Автономная некоммерческая организация высшего образования
«Волгоградский институт бизнеса»

Утверждаю
Проректор по учебной работе
и управлению качеством
_____ Г.В. Шарай-Курбатова
«13» 03 2020г.

Рабочая программа учебной дисциплины

Информационная безопасность
(Наименование дисциплины)

09.03.03 Прикладная информатика, направленность (профиль) «ПИЭ»
(Направление подготовки / Профиль)

Бакалавр
(Квалификация)

Прикладной бакалавр
(Вид)

Кафедра разработчик Экономики и управления

Год набора **2016, 2017, 2018**

Вид учебной деятельности	Трудоемкость (объем) дисциплины					
	Очная форма	Очно-заочная форма		Заочная форма		
	д	в	св	з	сз	вв
Зачетные единицы	3			3	3	3
Общее количество часов	108			108	108	108
Аудиторные часы контактной работы обучающегося с преподавателями:	36			14	6	6
– Лекционные (Л)	18			6	2	2
– Практические (ПЗ)	18			8	4	4
– Лабораторные (ЛЗ)						
– Семинарские (СЗ)						
Самостоятельная работа обучающихся (СРО)	72			90	98	98
К (Р-Г) Р (П) (+;-)						
Тестирование (+;-)						
ДКР (+;-)						
Зачет (+;-)	+			+ (4)	+ (4)	+ (4)
Зачет с оценкой (+;- (Кол-во часов))						
Экзамен (+;- (Кол-во часов))						

Волгоград 2020

Содержание

Раздел 1. Организационно-методический раздел

1.1. Цели освоения дисциплины

Дисциплина **«Информационная безопасность»** входит в **«базовую»** часть дисциплин подготовки обучающихся по направлению подготовки **«09.03.03 Прикладная информатика», направленность (профиль) «ПИЭ».**

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

Общепрофессиональных

- «способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности» ***(ОПК-4)***

Профессиональных

- «способностью принимать участие во внедрении, адаптации и настройке информационных систем» ***(ПК-10)***
- «способностью эксплуатировать и сопровождать информационные системы и сервисы» ***(ПК-11)***
- «способностью принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью» ***(ПК-18)***
- «способностью принимать участие в реализации профессиональных коммуникаций в рамках проектных групп, обучать пользователей информационных систем» ***(ПК-19)***

Перечисленные компетенции формируются в процессе достижения **результатов обучения (РО):**

Обучающийся должен знать:

на уровне представлений:

- основные подходы к изучению информационной безопасности ***(1)***
- правовое обеспечение информационной безопасности ***(2)***
- административный уровень информационной безопасности ***(3)***

на уровне воспроизведения:

- основные понятия и определения информационной безопасности ***(4)***
- концепцию информационной безопасности ***(5)***
- уровни обеспечения информационной безопасности ***(6)***

на уровне понимания:

- классификацию угроз информационной безопасности ***(7)***
- политику безопасности ***(8)***
- основные программно-технические меры и средства обеспечения информационной безопасности ***(9)***

Обучающийся должен уметь:

- использовать разграничение и ограничение доступа ***(10)***
- работать с антивирусным программным обеспечением ***(11)***
- формировать политику безопасности организации ***(12)***

Обучающийся должен владеть:

- настройкой различных уровней информационной безопасности автоматизированной системы ***(13)***
- современным программным обеспечением в области информационной безопасности ***(14)***
- навыками профессиональных коммуникаций в рамках проектных групп, обучения пользователей информационных систем ***(15)***

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

№	Предшествующие дисциплины (дисциплины, изучаемые параллельно)	Последующие дисциплины
1	*2*	*3*
1	Информатика и программирование	Администрирование баз данных
2	Правовые основы прикладной информатики	Web-программирование
3	Проектирование информационных систем	Администрирование локальных систем
4	Вычислительные системы, сети и телекоммуникации	Сетевое администрирование
5	Операционные системы	Разработка автоматизированных систем бухгалтерского учета
6	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) «ПИЭ»** 2016, 2017, 2018 года набора;
- Образца рабочей программы учебной дисциплины (утвержден приказом №185-О от 31.08.2017 г.).

