

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Майкопский государственный технологический университет»

Факультет информационных систем в экономике и юриспруденции

Кафедра информационной безопасности и прикладной информатики



УТВЕРЖДАЮ
Проректор по учебной работе
Л.И. Задорожная
28 августа 2019 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.Б.28 Информационная безопасность в глобальной сети

по направлению подготовки 40.03.01 Юриспруденция

профиль Уголовно-правовой

Квалификация (степень)

выпускника бакалавр

Уровень подготовки бакалавриат

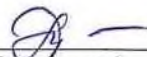
Форма обучения Очная, заочная

Год начала подготовки 2019

Рабочая программа составлена на основе ФГОС ВО и учебного плана МГТУ по направлению (специальности) 40.03.01 Юриспруденция

Составитель рабочей программы:

Старший преподаватель
(должность, ученое звание, степень)


(подпись)

Брикова И.В.
(Ф.И.О.)

Рабочая программа утверждена на заседании кафедры

Информационной безопасности и прикладной информатики

(наименование кафедры)

Заведующий кафедрой

«28» августа 2019 г.


(подпись)

Чундышко В.Ю..
(Ф.И.О.)

Одобрено учебно-методической комиссией факультета
(где осуществляется обучение)

«28» августа 2019 г.

Председатель
учебно-методического
совета направления (специальности)
(где осуществляется обучение)


(подпись)

Курбанова Е.М.
(Ф.И.О.)

Декан факультета
(где осуществляется обучение)

«28» августа 2019 г.


(подпись)

Доргушаева А.К.
(Ф.И.О.)

СОГЛАСОВАНО:

Начальник УМУ

«28» августа 2019 г.


(подпись)

Чудесова Н.Н..
(Ф.И.О.)

Зав. выпускающей кафедрой
по направлению (специальности)


(подпись)

Курбанова Е.М.
(Ф.И.О.)

1. Цели и задачи освоения дисциплины

Цель изучения дисциплины «Информационная безопасность в глобальной сети» - заложить терминологический фундамент, научить проводить анализ угроз информационной безопасности в глобальной сети, выполнять основные этапы решения задач информационной безопасности глобальной сети, рассмотреть основные общеметодологические принципы теории информационной безопасности; изучение методов и средств обеспечения информационной безопасности в глобальной сети.

Для реализации поставленной цели необходимо решить следующие **задачи**:

- ознакомление студентов с терминологией информационной безопасности;
- развитие мышления студентов;
- изучение угроз безопасности при функционировании глобальной сети;
- изучение методов и средств обеспечения информационной безопасности в глобальной сети.

2. Место дисциплины в структуре ОП бакалавриата

Дисциплина «Информационная безопасность в глобальной сети» входит в обязательный перечень базовой части ОП направления подготовки «Юриспруденция».

Для успешного освоения данной дисциплины необходимы базовые и специальные знания, полученные при изучении ОП бакалавриата, знания, полученные при изучении дисциплины «Информатика»; умения применять сетевые средства вычислительной техники для решения практических задач; навыки работы в компьютерных сетях использования современного программного обеспечения.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

В результате изучения учебной дисциплины у обучающегося формируются следующие компетенции:

- владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3);

- способность работать с информацией в глобальных компьютерных сетях (ОК-4);

В результате освоения дисциплины обучающийся должен:

Знать:

- сущность информации, основные свойства информации и закономерности развития современного информационного общества (ОК-3);

- основные характеристики современных компьютерных информационных сетей, основные тенденции развития технологий передачи информации в информационных системах (ОК-4).

Уметь:

- распознавать опасности и угрозы, возникающие в процессе работы с секретной информацией (ОК-3);

- применять сервисы глобальных компьютерных сетей в своей профессиональной деятельности (ОК-4).

Владеть:

- навыками получения, хранения и переработки информации, обработки конфиденциальной информации, в том числе содержащей государственную тайну, в соответствии со всеми требованиями по защите информации (ОК-3);

- навыками навигации и поиска информации по ресурсам глобальной компьютерной сети (ОК-4).

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа).

4.1. Объем дисциплины и виды учебной работы по очной форме обучения

Вид учебной работы	Всего часов/з.е.	Семестры
		3
Контактные часы	51,35/1,43	51,35/1,43
В том числе:		
Лекции (Л)	-	-
Практические занятия (ПЗ)	51/1,42	51/1,42
Семинары (С)	-	-
Лабораторные работы (ЛР)	-	--
Контактная работа в период аттестации (КРАТ)	0,35/0,01	0,35/0,01
Самостоятельная работа студентов (СРС) (всего)	57/1,58	57/1,58
В том числе:		
Курсовой проект (работа)		
Расчетно-графические работы		
Реферат	20/0,56	20/0,56
<i>Другие виды СРС (если предусматриваются, приводится перечень видов СРС)</i>		
1. Составление плана-конспекта первоисточников и другой учебной литературы.	30/0,83	30/0,83
2. Составление плана-конспекта.		
3. Проведение мониторинга, подбор и анализ статистических данных.		
4. Выполнение расчетных заданий.		
5. Подготовка к контрольным работам, КСЗ	7/0,19	7/0,19
Форма промежуточной аттестации:		
Экзамен	35,65/0,99	экзамен 35,65/0,99
Общая трудоемкость	144/4	144/4

4.2. Объем дисциплины и виды учебной работы по заочной форме обучения

Вид учебной работы	Всего часов/з.е.	Семестры
		5
Контактные часы	14,35/0,4	14,35/0,4
В том числе:		
Лекции (Л)		
Практические занятия (ПЗ)	6/0,17	6/0,17
Семинары (С)		
Лабораторные работы (ЛР)	-	-
Контактная работа в период аттестации (КРАТ)	0,35/0,01	0,35/0,01
Самостоятельная работа студентов (СРС) (всего)	129/3,58	129/3,58
В том числе:		
Курсовой проект (работа)		
Расчетно-графические работы		
Реферат	29/0,81	29/0,81
<i>Другие виды СРС (если предусматриваются, приводится перечень видов СРС)</i>		
1. Составление плана-конспекта первоисточников и другой учебной литературы. 2. Составление плана-конспекта. 3. Проведение мониторинга, подбор и анализ статистических данных. 4. Выполнение расчетных заданий. 5. Подготовка к контрольным работам, КСЗ	100/2,78	100/2,78
Форма промежуточной аттестации:		экзамен
Экзамен	8,65/0,24	8,65/0,24
Общая трудоемкость	144/4	144/4

