебной дисциплины (приказ № 113-О от 01.09.2021 г.).

Раздел 2. Тематический план

Очная форма обучения (полный срок)

№	Тема дисциплины	Трудоемкость					
		Всего	Аудиторные занятия			СРО	Код индикатора и дескриптора достижения компетенций
			Л	ПЗ (ЛЗ, СЗ)	Прак. Подг.		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	Понятие информационной безопасности. Основные составляющие.	8				8	ИД-1 УК- 8.1 ИД-1 ОПК- 3.1
2	Угрозы информационной безопасности. Их классификация	8				8	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	14		4	4	10	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
4	Административный уровень. Политика безопасности	8				8	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
5	Организация разноуровневого доступа в информационную систему	12		4	4	8	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
6	Основные программно-технические меры. Защита информации с помощью пароля	14		8	8	6	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
7	Защита от несанкционированного доступа и сетевых хакерских атак	10		4	4	6	ИД-1 УК- 8.1 ИД-5 ОПК- 3.1
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	16		8	8	8	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
9	Основы технологии построения защищенных ОС	18		8	8	10	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
Вид промежуточной аттестации (экзамен)		**36**					
Итого		**108**		**36**	**36**	**72**	

Заочная форма обучения (полный срок, ускоренное обучение на базе СПО)

№	Тема дисциплины	Трудоемкость					
		Всего	Аудиторные занятия			СРО	Код индикатора и дескриптора достижения компетенций
			Л	ПЗ (ЛЗ, СЗ)	Прак. Подг.		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	Понятие информационной безопасности. Основные составляющие. Важность	14				14	ИД-1 УК- 8.1 ИД-1 ОПК- 3.1

	проблемы						
2	Угрозы информационной безопасности. Их классификация	14				14	ИД-3 УК- 8.1 ИД-5 ОПК-3.1
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	16		2	2	14	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
4	Административный уровень. Политика безопасности	14				14	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
5	Организация разноуровневого доступа в информационную систему	18		2	2	16	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
6	Основные программно-технические меры. Защита информации с помощью пароля	17		2	2	15	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
7	Защита от несанкционированного доступа и сетевых хакерских атак	12				12	ИД-1 УК- 8.1 ИД-5 ОПК- 3.1
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	14		2	2	12	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
9	Основы технологии построения защищенных ОС	16		2	2	14	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
Вид промежуточной аттестации (экзамен)		**9**					
Итого		**144**		**10**	**10**	**125**	

Заочная форма обучения (ускоренное обучение на базе ВО)

№	Тема дисциплины	Трудоемкость					
		Всего	Аудиторные занятия			СРО	Код индикатора и дескриптора достижения компетенций
			Л	ПЗ (ЛЗ, СЗ)	Прак. Подг.		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	Понятие информационной безопасности. Основные составляющие. Важность проблемы	14				14	ИД-1 УК- 8.1 ИД-1 ОПК- 3.1
2	Угрозы информационной безопасности. Их классификация	14				14	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	16		2	2	14	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
4	Административный уровень. Политика безопасности	14				14	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
5	Организация разноуровневого доступа в информационную систему	18		2	2	16	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
6	Основные программно-технические меры. Защита информации с помощью пароля	17		2	2	15	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1

7	Защита от несанкционированного доступа и сетевых хакерских атак	14				14	ИД-1 УК- 8.1 ИД-5 ОПК- 3.1
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	14				12	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
9	Основы технологии построения защищенных ОС	16		2	2	14	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
Вид промежуточной аттестации (экзамен)		**9**					
Итого		**144**		**8**	**8**	**127**	

Раздел 3. Содержание дисциплины

3.1. Содержание дисциплины

Тема 1. Понятие информационной безопасности. Основные составляющие. Важность проблемы

Организация ИТ-инфраструктуры и управление информационной безопасностью. Информационная безопасность – защита интересов субъектов информационных отношений. Доктрина информационной безопасности РФ. Доступность, целостность и конфиденциальность информации. Предмет и объект защиты. Информационная безопасность один из важнейших аспектов интегральной безопасности.

