

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ващенко Андрей Александрович

Должность: Ректор

Дата подписания: 11.01.2021 16:14:17

Уникальный программный ключ:

51187754f94e37d00c9236cc9eaf21a22f0a3b731acd32879ec947ce3c66589d

Автономная некоммерческая организация высшего образования
«Волгоградский институт бизнеса»



Рабочая программа учебной дисциплины

Безопасность информации в сфере сервиса

(Наименование дисциплины)

43.03.01 Сервис, направленность (профиль) «Общий»

(Направление подготовки / Профиль)

Бакалавр

(Квалификация)

Прикладной бакалавр

(Вид бакалавриата)

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
Зачетные единицы	3			3	3	3
Общее количество часов	108			108	108	108
Аудиторные часы контактной работы обучающегося с преподавателями:	36			8	6	6
- Лекционные (Л)	18			2	2	2
- Практические (ПЗ)	18			6	4	4
- Лабораторные (ЛЗ)						
- Семинарские (СЗ)						
Самостоятельная работа обучающихся (СРО)	72			96	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	3
Раздел 2. Тематический план	5
Раздел 3. Содержание дисциплины	7
Раздел 4. Организация самостоятельной работы обучающихся.....	11
Раздел 5. Фонд оценочных средств для проведения промежуточной аттестации обучающихся	14
Раздел 6. Перечень учебной литературы, необходимой для освоения дисциплины	18
Раздел 7. Материально-техническая база	20
Раздел 8. Методические указания для обучающихся по освоению дисциплины	22

Раздел 1. Организационно-методический раздел

1.1. Цели освоения дисциплины

Дисциплина «Безопасность информации в сфере сервиса» входит в **вариативную часть** дисциплин подготовки обучающихся по направлению подготовки **43.03.01 Сервис, направленность (профиль) «Общий»** и является дисциплиной обязательной для изучения.

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

общефессиональных:

- «способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, использовать различные источники информации по объекту сервиса» (**ОПК-1**)

профессиональных:

- «готовностью к разработке процесса предоставления услуг, в том числе в соответствии с требованиями потребителя, на основе новейших информационных и коммуникационных технологий» (**ПК-7**)

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

1. Дать обучающимся теоретические знания о том, что такое информационная безопасность, какие угрозы информационной безопасности существуют.
2. Сформировать у обучающихся представление о важности проблемы информационной безопасности в современном обществе.
3. Научить обучающихся самостоятельно настраивать систему безопасности компьютера, используя штатные средства операционной системы, а также дополнительное программное обеспечение.

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 предприятия (12);
- соблюдать основные требования информационной безопасности при решении профессиональных задач (13);

Обучающийся должен владеть:

- навыками обеспечения информационной безопасности информационной системы предприятия (14).

**1.2. Место дисциплины в структуре ОПОП ВО
направления подготовки 43.03.01 Сервис,
направленность (профиль) «Общий»**

№	Предшествующие дисциплины (дисциплины, изучаемые параллельно)	Последующие дисциплины
1	Информатика	Экономика предприятий сервиса
2	Информационные технологии в сервисе	

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 **43.03.01 Сервис** (уровень бакалавриата);
- Учебного плана направления подготовки **43.03.01 Сервис, направленность (профиль) «Общий»** 2016, 2017, 2018 года набора;
- Образца рабочей программы учебной дисциплины (приказ № 185-О от 31.08.2017 г.).

Раздел 2. Тематический план

Очная форма обучения (полный срок)

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

Заочная форма обучения (полный срок)

№	Тема дисциплины	Трудоемкость				СРО	Результаты обучения
		Всего	Аудиторные занятия				
			Л	ПЗ (ЛЗ, СЗ)			
1	2	3	4	5	6	7	
1	Понятие информационной безопасности. Угрозы информационной безопасности	14	2		12	1,4,5,6,7,13	
2	Законодательный уровень информационной безопасности: обзор Российского и зарубежного законодательства	14			14	2,5,6	
3	Административный уровень. Политика безопасности	12			12	3,8,12	
4	Организация разноразовного доступа в информационную систему	12		2	10	9,10,13,14	
5	Основные программно-технические меры. Защита информации с помощью пароля	12		2	10	9,10,13,14	
6	Защита от несанкционированного доступа и сетевых хакерских атак	14			14	9	
7	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	12			12	7,11	
8	Основы технологии построения защищенного ПО	14		2	12	8,10,13,14	
Вид итогового контроля (Зачет)		4					
Итого		108	2	6	96		