5. Структура и содержание дисциплины

5.1. Структура дисциплины для очной формы обучения

№ п/п	Раздел дисциплины	Неделя се- местра	Виды учебной работы, включая самостоятельную и трудоемкость (в часах)				Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточ- ной аттестации (по семестрам)
			Лек	С/ПЗ	ЛР	СРС	
1.	Введение. Общие во- просы информацион- ной безопасности.	1-2		6		6	Устный опрос, тест
2.	Угрозы безопасности.	3-4		6		6	Устный опрос, тест
3.	Информационная без- опасность в условиях функционирования глобальных сетей	5-6		6		7	Устный опрос, реферат
4.	Алгоритмы безопасно- сти в компьютерных сетях.	7-8		6		6	Устный опрос, реферат
5.	Защита от удаленных атак в сети Интернет	9-10		6		6	Устный опрос, контрольная работа
6.	Программно- аппаратные методы защиты от удаленных атак в сети Интернет.	11-12		6		6	Устный опрос, тест
7.	Защита персональных данных в сети Интер- нет	13-14		6		6	Устный опрос, тест
8.	Рынок систем безопас- ности	15		2		7	Устный опрос, реферат
9.	Информационная вой- на	16-17		7		7	Устный опрос, реферат
10.	Промежуточная атте- стация.						Экзамен в устной форме
	ИТОГО:		-	51	-	57	

5.2. Структура дисциплины для заочной формы обучения

№ п/п	Раздел дисциплины	Виды учебной работы, включая самостоятельную и трудоемкость (в часах)			
		Л	С/ПЗ	ЛР	СРС
1.	Введение. Общие вопросы информационной безопасности.				13
2.	Угрозы безопасности.				13
3	Информационная безопасность в условиях функционирования глобальных сетей		1		15
4.	Алгоритмы безопасности в компьютерных сетях.		1		15
5.	Защита от удаленных атак в сети Интернет		1		13
6.	Программно-аппаратные методы защиты от удаленных атак в сети Интернет.		1		14
7.	Защита персональных данных в сети Интернет		1		14
8.	Рынок систем безопасности				16
9.	Информационная война		1		16
10.	Промежуточная аттестация экзамен				
	Итого:		6	-	129

5.3. Содержание разделов дисциплины «Информационная безопасность в глобальной сети», образовательные технологии

Лекционный курс учебным планом не предусмотрен

5.4. Практические и семинарские занятия, их наименование, содержание и объем в часах

№ п/п	№ раздела дисциплины	Наименование практических и семинарских занятий	Объем в часах / трудоемкость в з.е.	
			ОФО	ЗФО
1.	Введение. Общие вопросы информационной безопасности.	Понятия информации, информатизации, информационной системы, информационной безопасности, защиты информации. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Понятие тайны, виды тайн. Принципы защиты информации. Средства защиты информации. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.	6/0,17	-
2.	Угрозы безопасности.	Понятие угрозы. Классификация угроз информационной безопасности. Виды угроз. Основные нарушения. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации. Модель нарушителя. Стратегии защиты информации.	6/0,17	-
3.	Информационная безопасность в условиях функционирования глобальных сетей.	Понятие глобальной информационной сети. История появления и развития всемирной сети. Государственная политика обеспечения информационной безопасности в условиях функционирования глобальных сетей. Современные технологии обеспечения информационной безопасности в условиях функционирования глобальных сетей. Проблемы защиты информации в глобальной сети. Угрозы информационной безопасности функционированию глобальных сетей. Виртуальные частные сети.	6/0,17	1/0,03
4.	Алгоритмы безопасности в компьютерных сетях.	Межсетевые экраны. Проектирование МЭ. Снифферы. Эксплойты. Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании». Протоколирование. Сетевые защищенные протоколы. Криптографи-	6/0,17	1/0,03

		ческая защита информации. Использование электронной подписи. Аутентификация.		
5.	Защита от удаленных атак в сети Интернет	Обнаружение атак. Административные методы защиты от удаленных атак в сети Internet. Анализ сетевого трафика и защита от него. Защита от ложного ARP-сервера. Защита от ложного DNS -сервера. Защита от навязывания ложного маршрута при использовании протокола ICMP. Защита от подмены одной из сторон при взаимодействии с использованием базовых протоколов семейства TCP/IP. Защита от отказа в обслуживании. Атаки, использующие ошибки реализации сетевых служб. Атака через WWW. Методы защиты от удалённых атак в сети Internet.	6/0,17	1/0,03
6.	Программно-аппаратные методы защиты от удаленных атак в сети Интернет.	Программно-аппаратные средства обеспечения информационной безопасности. Методика Firewall как основное программно-аппаратное средство осуществления сетевой политики безопасности в выделенном сегменте IP-сети. Программные методы защиты, применяемые в сети Internet.	6/0,17	1/0,03
7.	Защита персональных данных в сети Интернет	Понятие персональных данных. Субъект, объект персональных данных. Общедоступные источники персональных данных. Незаконное распространение персональных данных в сети Интернет. Особенность распространения персональных данных в сети Интернет за пределами РФ.	6/0,17	1/0,03
8.	Рынок систем безопасности	Основные тенденции рынка систем безопасности: статистика и прогнозы. Структура рынка систем безопасности. Лидеры на ранке систем безопасности.	2/0,05	-
9.	Информационная война.	Технологии информационного противоборства в сети Интернет. Информационная война и ее виды. Информационное оружие и его классификация. Выявление признаков информационной войны в сети Интернет.	7/0,19	1/0,03
10.	Промежуточная аттестация		экзамен	
	Итого:		51/1,42	6/0,17

5.5. Лабораторные занятия, их наименование и объем в часах

№ п/п	№ раздела дисциплины	Наименование лабораторных работ	Объем в часах / трудоемкость в з.е.

5.6. Примерная тематика курсовых проектов (работ)

Не предусмотрены.