Раздел 2. Тематический план

Очная форма обучения (полный срок)

№	Тема дисциплины	Трудоемкость				Результаты обучения
		Всего	Аудиторные занятия		СРО	
			Л	ПЗ (ЛЗ, СЗ)		
1	*2*	*3*	*4*	*5*	*6*	*7*
1	Понятие информационной безопасности. Основные составляющие.	10	2		8	1, 4, 5, 6
2	Угрозы информационной безопасности. Их классификация	10	2		8	7
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	14	2	2	10	2, 5, 6
4	Административный уровень. Политика безопасности	10	2		8	3, 8, 12, 15
5	Организация разноуровневого доступа в информационную систему	12	2	2	8	9, 10, 13
6	Основные программно-технические меры. Защита информации с помощью пароля	12	2	4	6	9, 10, 13
7	Защита от несанкционированного доступа и сетевых хакерских атак	10	2	2	6	9
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	14	2	4	8	11,14,15
9	Основы технологии построения защищенных ОС	16	2	4	10	8, 10, 13
Вид промежуточной аттестации (Зачет)						
Итого		**108**	**18**	**18**	**72**	

Заочная форма обучения (полный срок)

№	Тема дисциплины	Трудоемкость				Результаты обучения
		Всего	Аудиторные занятия		СРО	
			Л	ПЗ (ЛЗ, СЗ)		
1	*2*	*3*	*4*	*5*	*6*	*7*
1	Понятие информационной безопасности. Основные составляющие. Важность проблемы	10	2		8	1, 4, 5, 6
2	Угрозы информационной безопасности. Их классификация	10	2		8	7
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	14		2	12	2, 5, 6
4	Административный уровень. Политика безопасности	12			12	3, 8, 12, 15
5	Организация разноуровневого доступа в информационную систему	12		2	10	9, 10, 13
6	Основные программно-технические меры. Защита информации с помощью пароля	12		2	10	9, 10, 13
7	Защита от несанкционированного доступа и сетевых хакерских атак	10			10	9
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	10	2		8	11,14, 15
9	Основы технологии построения защищенных ОС	14		2	12	8, 10, 13
Вид промежуточной аттестации (Зачет)		**4**				
Итого		**108**	**6**	**8**	**90**	

Заочная форма обучения (на базе СПО, на базе ВО)

№	Тема дисциплины	Трудоемкость				Результаты обучения
		Всего	Аудиторные занятия		СРО	
			Л	ПЗ (ЛЗ, СЗ)		
1	*2*	*3*	*4*	*5*	*6*	*7*
1	Понятие информационной безопасности. Основные составляющие. Важность проблемы	12	2		10	1, 4, 5, 6
2	Угрозы информационной безопасности. Их классификация	10			10	7
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	14		2	12	2, 5, 6
4	Административный уровень. Политика безопасности	12			12	3, 8, 12, 15
5	Организация разноуровневого доступа в информационную систему	10			10	9, 10, 13
6	Основные программно-технические меры. Защита информации с помощью пароля	10			10	9, 10, 13
7	Защита от несанкционированного доступа и сетевых хакерских атак	10			10	9
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	10			10	11, 14, 15
9	Основы технологии построения защищенных ОС	16		2	14	8, 10, 13
Вид промежуточной аттестации (Зачет)		**4**				
Итого		**108**	**2**	**4**	**98**	

Раздел 3. Содержание дисциплины

3.1. Содержание дисциплины

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

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

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

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
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)

№	Тема практического (семинарского, практического) занятия
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

Заочная форма обучения (на базе СПО, на базе ВО)

№	Тема практического (семинарского, практического) занятия
1	*2*
Основные программно-технические меры. Защита информации с помощью пароля	
ПЗ 1	Создание резервных копий файлов (для баз данных и проектов Access)
Основы технологии построения защищенных ОС	
ПЗ 2	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	Угрозы информационной безопасности. Их классификация	Л	Дискуссия	75
2	Административный уровень. Политика безопасности	Л	Деловая игра	100
3	Основные программно-технические меры. Защита информации с помощью пароля	ПЗ	Мозговой штурм	50
4	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	Л	Лекция-конференция	100
5	Основы технологии построения защищенных ОС	ПЗ	Дискуссия	50
Итого				**21%**