Заочная форма обучения (на базе СПО)

№	Тема дисциплины	Трудоемкость			СРО	Результаты обучения
		Всего	Аудиторные занятия			
			Л	ПЗ (ЛЗ, СЗ)		
1	2	3	4	5	6	7
1	Понятие информационной безопасности. Угрозы информационной безопасности	8	2		6	1,4,5,6,7,13
2	Законодательный уровень информационной безопасности: обзор Российского и зарубежного законодательства	4			4	2,5,6
3	Административный уровень. Политика безопасности	6			6	3,8,12
4	Организация равноуровневого доступа в информационную систему	6			6	9,10,13,14
5	Основные программно-технические меры. Защита информации с помощью пароля	6		2	4	9,10,13,14
6	Защита от несанкционированного доступа и сетевых хакерских атак	6			6	9
7	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	6			6	7,11
8	Основы технологии построения защищенного ПО	8		2	6	8,10,13,14
Вид итогового контроля (Зачет)		4				
Итого		108	2	4	44	

Заочная форма обучения (на базе ВО)

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

Раздел 3. Содержание дисциплины

3.1. Содержание дисциплины

Тема 1. Понятие информационной безопасности. Угрозы информационной безопасности

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.

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 2. 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 3. Административный уровень. Политика безопасности

Политика безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом.

Тема 4. Организация равноуровневого доступа в информационную систему

Типы политик безопасности. Ролевое управление доступом.

Тема 5. 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 6. Защита от несанкционированного доступа и сетевых хакерских атак

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

Тема 7. 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 8. Основы технологии построения защищенного ПО

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

3.2. Содержание практического блока дисциплины

Очная форма обучения (полный срок)

№	Тема практического (семинарского, лабораторного) занятия
1	2
Тема 2. Законодательный уровень информационной безопасности: обзор Российского и зарубежного законодательства	
ПЗ 1	Изучение нормативно – правовой базы в области информационной безопасности с помощью СПС Консультант Плюс
Тема 4. Организация разноразового доступа в информационную систему	
ПЗ 2	Администрирование баз данных и проектов Access
Тема 5. 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
Тема 6. Защита от несанкционированного доступа и сетевых хакерских атак	
ПЗ 5	Защита от несанкционированного доступа и сетевых хакерских атак
Тема 7. 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
Тема 8. Основы технологии построения защищенного ПО	
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, лабораторного) занятия
1	2
<i>Тема 4. Организация разноразовного доступа в информационную систему</i>	
ПЗ 1	Администрирование баз данных и проектов Access
<i>Тема 5. Основные программно-технические меры. Защита информации с помощью пароля</i>	
ПЗ 2	Создание резервных копий файлов (для баз данных и проектов Access)
<i>Тема 8. Основы технологии построения защищенного ПО</i>	
ПЗ 3	Основные признаки присутствия на компьютере вредоносных программ

Заочная форма обучения (на базе СПО)

№	Тема практического (семинарского, лабораторного) занятия
1	2
<i>Тема 5. Основные программно-технические меры. Защита информации с помощью пароля</i>	
ПЗ 1	Создание резервных копий файлов (для баз данных и проектов Access)
<i>Тема 8. Основы технологии построения защищенного ПО</i>	
ПЗ 2	Основные признаки присутствия на компьютере вредоносных программ

Заочная форма обучения (на базе ВО)