5.7. Самостоятельная работа студентов

Содержание и объем самостоятельной работы студентов

№ п/п	Разделы и темы рабочей программы самостоятельного изучения	Перечень домашних заданий и других вопросов для самостоятельного изучения	Сроки выполнения	Объем в часах / трудоемкость в з.е.	
				ОФО	ЗФО
1.	Введение. Общие вопросы информационной безопасности.	Подбор, обобщение и анализ информации из литературных источников и других информационных ресурсов по профилю подготовки.	1-2 неделя	6/0,17	13/0,36
2.	Угрозы безопасности.	Подбор, обобщение и анализ информации из литературных источников и других информационных ресурсов по профилю подготовки.	3-4 неделя	6/0,17	13/0,36
3.	Информационная безопасность в условиях функционирования глобальных сетей.	Подбор, обобщение и анализ информации из литературных источников и других информационных ресурсов по профилю подготовки. Написание реферата	5-6 неделя	7/0,19	15/0,42
4.	Алгоритмы безопасности в компьютерных сетях.	Подбор, обобщение и анализ информации из литературных источников и других информационных ресурсов по профилю подготовки. Написание реферата	7-8 неделя	6/0,17	15/0,42
5.	Защита от удаленных атак в сети Интернет	Подбор, обобщение и анализ информации из литературных источников и других информационных ресурсов по профилю подготовки.	9-10 неделя	6/0,17	13/0,36
6.	Программно-аппаратные методы защиты от удаленных атак в сети Интернет.	Подбор, обобщение и анализ информации из литературных источников и других информационных ресурсов по профилю подготовки.	11-12 неделя	6/0,17	14/0,39
7.	Защита персональных данных в сети Интернет	Подбор, обобщение и анализ информации из литературных источников и других информационных ресурсов по профилю подготовки.	13-14 неделя	6/0,17	14/0,39

8.	Рынок систем безопасности	Подбор, обобщение и анализ информации из литературных источников и других информационных ресурсов по профилю подготовки. Написание реферата	15 неделя	7/0,19	16/0,44
9.	Информационная война.	Подбор, обобщение и анализ информации из литературных источников и других информационных ресурсов по профилю подготовки. Написание реферата	16-17 неделя	7/0,19	16/0,44
10.	Экзамен	Подготовка к экзамену			
	Итого			57/1,58	129/3,58

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

6.1. Методические указания (собственные разработки) нет

6.2 Литература для самостоятельной работы

1. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем [Электронный ресурс]: учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: ИНФРА-М, 2019. - 118 с. - ЭБС «Znanium.com» - Режим доступа: <http://znanium.com/catalog/product/991792>

2. Баранова, Е.К. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: РИОР, ИНФРА-М, 2017. - 322 с. - ЭБС «Znanium.com» - Режим доступа: <http://znanium.com/catalog.php?bookinfo=763644>

3. Галатенко, В.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие / Галатенко В.А. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 266 с. - ЭБС «IPRbooks» - Режим доступа: <http://www.iprbookshop.ru/52209>

4. Защита информации [Электронный ресурс]: учебное пособие / А.П. Жук и др. - Москва: РИОР: ИНФРА-М, 2015. - 392 с. - ЭБС «Znanium.com» - Режим доступа: <http://znanium.com/catalog.php?bookinfo=474838>

5. Петров, С.В. Информационная безопасность [Электронный ресурс]: учебное пособие / Петров С.В., Кисляков П.А. - Саратов: Ай Пи Ар Букс, 2015. - 326 с. - ЭБС «IPRbooks» - Режим доступа: <http://www.iprbookshop.ru/33857>

6. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие / Нестеров С.А. - СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014. - 322 с. - ЭБС «IPRbooks» - Режим доступа: <http://www.iprbookshop.ru/43960>

6. Башлы, П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебник / П.Н. Башлы, А.В. Бабаш, Е.К. Баранова. - М.: РИОР, 2013 - 222с. - ЭБС «Znanium.com» - Режим доступа: <http://znanium.com/catalog.php?bookinfo=405000>

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Этапы формирования компетенции (номер семестра согласно учебному плану)		Наименование учебных дисциплин, формирующих компетенции в процессе освоения образовательной программы
ОФО	ЗФО	
ОК-3: владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией		
1	1	Информатика
3	5	Информационная безопасность в глобальной сети
8	9	Подготовка к сдаче и сдача государственного экзамена
8	9	Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы
ОК-4: способность работать с информацией в глобальных компьютерных сетях		
1	1	Информатика
3	5	Информационная безопасность в глобальной сети
8	9	Подготовка к сдаче и сдача государственного экзамена
8	9	Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетвори- тельно	удовлетворительно	хорошо	отлично	
ОК-3: владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией					
Знать: сущность информации, основные свойства информации и закономерности развития современного информационного общества.	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	тесты, рефераты, экзамен
Уметь: распознавать опасности и угрозы, возникающие в процессе работы с секретной информацией.	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть: навыками получения, хранения и переработки информации, обработки конфиденциальной информации, в том числе содержащей государственную тайну, в соответствии со всеми требованиями по защите информации.	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОК-4: способность работать с информацией в глобальных компьютерных сетях					
Знать: основные характеристики современных компьютерных информационных сетей, основные тенденции развития технологий передачи информации в информационных системах.	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	тесты, рефераты, экзамен
Уметь: применять сервисы глобальных компьютерных сетей в своей профессиональной деятельности.	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть: навыками навигации и поиска информации по ресурсам глобальной компьютерной сети.	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	

7.3. Типовые контрольные задания и иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерный перечень вопросов для текущего контроля знаний по дисциплине

1. Понятия информации, информатизации, информационной системы, информационной безопасности, защиты информации.
2. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене.
3. Понятие тайны, виды тайн.
4. Принципы и средства защиты информации.
5. Международные стандарты информационного обмена.
6. Показатели информации: важность, полнота, адекватность, релевантность, толерантность.
7. Требования к защите информации.
8. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.
9. Понятие угрозы. Классификация угроз информационной безопасности.
10. Виды угроз. Основные нарушения.
11. Характер происхождения угроз (умышленные и естественные факторы).
12. Источники угроз. Предпосылки появления угроз.
13. Классы каналов несанкционированного получения информации.
14. Причины нарушения целостности информации.
15. Модель нарушителя.
16. Стратегии защиты информации.
17. Понятие глобальной информационной сети.
18. Государственная политика обеспечения информационной безопасности в условиях функционирования глобальных сетей.
19. Современные технологии обеспечения информационной безопасности в условиях функционирования глобальных сетей.
20. Проблемы защиты информации в глобальной сети.
21. Угрозы информационной безопасности функционированию глобальных сетей.
22. Виртуальные частные сети.
23. Межсетевые экраны. Проектирование МЭ.
24. Снифферы. Эксплоиты.
25. Атаки на сервера. Атаки на рабочие станции.
26. Атака типа «отказ в обслуживании».
27. Протоколирование. Сетевые защищенные протоколы.
28. Использование электронной подписи.
29. Аутентификация.