Заочная форма обучения (полный срок)

№	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	50
2	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	Л	Лекция – конференция	100
Итого				**21%**

Заочная форма обучения (на базе СПО, 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	50
2	Основы технологии построения защищенных ОС	ПЗ	Дискуссия	50
Итого				**33%**

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			Результаты обучения
		Л	ПЗ (ЛЗ, СЗ)	СРО	
1	*2*	*3*	*4*	*5*	*6*
1	Понятие информационной безопасности. Основные составляющие. Важность проблемы	УО		ПРВ	1, 4, 5, 6
2	Угрозы информационной безопасности. Их классификация	УО		ПРВ	7
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	УО	УО	ПРВ	2, 5, 6
4	Административный уровень. Политика безопасности	УО		ПРВ	3, 8, 12, 15
5	Организация разноуровневого доступа в информационную систему	УО	УО	ПРВ	9, 10, 13
6	Основные программно-технические меры. Защита информации с помощью пароля	УО	МШ	ПРВ	9, 10, 13
7	Защита от несанкционированного доступа и сетевых хакерских атак	УО	УО	ПРВ	9
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	УО	УО	ПРВ	11, 14, 15
9	Основы технологии построения защищенных ОС	УО	Д	ПРВ	8, 10, 13

Заочная форма обучения (полный срок)

№	Контролируемые разделы (темы) дисциплины	Оценочные средства			Результаты обучения
		Л	ПЗ (ЛЗ, СЗ)	СРО	
1	*2*	*3*	*4*	*5*	*6*
1	Понятие информационной безопасности. Основные составляющие. Важность проблемы	УО		ПРВ	1, 4, 5, 6
2	Угрозы информационной безопасности. Их классификация	УО		ПРВ	7
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства		УО	ПРВ	2, 5, 6
4	Административный уровень. Политика безопасности			ПРВ	3, 8, 12, 15
5	Организация разноуровневого доступа в информационную систему		УО	ПРВ	9, 10, 13
6	Основные программно-технические меры. Защита информации с помощью пароля		МШ	ПРВ	9, 10, 13
7	Защита от несанкционированного доступа и сетевых хакерских атак			ПРВ	9
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	УО		ПРВ	11, 14, 15
9	Основы технологии построения защищенных ОС		Д	ПРВ	8, 10, 13

Заочная форма обучения (на базе СПО, на базе ВО)

№	Контролируемые разделы (темы) дисциплины	Оценочные средства			Результаты обучения
		Л	ПЗ (ЛЗ, СЗ)	СРО	
1	*2*	*3*	*4*	*5*	*6*
1	Понятие информационной безопасности. Основные составляющие. Важность проблемы	УО		ПРВ	1, 4, 5, 6
2	Угрозы информационной безопасности. Их классификация			ПРВ	7
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства		УО	ПРВ	2, 5, 6
4	Административный уровень. Политика безопасности			ПРВ	3, 8, 12, 15
5	Организация разноуровневого доступа в информационную систему			ПРВ	9, 10, 13
6	Основные программно-технические меры. Защита информации с помощью пароля			ПРВ	9, 10, 13
7	Защита от несанкционированного доступа и сетевых хакерских атак			ПРВ	9
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов			ПРВ	11, 14, 15
9	Основы технологии построения защищенных ОС			ПРВ	8, 10, 13

Условные обозначения оценочных средств (Столбцы 3, 4, 5):

УО – Устный (фронтальный, индивидуальный, комбинированный) опрос;

ПРВ – Проверка рефератов, отчетов, рецензий, аннотаций, конспектов, графического материала, эссе, переводов, решений заданий, выполненных заданий в электронном виде и т.д.