№	Тема практического (семинарского, лабораторного) занятия
1	2
<i>Тема 2. Законодательный уровень информационной безопасности: обзор Российского и зарубежного законодательства</i>	
ПЗ 1	Изучение нормативно – правовой базы в области информационной безопасности с помощью СПС Консультант Плюс
<i>Тема 8. Основы технологии построения защищенного ПО</i>	
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	Понятие информационной безопасности. Угрозы информационной безопасности.	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	75
4	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	Л	Лекция – конференция	100
5	Основы технологии построения защищенного ПО	ПЗ	Дискуссия	50
Итого				22,2%

Заочная форма обучения (полный срок)

№	Тема занятия	Вид учебного занятия	Форма / Методы интерактивного обучения	% учебного времени
1	Понятие информационной безопасности. Угрозы информационной безопасности.	Л	Дискуссия	50
2	Основные программно-технические меры. Защита информации с помощью пароля	ПЗ	Мозговой штурм	50
Итого				25%

Заочная форма обучения (на базе СПО)

№	Тема занятия	Вид учебного занятия	Форма / Методы интерактивного обучения	% учебного времени
1	Основные программно-технические меры. Защита информации с помощью пароля	ПЗ	Мозговой штурм	50
2	Основы технологии построения защищенного ПО	ПЗ	Дискуссия	50
Итого				33,3%

Заочная форма обучения (на базе ВО)

№	Тема занятия	Вид учебного занятия	Форма / Методы интерактивного обучения	% учебного времени
1	Понятие информационной безопасности. Угрозы информационной безопасности.	Л	Дискуссия	50
2	Основы технологии построения защищенного ПО	ПЗ	Дискуссия	50
Итого				33,3%

Раздел 4. Организация самостоятельной работы обучающихся

4.1. Организация самостоятельной работы обучающихся

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

Перечень вопросов, выносимых на СРО

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

22. Способы защиты от компьютерных атак.
23. Многоуровневая защита корпоративных сетей.
24. Современное антивирусное программное обеспечение. Примеры

4.2. Тематика письменных работ обучающихся

При изучении дисциплины обучающимся в рамках СРО предлагается написание рефератов. Такие работы направлены на развитие у обучающихся теоретических сведений об обеспечении информационной безопасности. При выполнении реферата обучающийся должен закрепить знания, ранее приобретенные при прослушивании курса лекций по указанной дисциплине.

Тематика рефератов:

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. Примеры реализации.
8. Процедурный уровень информационной безопасности.
9. Идентификация, аутентификация с помощью биометрических параметров.
10. История криптографии.
11. Основные понятия и определения криптологии. Шифрование.
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. Методы и средства защиты информационных ресурсов.
21. Системы защиты от несанкционированного доступа.
22. Защита от информационных инфекций.
23. Вирус: основные понятия, виды.
24. Троянский конь как одна из угроз безопасности информации.
25. Сетевые черви: милье создания или угроза информационной безопасности.
26. Профилактика и лечение информационных инфекций.
27. Программы обнаружения и защиты от вирусов.
28. Современные антивирусные программы (на примере трех программ).
29. Методы обнаружения и удаления вирусов.

30. Общая характеристика организационных методов защиты.
31. Организационные каналы передачи информации.

4.3. 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. Лекционные материалы 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 промежуточной аттестации обучающихся

Фонд оценочных средств по дисциплине представляет собой совокупность контролируемых материалов предназначенных для измерения уровня достижения обучающимися установленных результатов образования. ФОС по дисциплине используется при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся. В полном объеме ФОС размещен в учебно-методическом комплексе по дисциплине.

5.1. Структура фонда оценочных средств

Очная форма обучения (полный срок)

№	Наименование темы дисциплины	Оценочные средства			Результаты обучения
		Л	ПЗ (ПЗ, СЗ)	СРО	
1	2	3	4	5	6
1	Понятие информационной безопасности. Угрозы информационной безопасности	ПРВ, Д		ПРВ	1,4,5,6,7,13
2	Законодательный уровень информационной безопасности: обзор Российского и зарубежного законодательства	ПРВ	УО	ПРВ	2,5,6
3	Административный уровень. Политика безопасности	ПРВ, ДИ		ПРВ	3,8,12
4	Организация равноуровневого доступа в информационную систему	ПРВ	УО	ПРВ	9,10,13,14
5	Основные программно-технические меры. Защита информации с помощью пароля	ПРВ	УО, МШ	ПРВ	9,10,13,14
6	Защита от несанкционированного доступа и сетевых хакерских атак	ПРВ	УО	ПРВ	9
7	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	ПРВ, ЛК	УО	ПРВ	7,11
8	Основы технологии построения защищенного ПО	ПРВ	Д, Т	ПРВ	8,10,13,14