Темы рефератов

1. История появления и развития всемирной сети.
2. Криптографическая защита информации.
3. Структура рынка систем безопасности.
4. Лидеры на рынке систем безопасности.
5. Информационная война и ее виды.
6. Информационное оружие и его классификация.

Примерный перечень вопросов к экзамену по дисциплине для обучающихся

1. Понятия информации, информатизации, информационной системы, информационной безопасности, защиты информации.

2. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене.
3. Понятие тайны, виды тайн.
4. Принципы и средства защиты информации.
5. Международные стандарты информационного обмена.
6. Показатели информации: важность, полнота, адекватность, релевантность, толерантность.
7. Требования к защите информации.
8. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.
9. Понятие угрозы. Классификация угроз информационной безопасности.
10. Виды угроз. Основные нарушения.
11. Характер происхождения угроз (умышленные и естественные факторы).
12. Источники угроз. Предпосылки появления угроз.
13. Классы каналов несанкционированного получения информации.
14. Причины нарушения целостности информации.
15. Модель нарушителя.
16. Стратегии защиты информации.
17. Понятие глобальной информационной сети.
18. Государственная политика обеспечения информационной безопасности в условиях функционирования глобальных сетей.
19. Современные технологии обеспечения информационной безопасности в условиях функционирования глобальных сетей.
20. Проблемы защиты информации в глобальной сети.
21. Угрозы информационной безопасности функционированию глобальных сетей.
22. Виртуальные частные сети.
23. Межсетевые экраны. Проектирование МЭ.
24. Снифферы. Эксплоиты.
25. Атаки на сервера. Атаки на рабочие станции.
26. Атака типа «отказ в обслуживании».
27. Протоколирование. Сетевые защищенные протоколы.
28. Использование электронной подписи.
29. Аутентификация.
30. Обнаружение атак.
31. Административные методы защиты от удаленных атак в сети Internet.
32. Анализ сетевого трафика и защита от него.
33. Защита от ложного ARP-сервера. Защита от ложного DNS -сервера.
34. Защита от навязывания ложного маршрута при использовании протокола ICMP.
35. Защита от подмены одной из сторон при взаимодействии с использованием базовых протоколов семейства TCP/IP.
36. Защита от отказа в обслуживании.
37. Атаки, использующие ошибки реализации сетевых служб.
38. Атака через WWW.
39. Методы защиты от удалённых атак в сети Internet.
40. Программно-аппаратные средства обеспечения информационной безопасности.
41. Методика Firewall как основное программно-аппаратное средство осуществления сетевой политики безопасности в выделенном сегменте IP-сети.
42. Программные методы защиты, применяемые в сети Internet.
43. Понятие персональных данных. Субъект, объект персональных данных.
44. Общедоступные источники персональных данных. Незаконное распространение персональных данных в сети Интернет.
45. Особенность распространения персональных данных в сети Интернет за пределами РФ.

46. Основные тенденции рынка систем безопасности: статистика и прогнозы.
47. Технологии информационного противоборства в сети Интернет.

Тестовые задания для контроля остаточных знаний по дисциплине

1 вариант

1. К каким средствам защиты информации относятся физические, аппаратные и программные средства?
- а) к формальным;
 - б) к неформальным;
 - в) к техническим.
2. Удаленные атаки можно разделить на два класса:
- а) пассивные и активные
 - б) пассивные и агрессивные
 - в) опасные и безвредные
3. Наступательная стратегия применяется для:
- а) наиболее опасных угроз;
 - б) всех известных угроз;
 - в) всех потенциально возможных угроз.
4. Как называется код, способный самостоятельно вызывать распространение своих копий по ИС и их выполнение?
- а) руткит;
 - б) вирус;
 - в) компьютерный «червь».
5. Упреждающая стратегия применяется для:
- а) наиболее опасных угроз;
 - б) всех известных угроз;
 - в) всех потенциально возможных угроз.
6. К какой стратегии защиты информации относится разработка для существующего объекта организационных мер использования технических средств по ограничению НСД к объекту?
- а) оборонительная;
 - б) наступательная;
 - в) упреждающая.
7. К активным атакам относятся:
- а) отказ в обслуживании - DoS-атака
 - б) модификация потока данных - атака "man in the middle"
 - в) создание ложного потока (фальсификация)
8. Идентификация - это
- а) установление подлинности пользователя;
 - б) установление личности пользователя;
 - в) определение набора прав пользователя;
9. Какие угрозы не относятся к случайным?
- а) сбои и отказы в работе технических средств;
 - б) программные закладки в ПО;
 - в) стихийные бедствия и аварии.

10. К каким средствам защиты относятся механические, электрические, электромеханические устройства и системы, функционирующие автономно, создавая различного рода препятствия на пути дестабилизирующих факторов?

- а) к физическим;
- б) к аппаратным;
- в) к техническим.

11. Что не является целью программно-аппаратной безопасности?

- а) защита данных;
- б) защита каналов связи;
- в) защита пользователя.

2 вариант

1. Оборонительная стратегия применяется для:

- а) наиболее опасных угроз;
- б) всех известных угроз;
- в) всех потенциально возможных угроз.

2. Какие два основных элемента включает понятие «информация»?

- а) сведения и сообщения;
- б) сведения и данные;
- в) сообщения и данные.

3. К каким средствам защиты информации относятся организационные, законодательные и морально-этические средства?

- а) к формальным;
- б) к неформальным;
- в) к техническим.

4. Какая процедура используется для защиты от НСД?

- а) аутентификация;
- б) шифрование;
- в) конфиденциальность.

5. К каким средствам защиты информации относятся физические и аппаратные средства?

- а) к формальным;
- б) к неформальным;
- в) к техническим.