Тема 2. Угрозы информационной безопасности. Их классификация

Информационная безопасность, как часть эксплуатации современных информационных систем. Угроза. Угроза информационной безопасности. Утечка информации. Наиболее распространенные угрозы доступности. Примеры угроз доступности. Основные угрозы целостности. Основные угрозы конфиденциальности. Классификация угроз по основным признакам.

Тема 3. Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства

Важность законодательного уровня информационной безопасности. Обзор российского законодательства в области информационной безопасности. Закон «Об информации, информационных технологиях и защите информации». Другие законы и нормативные акты федеральной службы экспертного и технического контроля (гостехкомиссии). Обзор зарубежного законодательства в области информационной безопасности. О текущем состоянии российского законодательства в области информационной безопасности.

Тема 4. Административный уровень. Политика безопасности

Управление информационной безопасностью. Политика безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом.

Тема 5. Организация разноуровневого доступа в информационную систему

Типы политик безопасности. Ролевое управление доступом.

Тема 6. Основные программно-технические меры. Защита информации с помощью пароля

Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность. Идентификация и аутентификация. Парольная аутентификация. Одноразовые пароли. Идентификация / аутентификация с помощью биометрических данных.

Тема 7. Защита от несанкционированного доступа и сетевых хакерских атак

Противодействие несанкционированному доступу. Способы несанкционированного доступа. Методы и средства борьбы с несанкционированным доступом.

Тема 8. Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов

Программы обнаружения и защиты от вирусов. Программы-доктора. Программы-детекторы. Программы-мониторы и др. Обзор антивирусного программного обеспечения. Информационная инфекция. Вирус. Резидентные вирусы. Полиморфизм. Троянские кони. Сетевые черви. Классификация компьютерных вирусов.

Тема 9. Основы технологии построения защищенных ОС

Подходы к обеспечению безопасности ОС. Задачи разработки защищенных ОС. Проблема внедрения модели безопасности в ОС. Критика внедрения моделей. Постановка задачи внедрения модели безопасности в ОС. Решение проблемы внедрения моделей безопасности в ОС.

3.2. Содержание практического блока дисциплины

Очная форма обучения (полный срок)

№	Тема практического (семинарского, практического) занятия *В том числе в форме практической подготовки*
1	***2***
Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	
ПЗ 1	Изучение нормативно – правовой базы в области информационной безопасности
Организация разноуровневого доступа в информационную систему	
ПЗ 2	Администрирование баз данных и проектов Access
Основные программно-технические меры. Защита информации с помощью пароля	
ПЗ 3	Создание резервных копий файлов (для баз данных и проектов Access)
ПЗ 4	Защита информации с помощью пароля
Защита от несанкционированного доступа и сетевых хакерских атак	
ПЗ 5	Защита от несанкционированного доступа и сетевых хакерских атак
Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	
ПЗ 6	Защита съемных устройств с помощью современного антивирусного программного обеспечения
ПЗ 7	Настройка антивирусной системы безопасности
Основы технологии построения защищенных ОС	
ПЗ 8	Основные признаки присутствия на компьютере вредоносных программ
ПЗ 9	Общие требования к построению системы безопасности

Заочная форма обучения (полный срок, ускоренное обучение на базе СПО)

№	Тема практического (семинарского, практического) занятия *В том числе в форме практической подготовки*
1	***2***
Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	
ПЗ 1	Изучение нормативно – правовой базы в области информационной безопасности
Организация разноуровневого доступа в информационную систему	
ПЗ 2	Администрирование баз данных и проектов Access
Основные программно-технические меры. Защита информации с помощью пароля	
ПЗ 3	Создание резервных копий файлов (для баз данных и проектов Access)
Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	
ПЗ 4	Защита съемных устройств с помощью современного антивирусного программного обеспечения
Основы технологии построения защищенных ОС	
ПЗ 5	Основные признаки присутствия на компьютере вредоносных программ

Заочная форма обучения (ускоренное обучение на базе ВО)

№	Тема практического (семинарского, практического) занятия *В том числе в форме практической подготовки*
1	***2***
Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	
ПЗ 1	Изучение нормативно – правовой базы в области информационной безопасности
Организация разноуровневого доступа в информационную систему	
ПЗ 2	Администрирование баз данных и проектов Access
Основные программно-технические меры. Защита информации с помощью пароля	
ПЗ 3	Создание резервных копий файлов (для баз данных и проектов Access)
Основы технологии построения защищенных ОС	
ПЗ 4	Основные признаки присутствия на компьютере вредоносных программ