Д – Дискуссия, полемика, диспут, дебаты

МШ – Метод мозгового штурма

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 зачету:

1. Основные понятия информационной безопасности.
2. Основные составляющие. Доступность, целостность и конфиденциальность информации.
3. Доктрина информационной безопасности РФ.
4. Классификация защищаемой информации по степени важности и ценности.
5. Основные определения и критерии классификации угроз.
6. Законодательный уровень информационной безопасности.
7. Административный уровень информационной безопасности.
8. Содержание политики безопасности. Программа безопасности.
9. Управление рисками. Основные понятия. Подготовительный этап управления рисками.
10. Управление рисками. Основные этапы управления рисками.
11. Методы и модели анализа угроз.
12. Поддержание работоспособности. Реагирование на нарушения режима безопасности.
13. Основные программно-технические меры.
14. Архитектурная безопасность.
15. Идентификация и аутентификация, управление доступом.
16. Мониторинг и аудит.
17. Шифрование, контроль целостности.
18. Экранирование, анализ защищенности.
19. Классификация межсетевых экранов.
20. Обеспечение высокой доступности.

Раздел 6. Перечень учебной литературы, необходимой для освоения дисциплины

6.1. Основная литература

1. Никифоров С.Н. Защита информации. Защита от внешних вторжений [Электронный ресурс] : учебное пособие / С.Н. Никифоров. — Электрон. текстовые данные. — СПб. : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 84 с. — 978-5-9227-0757-2. — Режим доступа: http://www.iprbookshop.ru/74381.html
2. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д.А. Скрипник. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 424 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52161.html
3. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 с. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html
4. Фомин Д.В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства [Электронный ресурс] : учебно-методическое пособие / Д.В. Фомин. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 218 с. — 978-5-4487-0297-6. — Режим доступа: http://www.iprbookshop.ru/77317.html

6.2. Дополнительная литература

5. Авдошин С.М. Технологии и продукты Microsoft в обеспечении информационной безопасности [Электронный ресурс] / С.М. Авдошин, А.А. Савельева, В.А. Сердюк. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 412 с. — 978-5-4487-0147-4. — Режим доступа: http://www.iprbookshop.ru/72341.html
6. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс] : учебное пособие / Ю.Н. Сычев. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 195 с. — 978-5-4487-0128-3. — Режим доступа: http://www.iprbookshop.ru/72345.html
7. Бурняшов Б.А. Меры защиты информации на уровне пользователя информационно-технологическими средствами [Электронный ресурс]: методические указания к самостоятельной работе студентов. Учебно-методическое пособие/ Бурняшов Б.А.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2014.— 55 с.— Режим доступа: http://www.iprbookshop.ru/23077.— ЭБС «IPRbooks».

6.3. Другие источники информации и средства обеспечения освоения дисциплины

8. Журнал «Бизнес. Образование. Право. Вестник Волгоградского института бизнеса» [Электронный ресурс] // Режим доступа: http://vestnik.volbi.ru/
9. Журнал «Мир ПК» [Электронный ресурс] // Режим доступа: http://www.osp.pcworld
10. Журнал «Компьютерра-онлайн» [Электронный ресурс] // Режим доступа: http://www2.computerra.ru
11. Журнал «Хакер» [Электронный ресурс] // Режим доступа: http://www.xakep.ru
12. Журнал «Сети» [Электронный ресурс] // Режим доступа: http://www.osp.ru/nets.
13. Журнал «Computerworld» [Электронный ресурс] // Режим доступа: http://www.osp.ru/cw.
14. Журнал «LAN» [Электронный ресурс] // Режим доступа: URL: http://www.osp.ru/lan /+электронный ресурс/.
15. Издательство “Открытые системы” [Электронный ресурс] // Режим доступа: http://www.osp.ru.
16. СПС Гарант [Электронный ресурс] // Режим доступа: http://www.garant.ru/
17. СПС Консультант [Электронный ресурс] // Режим доступа: http://www.consultant.ru/
18. ЦИТ Форум [Электронный ресурс] // Режим доступа: http://citforum.ru.
19. ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. http://base.garant.ru/12148555/

Раздел 7. Материально-техническая база и информационные технологии

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине:

Материально-техническое обеспечение дисциплины **«Информационная безопасность»** включает в себя учебные аудитории для проведения 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.

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)