6. Аутентификация - это

- а) определение набора прав пользователя;
- б) процесс авторизации пользователя в компьютерной системе;
- в) установление подлинности пользователя.

7. Какая стратегия защиты информации предполагает использование конкретных мер защиты для каждого конкретного вида угроз (например, антивирусные программы – против компьютерных инфекций)?

- а) оборонительная;
- б) наступательная;
- в) упреждающая.

8. Как называется код, обладающий способностью к распространению путем внедрения в другие программы?

- а) руткит;
- б) вирус;

в) компьютерный «червь».

9. Какая стратегия защиты информации предполагает тщательное исследование возможных угроз системы обработки информации и разработку мер по их нейтрализации еще на стадии проектирования и изготовления системы?

- а) оборонительная;
- б) наступательная;
- в) упреждающая.

10. К каким средствам защиты относятся электронные и электронномеханические устройства, встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации?

- а) к физическим;
- б) к аппаратным;
- в) к техническим.

11. К активным атакам относятся:

- а) отказ в обслуживании - DoS-атака
- б) модификация потока данных - атака "man in the middle"
- в) создание ложного потока (фальсификация).

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений и навыков, и опыта деятельности, характеризующих этапы формирования компетенций

Требования к выполнению тестового задания

Тестирование является одним из основных средств формального контроля качества обучения. Это метод, основанный на стандартизированных заданиях, которые позволяют измерить психофизиологические и личностные характеристики, а также знания, умения и навыки испытуемого.

Основные принципы тестирования, следующие:

- связь с целями обучения - цели тестирования должны отвечать критериям социальной полезности и значимости, научной корректности и общественной поддержки;
- объективность - использование в педагогических измерениях этого принципа призвано не допустить субъективизма и предвзятости в процессе этих измерений;
- справедливость и гласность - одинаково доброжелательное отношение ко всем обучающимся, открытость всех этапов процесса измерений, своевременность ознакомления обучающихся с результатами измерений;
- систематичность – систематичность тестирований и самопроверок каждого учебного модуля, раздела и каждой темы; важным аспектом данного принципа является требование репрезентативного представления содержания учебного курса в содержании теста;
- гуманность и этичность - тестовые задания и процедура тестирования должны исключать нанесение какого-либо вреда обучающимся, не допускать ущемления их по национальному, этническому, материальному, расовому, территориальному, культурному и другим признакам;

Важнейшим является принцип, в соответствии с которым тесты должны быть построены по методике, обеспечивающей выполнение требований соответствующего федерального государственного образовательного стандарта.

В тестовых заданиях используются четыре типа вопросов:

- закрытая форма - является наиболее распространенной и предлагает несколько альтернативных ответов на поставленный вопрос. Например, обучающемуся задается вопрос, требующий альтернативного ответа «да» или «нет», «является» или «не является», «относится» или «не относится» и т.п. Тестовое задание, содержащее вопрос в закрытой форме, включает в себя

один или несколько правильных ответов и иногда называется выборочным заданием. Закрытая форма вопросов используется также в тестах-задачах с выборочными ответами. В тестовом задании в этом случае сформулированы условие задачи и все необходимые исходные данные, а в ответах представлены несколько вариантов результата решения в числовом или буквенном виде. Обучающийся должен решить задачу и показать, какой из представленных ответов он получил.

– открытая форма - вопрос в открытой форме представляет собой утверждение, которое необходимо дополнить. Данная форма может быть представлена в тестовом задании, например, в виде словесного текста, формулы (уравнения), графика, в которых пропущены существенные составляющие - части слова или буквы, условные обозначения, линии или изображения элементов схемы и графика. Обучающийся должен по памяти вставить соответствующие элементы в указанные места («пропуски»).

– установление соответствия - в данном случае обучающемуся предлагают два списка, между элементами которых следует установить соответствие;

– установление последовательности - предполагает необходимость установить правильную последовательность предлагаемого списка слов или фраз.

Критерии оценки знаний при проведении тестирования

Отметка «отлично» выставляется при условии правильного ответа не менее чем 85% тестовых заданий;

Отметка «хорошо» выставляется при условии правильного ответа не менее чем 70 % тестовых заданий;

Отметка «удовлетворительно» выставляется при условии правильного ответа не менее 50 %;

Отметка «неудовлетворительно» выставляется при условии правильного ответа менее чем на 50 % тестовых заданий.

Результаты текущего контроля используются при проведении промежуточной аттестации.

Требования к написанию реферата

Продукт самостоятельной работы обучающегося, представляющий собой краткое изложение в письменном виде полученных результатов (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.

Реферат должен быть структурирован (по главам, разделам, параграфам) и включать разделы: введение, основная часть, заключение, список использованных источников. В зависимости от тематики реферата к нему могут быть оформлены приложения, содержащие документы, иллюстрации, таблицы, схемы и т.д. Объем реферата – 15-20 страниц печатного текста, включая титульный лист, введение, заключение и список литературы.

Его задачами являются:

1. Формирование умений самостоятельной работы с источниками литературы, их систематизация;

2. Развитие навыков логического мышления;

3. Углубление теоретических знаний по проблеме исследования.

При оценке реферата используются следующие критерии:

- новизна текста;

- обоснованность выбора источника;

- степень раскрытия сущности вопроса;

- соблюдения требований к оформлению.

Критерии оценивания реферата:	
«отлично»	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.
«хорошо»	Основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; невыдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.
«удовлетворительно»	Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.
«неудовлетворительно»	Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.

Тематика рефератов выдается преподавателем в конце семинарского занятия.

Критерии оценки знаний на экзамене

Экзамен может проводиться в форме устного опроса по билетам (вопросам) или без билетов, с предварительной подготовкой или без подготовки, по усмотрению преподавателя. Экзаменатор вправе задавать вопросы сверх билета, а также, помимо теоретических вопросов, давать задачи по программе данного курса.

Экзаменационные билеты (вопросы) утверждаются на заседании кафедры и подписываются заведующим кафедрой. В билете должно содержаться не более трех вопросов. Комплект экзаменационных билетов по дисциплине должен содержать 15—20 билетов.

Экзаменатор может проставить экзамен без опроса или собеседования тем обучающимся, которые активно участвовали в практических и лабораторных занятиях.