3.3. Образовательные технологии

Очная форма обучения (полный срок)

№	Тема занятия	Вид учебного занятия	Форма / Методы интерактивного обучения	% учебного времени
1	***2***	***3***	***4***	***5***
1	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	ПЗ	Дискуссия	25
2	Организация разноуровневого доступа в информационную систему	ПЗ	Деловая игра	25
3	Основные программно-технические меры. Защита информации с помощью пароля	ПЗ	Мозговой штурм	25
4	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	ПЗ	Конференция	25
5	Основы технологии построения защищенных ОС	ПЗ	Дискуссия	25
Итого				**25%**

Заочная форма обучения (полный срок, ускоренное обучение на базе СПО)

№	Тема занятия	Вид учебного занятия	Форма / Методы интерактивного обучения	% учебного времени
1	***2***	***3***	***4***	***5***
1	Основные программно-технические меры. Защита информации с помощью пароля	ПЗ	Мозговой штурм	25
2	Современные антивирусные программы. Защита от	ПЗ	Конференция	25

	информационных инфекций. Классификация компьютерных вирусов			
3	Основы технологии построения защищенных ОС	ПЗ	Дискуссия	25
Итого				**25%**

Заочная форма обучения (ускоренное обучение на базе ВО)

№	**Тема занятия**	**Вид учебного занятия**	**Форма / Методы интерактивного обучения**	**% учебного времени**
1	***2***	***3***	***4***	***5***
1	Основные программно-технические меры. Защита информации с помощью пароля	ПЗ	Мозговой штурм	25
3	Основы технологии построения защищенных ОС	ПЗ	Дискуссия	25
Итого				**25%**

Раздел 4. Организация самостоятельной работы обучающихся

4.1. Организация самостоятельной работы обучающихся

№	Тема дисциплины	№ вопросов	№ рекомендуемой литературы
1	*2*	*3*	*4*
1	Понятие информационной безопасности. Основные составляющие. Важность проблемы	1,2,3	3, 6, 7
2	Угрозы информационной безопасности. Их классификация	2,3	1, 2, 3, 4
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	4,5,6,7,8,9,10	2, 3, 4
4	Административный уровень. Политика безопасности	11,12,17,18,19	1, 3, 4
5	Организация разноуровневого доступа в информационную систему	20,21	1, 3, 4
6	Основные программно-технические меры. Защита информации с помощью пароля	13,14	3, 6, 7
7	Защита от несанкционированного доступа и сетевых хакерских атак	17,18,19.20,21	3, 6, 7
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	15,16,19,22	3, 6, 7
9	Основы технологии построения защищенных ОС	17,18,19,20,21	3, 6, 7

Перечень вопросов, выносимых на самостоятельную работу обучающихся

1. Подходы к изучению информационной безопасности
2. Моделирование информационной безопасности
3. Причины, виды и каналы утечки информации
4. Закон «Об информации, информационных технологиях и защите информации».
5. Зарубежное законодательство в области информационной безопасности.
6. Роль стандартов информационной безопасности.
7. Стандарты ISO 17799 и ISO/IEC 15408 «Критерии оценки безопасности информационных технологий».
8. Функциональные требования. Требования доверия безопасности.
9. Гармонизированные критерии Европейских стран.
10. Спецификации в области информационной безопасности.
11. Политика безопасности. Типы политик безопасности
12. Программа безопасности
13. Основные классы мер процедурного уровня
14. Архитектурная безопасность
15. Отказоустойчивость и зона риска. Обеспечение отказоустойчивости.
16. Туннелирование и управление.
17. Мотивация как лояльность персонала с точки зрения информационной безопасности.
18. Человеческий фактор в обеспечении безопасности конфиденциальной информации
19. Особенности современных информационных систем, существенные с точки зрения безопасности.
20. Анализ и классификация удаленных атак на компьютерные сети
21. Многоуровневая защита корпоративных сетей
22. Современное антивирусное программное обеспечение

4.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся

Самостоятельная работа обучающихся обеспечивается следующими учебно-методическими материалами:

1. Указаниями в рабочей программе по дисциплине (п.4.1.)
2. Лекционными материалами в составе учебно-методического комплекса по дисциплине
3. Заданиями и методическими рекомендациями по организации самостоятельной работы обучающихся в составе учебно-методического комплекса по дисциплине.
4. Глоссарием по дисциплине в составе учебно-методического комплекса по дисциплине.