Заочная форма обучения (полный срок)

№	Наименование темы дисциплины	Оценочные средства			Результаты обучения
		Л	ПЗ (ПЗ, СЗ)	СРО	
1	2	3	4	5	6
1	Понятие информационной безопасности. Угрозы информационной безопасности	ПРВ, Д		ПРВ	1,4,5,6,7,13
2	Законодательный уровень информационной безопасности: обзор Российского и зарубежного законодательства			ПРВ	2,5,6
3	Административный уровень. Политика безопасности			ПРВ	3,8,12
4	Организация равноуровневого доступа в информационную систему		УО	ПРВ	9,10,13,14
5	Основные программно-технические меры. Защита информации с помощью пароля		УО, МШ	ПРВ	9,10,13,14
6	Защита от несанкционированного доступа и сетевых хакерских атак			ПРВ	9

7	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов			ПРВ	7,11
8	Основы технологии построения защищенного ПО		УО	ПРВ	8,10,13,14

Заочная форма обучения (на базе СПО)

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

Заочная форма обучения (на базе ВО)

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

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;
МШ – Метод мозгового штурма;
МКС – Метод компьютерной симуляции;
Д – Дискуссия, полемика, диспут, дебаты;
МП – Метод проектов;
ЛС – Лекция ситуация;
ЛК – Лекция-конференция;
ПЛ – Проблемная лекция;
П – Портфолио.

5.2. Перечень вопросов к итоговому контролю знаний 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. Разработка системы технической защиты информации [Электронный ресурс]: учебное пособие/ В.И. Аверченков [и др.].— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 187 с.— Режим доступа: <http://www.iprbookshop.ru/7005>.— ЭБС «IPRbooks»
2. Аверченков В.И. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 184 с.— Режим доступа: <http://www.iprbookshop.ru/7002>.— ЭБС «IPRbooks».
3. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: <http://www.iprbookshop.ru/10677>.— ЭБС «IPRbooks».

6.2. Дополнительная литература

4. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И.— Электрон. текстовые данные.— Брянск: БГТУ, 2012.— 268 с.— Режим доступа: <http://www.iprbookshop.ru/6991>.— ЭБС «IPRbooks».
5. Аверченков В.И. История развития системы государственной безопасности России [Электронный ресурс]: учебное пособие/ Аверченков В.И., Ерохин В.В.— Электрон. текстовые данные.— Брянск: БГТУ, 2012.— 192 с.— Режим доступа: <http://www.iprbookshop.ru/6997>.— ЭБС «IPRbooks».
6. 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».
7. Малюк А.А. Теория защиты информации [Электронный ресурс]: монография/ Малюк А.А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 184 с.— Режим доступа: <http://www.iprbookshop.ru/12048>.— ЭБС «IPRbooks».

6.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

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.haker.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/](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

Материально-техническое обеспечение дисциплины «**Безопасность информации в сфере сервиса**» 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\O3Y 4Gb\500GB\RadeonHD5450
- 2) Intel PENTIUM 2.9GHz\O3Y 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 NAP-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 XP/7/8/10,
- Архиватор 7-zip,
- Система тестирования AST-Test,
- Microsoft Office 2007/2010,
- 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 «Безопасность информации в сфере сервиса» - 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. Решение 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 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 следующей практической работы допускается только после отчета выполненной работы.

Учебно-методическое издание

Рабочая программа учебной дисциплины

Безопасность информации в сфере сервиса

(Наименование дисциплины в соответствии с учебным планом)

Филиппов Михаил Владимирович

(Фамилия, Имя, Отчество составителя)