Отметка «отлично» - обучающийся глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, тесно увязывает теорию с практикой. Обучающийся не затрудняется с ответом при видоизменении задания, свободно справляется с задачами, заданиями и другими видами применения знаний, показывает знания законодательного и нормативно-технического материалов, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических работ, обнаруживает умение самостоятельно обобщать и излагать материал, не допуская ошибок.

Отметка «хорошо» - обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применять теоретические положения и владеет необходимыми навыками при выполнении практических заданий.

Отметка «удовлетворительно» - обучающийся усвоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала и испытывает затруднения в выполнении практических заданий.

Отметка «неудовлетворительно» - обучающийся не знает значительной части программного материала, допускает существенные ошибки, с большими затруднениями выполняет практические работы.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Основная литература

1. Баранова, Е.К. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие / Е.К. Баранова, А.В. Бабаши. - М.: РИОР, ИНФРА-М, 2017. - 322 с. - ЭБС «Znanium.com» - Режим доступа: <http://znanium.com/catalog.php?bookinfo=763644>
2. Галатенко, В.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие / Галатенко В.А. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 266 с. - ЭБС «IPRbooks» - Режим доступа: <http://www.iprbookshop.ru/52209>
3. Защита информации [Электронный ресурс]: учебное пособие / А.П. Жук и др. - Москва: РИОР: ИНФРА-М, 2015. - 392 с. - ЭБС «Znanium.com» - Режим доступа: <http://znanium.com/catalog.php?bookinfo=474838>

8.2. Дополнительная литература

1. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем [Электронный ресурс]: учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: ИНФРА-М, 2019. - 118 с. - ЭБС «Znanium.com» - Режим доступа: <http://znanium.com/catalog/product/991792>
2. Петров, С.В. Информационная безопасность [Электронный ресурс]: учебное пособие / Петров С.В., Кисляков П.А. - Саратов: Ай Пи Ар Букс, 2015. - 326 с. - ЭБС «IPRbooks» - Режим доступа: <http://www.iprbookshop.ru/33857>
3. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие / Нестеров С.А. - СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014. - 322 с. - ЭБС «IPRbooks» - Режим доступа: <http://www.iprbookshop.ru/43960>
4. Башлы, П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебник / П.Н. Башлы, А.В. Бабаши, Е.К. Баранова. - М.: РИОР, 2013 - 222с. - ЭБС «Znanium.com» - Режим доступа: <http://znanium.com/catalog.php?bookinfo=405000>

8.3. Информационно-телекоммуникационные ресурсы сети «Интернет»

1. Органы исполнительной власти:

- Президент РФ: <http://www.kremlin.ru>
- Председатель Правительства РФ: <http://www.premier.gov.ru>
- Правительство РФ: <http://www.government.gov.ru>

2. Органы судебной власти:

- Конституционный Суд РФ: <http://www.ksrf.ru>
- Высший арбитражный суд Российской Федерации: <http://www.arbitr.ru>
- Верховный суд Российской Федерации: <http://www.supcourt.ru>

3. Иные органы исполнительной власти:

- Совет безопасности РФ: <http://www.scrf.gov.ru>
- Центральная избирательная комиссия РФ: <http://www.cikrf.ru>
- Счетная палата РФ: <http://www.ach.gov.ru/ru/>
- Генеральная прокуратура РФ: <http://www.genproc.gov.ru>
- Уполномоченный по правам человека в РФ: <http://www.ombudsman.gov.ru>

4. Министерство внутренних дел РФ

- Министерство внутренних дел: <http://www.mvd.ru>
- Федеральная миграционная служба: <http://www.fms.gov.ru>
- Министерство юстиции РФ: <http://www.minjust.ru>
- Федеральная служба исполнения наказаний: <http://www.fsin.ru>
- Федеральная служба судебных приставов: <http://www.fssprus.ru>
- Федеральная служба РФ по контролю за оборотом наркотиков: <http://www.fskn.gov.ru>

9. Методические указания для обучающихся по освоению дисциплины (модуля) Б1.Б.28 Информационная безопасность в глобальной сети

Раздел / Тема с указанием основных учебных элементов	Методы обучения	Способы (формы) обучения	Средства обучения	Формируемые компетенции
Тема 1. Введение. Общие вопросы информационной безопасности.	по источнику знаний: чтение, конспектирование по назначению: приобретение знаний, анализ, закрепление, проверка знаний по типу познавательной деятельности: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия	владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) способность работать с информацией в глобальных компьютерных сетях (ОК-4)
Тема 2. Угрозы безопасности.	по источнику знаний: чтение, конспектирование по назначению: приобретение знаний, анализ, закрепление, проверка знаний по типу познавательной деятельности: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия	владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) способность работать с информацией в глобальных компьютерных сетях (ОК-4)
Тема 3. Информационная безопасность в условиях функционирования глобальных сетей.	по источнику знаний: чтение, конспектирование по назначению: приобретение знаний, анализ, закрепление, проверка знаний по типу познавательной деятельности: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия, первоисточники	владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) способность работать с информацией в глобальных компьютерных сетях (ОК-4)
Тема 4. Алгоритмы безопасности в компьютерных сетях.	по источнику знаний: чтение, конспектирование по назначению: приобретение	Самостоятельная работа обучающегося, домашние	Учебники, учебные пособия	владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством

	знаний, анализ, закрепление, проверка знаний по типу познавательной деятельности: объяснительно-иллюстративный, репродуктивный	задания		управления информацией (ОК-3) способность работать с информацией в глобальных компьютерных сетях (ОК-4)
Тема 5. Защита от удаленных атак в сети Интернет	по источнику знаний: чтение, конспектирование по назначению: приобретение знаний, анализ, закрепление, проверка знаний по типу познавательной деятельности: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия	владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) способность работать с информацией в глобальных компьютерных сетях (ОК-4)
Тема 6. Программно-аппаратные методы защиты от удаленных атак в сети Интернет.	по источнику знаний: чтение, конспектирование по назначению: приобретение знаний, анализ, закрепление, проверка знаний по типу познавательной деятельности: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия	владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) способность работать с информацией в глобальных компьютерных сетях (ОК-4)
Тема 7. Защита персональных данных в сети Интернет	по источнику знаний: чтение, конспектирование по назначению: приобретение знаний, анализ, закрепление, проверка знаний по типу познавательной деятельности: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия	владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) способность работать с информацией в глобальных компьютерных сетях (ОК-4)
Тема 8. Рынок систем безопасности	по источнику знаний: чтение, конспектирование	Самостоятельная работа обучающегося	Учебники, учебные	владение основными методами, способами и средствами получения, хранения, переработки информа-