Раздел 5. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся

Фонд оценочных средств по дисциплине представляет собой совокупность контролирующих материалов, предназначенных для измерения уровня достижения обучающимися установленных результатов образовательной программы. ФОС по дисциплине используется при проведении оперативного контроля и промежуточной аттестации обучающихся. Требования к структуре и содержанию ФОС дисциплины регламентируются Положением о фонде оценочных материалов по программам высшего образования – программам бакалавриата, магистратуры.

5.1. Паспорт фонда оценочных средств

Очная форма обучения (полный срок)

№	Контролируемые разделы (темы) дисциплины	Оценочные средства				
		Л	ПЗ (ЛЗ, СЗ)	Прак. Подг.	СРО	Код индикатора и дескриптора достижения компетенций
1	*2*	*3*	*4*	*5*	*6*	*7*
1	Понятие информационной безопасности. Основные составляющие. Важность проблемы				ПРВ	ИД-1 УК- 8.1 ИД-1 ОПК- 3.1
2	Угрозы информационной безопасности. Их классификация				ПРВ	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства		УО	УО	ПРВ	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
4	Административный уровень. Политика безопасности				ПРВ	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
5	Организация разноуровневого доступа в информационную систему		УО	УО	ПРВ	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
6	Основные программно-технические меры. Защита информации с помощью пароля		МШ	МШ	ПРВ	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
7	Защита от несанкционированного доступа и сетевых хакерских атак		УО	УО	ПРВ	ИД-1 УК- 8.1 ИД-5 ОПК- 3.1
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов		УО	УО	ПРВ	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
9	Основы технологии построения защищенных ОС		Д	Д	ПРВ	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1

Заочная форма обучения (полный срок, ускоренное обучение на базе СПО)

№	Контролируемые разделы (темы) дисциплины	Оценочные средства				
		Л	ПЗ (ЛЗ, СЗ)	Прак. Подг.	СРО	Код индикатора и дескриптора достижения компетенций
1	*2*	*3*	*4*	*5*	*6*	*7*
1	Понятие информационной безопасности. Основные составляющие. Важность проблемы				ПРВ	ИД-1 УК- 8.1 ИД-1 ОПК- 3.1
2	Угрозы информационной безопасности. Их классификация				ПРВ	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства		УО	УО	ПРВ	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
4	Административный уровень. Политика безопасности				ПРВ	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
5	Организация разноуровневого доступа в информационную систему		УО	УО	ПРВ	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
6	Основные программно-технические меры. Защита информации с помощью пароля		МШ	МШ	ПРВ	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
7	Защита от несанкционированного доступа и сетевых хакерских атак				ПРВ	ИД-1 УК- 8.1 ИД-5 ОПК- 3.1
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов				ПРВ	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
9	Основы технологии построения защищенных ОС		Д	Д	ПРВ	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1

Заочная форма обучения (ускоренное обучение на базе ВО)

№	Контролируемые разделы (темы) дисциплины	Оценочные средства				
		Л	ПЗ (ЛЗ, СЗ)	Прак. Подг.	СРО	Код индикатора и дескриптора достижения компетенций
1	*2*	*3*	*4*		*5*	*6*
1	Понятие информационной безопасности. Основные составляющие. Важность проблемы				ПРВ	ИД-1 УК- 8.1 ИД-1 ОПК- 3.1

2	Угрозы информационной безопасности. Их классификация				ПРВ	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства		УО	УО	ПРВ	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
4	Административный уровень. Политика безопасности				ПРВ	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
5	Организация разноуровневого доступа в информационную систему		УО	УО	ПРВ	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
6	Основные программно-технические меры. Защита информации с помощью пароля		МШ	МШ	ПРВ	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
7	Защита от несанкционированного доступа и сетевых хакерских атак				ПРВ	ИД-1 УК- 8.1 ИД-5 ОПК- 3.1
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов				ПРВ	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
9	Основы технологии построения защищенных ОС		Д	Д	ПРВ	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1

Условные обозначения оценочных средств (Столбцы 3, 4, 5):
ЗЗ – Защита выполненных заданий (творческих, расчетных и т.д.), представление презентаций;
Т – Тестирование по безмашинной технологии;
АСТ – Тестирование компьютерное;
УО – Устный (фронтальный, индивидуальный, комбинированный) опрос;
КР – Контрольная работа (аудиторные или домашние, индивидуальные, парные или групповые контрольные, самостоятельные работы, диктанты и т.д.);
К – Коллоквиум;
ПРВ – Проверка рефератов, отчетов, рецензий, аннотаций, конспектов, графического материала, эссе, переводов, решений заданий, выполненных заданий в электронном виде и т.д.;
ДИ – Деловая игра;
РИ – Ролевая игра;
КМ – Кейс-метод;
КС – Круглый стол;
КСМ – Компьютерная симуляция;
МШ – Метод мозгового штурма;
ЛС – Лекция-ситуация;
ЛК – Лекция-конференция;
ЛВ – Лекция-визуализация;
ПЛ – Проблемная лекция;
Д – Дискуссия, полемика, диспут, дебаты;
П – Портфолио;
ПВУ – Просмотр видеоуроков;
МП – Метод проектов.

5.2. Тематика письменных работ обучающихся

В течение изучения дисциплины «Информационная безопасность» обучающиеся должны сдать и отчитать реферат по одной из предложенных ниже тем:

1. Концепция национальной безопасности.
2. Основные виды угроз информационной безопасности.

3. Законодательный уровень информационной безопасности: обзор российского законодательства.
4. Законодательный уровень информационной безопасности: обзор зарубежного законодательства.
5. Обзор действующих стандартов и рекомендаций в области информационной безопасности.
6. Административный уровень информационной безопасности.
7. Модели основных политик безопасности.
8. Процедурный уровень информационной безопасности.
9. Идентификация, аутентификация с помощью биометрических параметров.
10. История криптографии.
11. Основные понятия и определения криптологии.
12. Симметричные методы шифрования.
13. Ассиметричные методы шифрования.
14. Цифровая подпись: основные понятия.
15. История возникновения электронной цифровой подписи.
16. Алгоритмы ЭЦП.
17. Защита информации от утечки по техническим каналам.
18. Способы несанкционированного доступа к информации.
19. Технические средства несанкционированного доступа.
20. Системы защиты от несанкционированного доступа.
21. Защита от информационных инфекций.
22. Вирус: основные понятия, виды.
23. Троянский конь как одна из угроз безопасности информации.
24. Сетевые черви: милые создания или угроза информационной безопасности.
25. Профилактика и лечение информационных инфекций.
26. Программы обнаружения и защиты от вирусов.
27. Современные антивирусные программы (на примере трех программ).
28. Методы обнаружения и удаления вирусов.
29. Общая характеристика организационных методов защиты.
30. Организационные каналы передачи информации.

5.3. Перечень вопросов промежуточной аттестации по дисциплине

Вопросы к экзамену:

1. Информационная безопасность, как часть эксплуатации современных информационных систем.
2. Организация ИТ-инфраструктуры и управление информационной безопасностью. Доступность, целостность и конфиденциальность информации.
3. Доктрина информационной безопасности РФ.
4. Обзор действующих стандартов и рекомендаций в области информационной безопасности.
5. Классификация защищаемой информации по степени важности и ценности.
6. Основные определения и критерии классификации угроз.
7. Законодательный уровень информационной безопасности.
8. Административный уровень информационной безопасности.
9. Управление информационной безопасностью. Политика безопасности. Содержание политики безопасности. Программа безопасности.
10. Модели основных политик безопасности.
11. Управление рисками. Основные понятия. Подготовительный этап управления рисками.
12. Управление рисками. Основные этапы управления рисками.
13. Методы и модели анализа угроз.
14. Поддержание работоспособности. Реагирование на нарушения режима безопасности.
15. Основные программно-технические меры.
16. Архитектурная безопасность.
17. Идентификация и аутентификация, управление доступом.