	по назначению: приобретение знаний, анализ, закрепление, проверка знаний по типу познавательной деятельности: объяснительно-иллюстративный, репродуктивный	гося, домашние задания	пособия	ции, навыками работы с компьютером как средством управления информацией (ОК-3) способность работать с информацией в глобальных компьютерных сетях (ОК-4)
Тема 9. Информационная война.	по источнику знаний: чтение, конспектирование по назначению: приобретение знаний, анализ, закрепление, проверка знаний по типу познавательной деятельности: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия	владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) способность работать с информацией в глобальных компьютерных сетях (ОК-4)

9.1. Учебно-методические материалы по практическим (лабораторным) занятиям дисциплины Б1.Б.28 Информационная безопасность в глобальной сети

№ раздела дисциплины	Наименование практических работ	Методы обучения	Способы (формы) обучения	Средства обучения	Формируемые компетенции
Тема 1. Введение. Общие вопросы информационной безопасности.	Понятия информации, информатизации, информационной системы, информационной безопасности, защиты информации. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Понятие тайны, виды тайн. Принципы защиты информации. Средства защиты информации. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.	по источнику знаний: чтение, конспектирование по назначению: приобретение знаний, анализ, закрепление, проверка знаний по типу познавательной деятельности: объяснительно-иллюстративный, репродуктивный	Учебники, учебные пособия	Устная речь, учебники, учебные пособия	владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) способность работать с информацией в глобальных компьютерных сетях (ОК-4)
Тема 2. Угрозы безопасности.	Понятие угрозы. Классификация угроз информационной безопасности. Виды угроз. Основные нарушения. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного	по источнику знаний: чтение, конспектирование по назначению: приобретение знаний, анализ, закрепление, проверка знаний по типу познавательной деятельности: объяснительно-иллюстративный, репродуктивный	Учебники, учебные пособия	Устная речь, учебники, учебные пособия	владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) способность работать с информацией в глобаль-

	получения информации. Причины нарушения целостности информации. Модель нарушителя. Стратегии защиты информации.				ных компьютерных сетях (ОК-4)
Тема 3. Информационная безопасность в условиях функционирования глобальных сетей.	Понятие глобальной информационной сети. История появления и развития всемирной сети. Государственная политика обеспечения информационной безопасности в условиях функционирования глобальных сетей. Современные технологии обеспечения информационной безопасности в условиях функционирования глобальных сетей. Проблемы защиты информации в глобальной сети. Угрозы информационной безопасности функционированию глобальных сетей. Виртуальные частные сети.	по источнику знаний: чтение, конспектирование по назначению: приобретение знаний, анализ, закрепление, проверка знаний по типу познавательной деятельности: объяснительно-иллюстративный, репродуктивный	Учебники, учебные пособия, первоисточники	Устная речь, учебники, учебные пособия, первоисточники	владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) способность работать с информацией в глобальных компьютерных сетях (ОК-4)
Тема 4. Алгоритмы безопасности в компьютерных сетях.	Межсетевые экраны. Проектирование МЭ. Снифферы. Эксплойты. Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании». Протоколирование. Сетевые защищенные протоколы. Криптографическая защита информации. Использование электронной подписи. Аутентификация.	по источнику знаний: чтение, конспектирование по назначению: приобретение знаний, анализ, закрепление, проверка знаний по типу познавательной деятельности: объяснительно-иллюстративный, репродуктивный	Учебники, учебные пособия	Устная речь, учебники, учебные пособия	владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) способность работать с информацией в глобальных компьютерных сетях (ОК-4)

Тема 5. Защита от удаленных атак в сети Интернет	Обнаружение атак. Административные методы защиты от удаленных атак в сети Internet. Анализ сетевого трафика и защита от него. Защита от ложного ARP-сервера. Защита от ложного DNS -сервера. Защита от навязывания ложного маршрута при использовании протокола ICMP. Защита от подмены одной из сторон при взаимодействии с использованием базовых протоколов семейства TCP/IP. Защита от отказа в обслуживании. Атаки, использующие ошибки реализации сетевых служб. Атака через WWW. Методы защиты от удалённых атак в сети Internet.	по источнику знаний: чтение, конспектирование по назначению: приобретение знаний, анализ, закрепление, проверка знаний по типу познавательной деятельности: объяснительно-иллюстративный, репродуктивный	Учебники, учебные пособия	Устная речь, учебники, учебные пособия	владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) способность работать с информацией в глобальных компьютерных сетях (ОК-4)
Тема 6. Программно-аппаратные методы защиты от удаленных атак в сети Интернет.	Программно-аппаратные средства обеспечения информационной безопасности. Методика Firewall как основное программно-аппаратное средство осуществления сетевой политики безопасности в выделенном сегменте IP-сети. Программные методы защиты, применяемые в сети Internet.	по источнику знаний: чтение, конспектирование по назначению: приобретение знаний, анализ, закрепление, проверка знаний по типу познавательной деятельности: объяснительно-иллюстративный, репродуктивный	Учебники, учебные пособия	Устная речь, учебники, учебные пособия, раздаточный материал	владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) способность работать с информацией в глобальных компьютерных сетях (ОК-4)
Тема 7. Защита персональных данных в сети Интернет	Понятие персональных данных. Субъект, объект персональных данных. Общедоступные источники персо-	по источнику знаний: чтение, конспектирование по назначению: приобретение знаний, анализ, за-	Учебники, учебные пособия	Устная речь, учебники, учебные пособия	владение основными методами, способами и средствами получения, хранения, переработки