18. Идентификация, аутентификация с помощью биометрических параметров.
19. Мониторинг и аудит.
20. История криптографии. Основные понятия и определения криптологии.
21. Шифрование, контроль целостности.
22. Симметричные методы шифрования. Ассиметричные методы шифрования.
23. Цифровая подпись: основные понятия. Алгоритмы ЭЦП.
24. Экранирование, анализ защищенности.
25. Классификация межсетевых экранов.
26. Обеспечение высокой доступности.
27. Вирус: основные понятия, виды. Современные антивирусные программы (на примере трех программ).
28. Методы обнаружения и удаления вирусов.

Раздел 6. Перечень учебной литературы, необходимой для освоения дисциплины

6.1. Основная литература

1. Никифоров, С. Н. Защита информации. Защита от внешних вторжений : учебное пособие / С. Н. Никифоров. — Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 84 с. — ISBN 978-5-9227-0757-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/74381.html
2. Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 424 с. — ISBN 978-5-4497-0336-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/89451.html
3. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/87995.html

6.2. Дополнительная литература

4. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности : учебное пособие / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 431 с. — ISBN 978-5-4497-0935-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102070.html
5. Рагозин, Ю. Н. Инженерно-техническая защита информации : учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности / Ю. Н. Рагозин ; под редакцией Т. С. Кулакова. — Санкт-Петербург : Интермедия, 2018. — 168 с. — ISBN 978-5-4383-0161-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/73641.html.
6. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю. Н. Сычев. — Саратов : Вузовское образование, 2018. — 195 с. — ISBN 978-5-4487-0128-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/72345.html

6.3. Другие источники информации и средства обеспечения освоения дисциплины

7. Журнал «Бизнес. Образование. Право. Вестник Волгоградского института бизнеса» // URL: http://vestnik.volbi.ru/
8. Журнал «Мир ПК» // URL: http://www.osp.pcworld
9. Журнал «Компьютерра-онлайн» // URL: http://www2.computerra.ru
10. Журнал «Хакер» // URL: http://www.xakep.ru
11. Журнал «Сети» // URL: http://www.osp.ru/nets.
12. Журнал «Computerworld» // URL: http://www.osp.ru/cw.
13. Журнал «LAN» // URL: URL: http://www.osp.ru/lan /+электронный ресурс/.
14. Издательство “Открытые системы” // URL: http://www.osp.ru.
15. Официальный сайт компании Microsoft // URL: http://www.microsoft.com.
16. ПО для организации конференций: ZOOM // URL: https://zoom.us/
17. СПС «КонсультантПлюс» // URL: http://www.consultant.ru/document/cons_doc
18. СПС «ГАРАНТ» // URL: http://base.garant.ru/
19. ЦИТ Форум // URL: http://citforum.ru.
20. ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. // URL: http://base.garant.ru/12148555/

Раздел 7. Материально-техническая база и информационные технологии

Материально-техническое обеспечение дисциплины «**Информационная безопасность**» включает в себя учебные аудитории для проведения лекционных, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы обучающихся.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения. Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети Интернет.

Дисциплина может реализовываться с применением дистанционных технологий обучения. Специфика реализации дисциплины с применением дистанционных технологий обучения устанавливается дополнением к рабочей программе. В части не противоречащей специфике, изложенной в дополнении к программе, применяется настоящая рабочая программа.

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине с применением дистанционных образовательных технологий включает в себя:
Компьютерная техника, расположенная в учебном корпусе Института (ул.Качинцев, 63, кабинет Центра дистанционного обучения):

1) Intel i 3 3.4Ghz\ОЗУ 4Gb\500GB\RadeonHD5450
2) Intel PENTIUM 2.9GHz\ОЗУ 4GB\500GB
3) личные электронные устройства (компьютеры, ноутбуки, планшеты и иное), а также средства связи преподавателей и студентов.

Информационные технологии, необходимые для осуществления образовательного процесса по дисциплине с применением дистанционных образовательных технологий включают в себя:

- система дистанционного обучения (СДО) (Learning Management System) (LMS) Moodle (Modular Object-Oriented Dynamic Learning Environment);
- электронная почта;
- система компьютерного тестирования АСТ-тест;
- электронная библиотека IPRbooks;
- система интернет-связи skype;
- телефонная связь;
- система потоковой видеотрансляции семинара с интерактивной связью в форме чата (вебинар).