	нальных данных. Незаконное распространение персональных данных в сети Интернет. Особенность распространения персональных данных в сети Интернет за пределами РФ.	крепление, проверка знаний по типу познавательной деятельности: объяснительно-иллюстративный, репродуктивный			информации, навыками работы с компьютером как средством управления информацией (ОК-3) способность работать с информацией в глобальных компьютерных сетях (ОК-4)
Тема 8. Рынок систем безопасности	Основные тенденции рынка систем безопасности: статистика и прогнозы. Структура рынка систем безопасности. Лидеры на рынке систем безопасности.	по источнику знаний: чтение, конспектирование по назначению: приобретение знаний, анализ, закрепление, проверка знаний по типу познавательной деятельности: объяснительно-иллюстративный, репродуктивный	Учебники, учебные пособия	Устная речь, учебники, учебные пособия	владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) способность работать с информацией в глобальных компьютерных сетях (ОК-4)
Тема 9. Информационная война.	Технологии информационного противоборства в сети Интернет. Информационная война и ее виды. Информационное оружие и его классификация. Выявление признаков информационной войны в сети Интернет.	по источнику знаний: чтение, конспектирование по назначению: приобретение знаний, анализ, закрепление, проверка знаний по типу познавательной деятельности: объяснительно-иллюстративный, репродуктивный	Учебники, учебные пособия	Устная речь, учебники, учебные пособия	владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) способность работать с информацией в глобальных компьютерных сетях (ОК-4)

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, позволяют:

- организовать процесс образования путем визуализации изучаемой информации посредством использования презентаций, учебных фильмов;
- контролировать результаты обучения на основе компьютерного тестирования;
- автоматизировать расчеты аналитических показателей, предусмотренные программой научно-исследовательской работы;
- автоматизировать поиск информации посредством использования справочных систем.

10.1. Перечень необходимого программного обеспечения

Для осуществления учебного процесса используется свободно распространяемое (бесплатное не требующее лицензирования) программное обеспечение и лицензионное программное обеспечение компаний Microsoft и Kaspersky:

1. Операционная система на базе Linux;
2. Тестовая система собственной разработки, правообладатель ФГБОУ ВО «МГТУ», свидетельство №2013617338.
3. Операционная система Windows7 Профессиональная, MicrosoftCorp., № 00371-838-5849405-85257, 23.01.2012, бессрочный.
4. Текстовый процессор Microsoft Office Word 2010. Номер продукта 14.0.6024.1000 SP1 MSO (14.0.6024.1000) 02260-018-0000106-48095.
5. Антивирусные программы: Kaspersky Anti-virus 6/0 – № лицензии 26FE-000451-5729CF81, срок лицензии 07.02.2020.
6. Cisco Packet Tracer – симулятор сети передачи данных. Производитель: CISCO Systems.
7. **Wireshark** – sniffер, предназначенный для анализа трафика компьютерных сетей (Ethernet, FDDI, PPP, Token-Ring и других) в режиме реального времени, используя широковещательный режим сетевой карты. Свободно распространяемое ПО.

10.2. Перечень необходимых информационных справочных систем и профессиональных баз данных:

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронно-библиотечным системам:

1. Электронная библиотечная система IPRbooks ([http:// www.iprbookshop.ru](http://www.iprbookshop.ru))
2. Электронная библиотечная система «ZNANIUM.COM» (www.znanium.com).

Для обучающихся обеспечен доступ (удаленный доступ) к следующим современным профессиональным базам данных, информационным справочным и поисковым системам:

1. Консультант Плюс – справочная правовая система (<http://consultant.ru>)
2. Web of Science (WoS) (<http://apps.webofknowledge.com>)
3. Научная электронная библиотека (НЭБ) (<http://www.elibrary.ru>)
4. Электронная Библиотека Диссертаций (<https://dvs.rsl.ru>)
5. КиберЛенинка (<http://cyberleninka.ru>)
6. Национальная электронная библиотека (<http://нэб.рф>)

11. Описание материально-технической базы необходимой для осуществления образовательного процесса по дисциплине (модулю)

Наименования специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Специальные помещения		
Лекционные аудитории: 3-6, 3-12,3-18, 3-19 Аудитории для занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации: 3-1, 3-2, 3-13, 3-15,3-17, 3-20, 3-22	LCD экран. компьютер, мультимедиа проектор.	Операционная система Windows7 Профессиональная, Приложение 4 MicrosoftCorp., № 00371-838-5849405-85257, 23.01.2012, бессрочный. Текстовый процессор Microsoft Office Word 2010. Номер продукта 14.0.6024.1000 SP1 MSO (14.0.6024.1000) 02260-018-0000106-48095. Антивирусные программы: Kaspersky Anti-virus 6/0 – № лицензии 26FE-000451-5729CF81, срок лицензии 07.02.2020. Cisco Packet Tracer – симулятор сети передачи данных. Производитель: CISCO Systems. Wireshark – сниффер, предназначенный для анализа трафика компьютерных сетей (Ethernet, FDDI, PPP, Token-Ring и других) в режиме реального времени, используя широкополосный режим сетевой карты. Свободно распространяемое ПО.
Помещения для самостоятельной работы		
Читальный зал ФГБОУ ВО «МГТУ»: ул. Первомайская, 191, 3 этаж.	Читальный зал имеет 150 посадочных мест, компьютерное оснащение с выходом в Интернет на 30 посадочных мест; оснащен специализированной мебелью (столы, стулья, шкафы, шкафы выставочные), стационарное мультимедийное оборудование, оргтехника (принтеры, сканеры, ксероксы)	Операционная система Windows7 Профессиональная, MicrosoftCorp., № 00371-838-5849405-85257, 23.01.2012, бессрочный. Текстовый процессор Microsoft Office Word 2010. Номер ³⁰продукта 14.0.6024.1000 SP1 MSO (14.0.6024.1000) 02260-018-0000106-48095. Антивирусные программы: Kaspersky Anti-virus 6/0 – № лицензии 26FE-000451-5729CF81, срок лицензии 07.02.2020.

Дополнения и изменения в рабочей программе
за _____/_____ учебный год

В рабочую программу Б1.Б.28 Информационная безопасность в глобальной сети
(наименование дисциплины)

для направления (специальности) 40.03.01 Юриспруденция
(номер направления (специальности))

вносятся следующие дополнения и изменения:

Дополнения и изменения внес _____
(должность, Ф.И.О., подпись)

Рабочая программа пересмотрена и одобрена на заседании кафедры _____
(наименование кафедры)

« ____ » _____ 20 __ г.

31

Заведующий кафедрой _____
(подпись) (Ф.И.О.)