Обучение обучающихся инвалидов и обучающихся с ограниченными возможностями здоровья осуществляется посредством применения специальных технических средств в зависимости от вида нозологии.

При проведении учебных занятий по дисциплине используются мультимедийные комплексы, электронные учебники и учебные пособия, адаптированные к ограничениям здоровья обучающихся.

Лекционные аудитории оборудованы мультимедийными кафедрами, подключенными к звуковым колонкам, позволяющими усилить звук для категории слабослышащих обучающихся, а также проекционными экранами которые увеличивают изображение в несколько раз и позволяют воспринимать учебную информацию обучающимся с нарушениями зрения.

При обучении лиц с нарушениями слуха используется усилитель слуха для слабослышащих людей Cyber Ear модель HAP-40, помогающий обучаемым лучше воспринимать учебную информацию.

Обучающиеся с ограниченными возможностями здоровья, обеспечены печатными и электронными образовательными ресурсами (программы, учебники, учебные пособия, материалы для самостоятельной работы и т.д.) в формах, адаптированных к ограничениям их здоровья и восприятия информации:

для лиц с нарушениями зрения:

- в форме электронного документа;
- в форме аудиофайла;

для лиц с нарушениями слуха:

- в печатной форме;
- в форме электронного документа;

для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Программное обеспечение, используемое на занятиях**:**

- Операционная система Windows,
- Архиватор 7-zip,
- Система тестирования AST-Test,
- Microsoft Office 2007,
- Антивирус Касперский 6,
- Консультант+,
- Виртуальная машина VirtualBox,
- Виртуальная машина VirtualPC,
- Internet Explorer.

Раздел 8. Методические указания для обучающихся по освоению дисциплины

Для успешного усвоения материала курса требуются значительное время, концентрация внимания и усилия: посещение лекционных занятий и конспектирование преподаваемого материала, работа с ним дома, самостоятельная проработка материала рекомендуемых учебников и учебных пособий при самостоятельной подготовке. Особое внимание следует обратить на выполнение практических работ, практических заданий по СРО, тестовых вопросов.

При самостоятельной работе с учебниками и учебными пособиями полезно иметь под рукой справочную литературу (энциклопедии) или доступ к сети Интернет, так как могут встречаться новые термины, понятия, которые раньше обучающиеся не знали.

Цель практических занятий по дисциплине «Информационная безопасность» - закрепление знаний по определенной теме, приобретенных в результате прослушивания лекций, получения консультаций и самостоятельного изучения различных источников литературы. При выполнении данных работ обучающиеся должны будут глубоко изучить методы и методики обеспечения информационной безопасности. Получить навыки настройки и обслуживания антивирусного программного обеспечения.

Перед практическим занятием обучающийся должен детально изучить теоретические материалы вопросов практики в учебниках, конспектах лекций, периодических журналах и прочее. Если при выполнении практического задания у обучающегося остаются неясности, то ему необходимо оперативно обратиться к преподавателю за уточнением.

После выполнения практического задания обучающиеся должны выполнить самостоятельную работу. Самостоятельная работа включает в себя индивидуальное задание по пройденной теме. Таким образом, каждый обучающийся выполняет только свой вариант задания. Выполнение практических заданий сопровождается выполнением письменного отчета в тетради. Отчет должен выполняться аккуратно, быть легко читаемым подчерком, при этом допускаются общепринятые сокращения.

При дистанционном выполнении практических работ, обучающийся может самостоятельно приобрести операционные системы Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10. Ответственность за установку и настройку программного обеспечения в данном случае ложится на обучающегося. Следует воспользоваться методическими указаниями по установке данных программных систем.

Результаты выполненных заданий оцениваются с учетом теоретических знаний по соответствующим разделам дисциплины, техники выполнения работы, объективности и обоснованности принимаемых решений в процессе работы с данными, качества оформления. Переход к выполнению следующего практического задания допускается только после отчета выполненной работы.

Учебно-методическое издание

Рабочая программа учебной дисциплины

Информационная безопасность

(Наименование дисциплины в соответствии с учебным планом)

Филиппов Михаил Владимирович

(Фамилия, Имя, Отчество составителя)