Приложение 7. ОП ВО

Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

ФАКУЛЬТЕТ ФИНАНСОВ И БАНКОВСКОГО ДЕЛА
(наименование структурного подразделения (института/факультета/филиала)
Кафедра экономической теории и политики
(наименование кафедры)

УТВЕРЖДЕНА

Кафедрой экономической теории и политики

Факультета финансов и банковского дела

Протокол от «04» сентября 2019 г.

№5

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.16 «Корпоративная и финансовая кибербезопасность»

(индекс, наименование дисциплины , в соответствии с учебным планом)

38.04.01 Экономика

(код, наименование направления подготовки (специальности)

"Финансовая дипломатия"

(направленность(и) (профиль (и)/специализация(ии)

Магистр

(квалификация)

Очная/очно-заочная/заочная

(форма(ы) обучения)

Год набора: 2020

Москва, 2019 г.

Автор–составитель:
к.э.н., доцент Соляр А.В., доцент кафедры «Фондовые рынки и финансовый инжиниринг»

Заведующий кафедрой
экономической теории и политики д.э.н., проф., академик РАН Аганбегян А.Г.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине , соотнесенных с планируемыми результатами освоения программы....4
2. Объем и место дисциплины в структуре ОП ВО....9
3. Содержание и структура дисциплины....9
4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине....13
5. Методические указания для обучающихся по освоению дисциплины....19
6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине....21
6.1. Основная литература....21
6.2. Дополнительная литература....21
6.3. Учебно-методическое обеспечение самостоятельной работы....21
6.4. Нормативные правовые документы....21
6.5. Интернет-ресурсы....21
6.6. Иные источники....21
7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы....24

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

1.1 Дисциплина Б1.В.16 «Корпоративная и финансовая кибербезопасность» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-3	Способность проводить самостоятельные исследования в соответствии с разработанной программой	ПК-3.3.1	Способность оценивать и анализировать национальные и международные стандарты кибербезопасности, применяя современные информационные технологии.
ДПК-5	Способность комплексно оценивать эволюцию и современное состояние мировой системы, рассматривать актуальные международно-политические ситуации в контексте более широких тенденций и процессов, и на этой основе формулировать стратегически-ориентированные рекомендации, владеть основами многосторонней и интеграционной дипломатии, понимать логику становления и развития региональных межгосударственных связей и уметь использовать дипломатические возможности для решения региональных проблем, налаживания социально-экономических связей.	ДПК-5.3.1.	Способность рассматривать актуальные международно-политические ситуации в международных организациях, использовать возможности современной кибербезопасности и полученные результаты отражать в исследовательской работе и преддипломной практике при помощи информационных технологий.

1.2**.** В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ (при наличии профстандарта)	Код этапа освоения компетенции	Результаты обучения
ПС «Специалист по финансовому мониторингу (в сфере противодействия легализации доходов, полученных преступным путем, и финансированию терроризма)» ОТФ Проведение финансовых расследований в целях ПОД/ФТ в организации (В) (ч.); ТФ В/03.7 Подготовка аналитических материалов для принятия мер по линии ПОД/ФТ в организации ТФ В/04.07 Подготовка предложений по совершенствованию законодательства в сфере ПОД/ФТ в организации	ДПК-1.1.1 ДПК-5.4.1.	**На уровне знаний:** **Знать:** 1. Законодательство Российской Федерации, международные акты и стандарты, регулирующие отношения в сфере ПОД/ФТ 2. Методы финансового анализа 3. Источники информации для финансового анализа 4. Перечень предикатных преступлений в отношении ОД/ФТ 4. Типологии отмывания денег 5. Требования к оформлению документов 6. Специализированные программные продукты, используемые в профессиональной деятельности. 7. Функциональные возможности специального программного обеспечения, используемого в целях анализа информации 8. Принципы построения и использования баз данных 9. Требования к апробации новых алгоритмов
		На уровне умений: **Уметь:** 1. Обобщать, интерпретировать и систематизировать информацию 2. Анализировать и оценивать информацию 3. Формулировать выводы 4. Выявлять причинно-следственные связи 5. Прогнозировать развитие событий 6. Использовать специализированные программные продукты 7. Подготавливать аналитические материалы 8. Определять важность информации 9. Определять целевые группы и характер рекомендаций для каждой группы 10. Разрабатывать рекомендации, методические материалы по направлению деятельности подразделения 11. Организовывать взаимодействие заинтересованных сторон.
		На уровне навыков: **Владеть навыками:** 1. Финансовый анализ информации об операциях (сделках) в совокупности с внешними

		информационными ресурсами с целью выявления типовых схем отмывания преступных доходов, действующих в различных регионах, отраслях и секторах экономики в целях ПОД/ФТ 2. Мониторинг деятельности организаций, отдельных сегментов финансового рынка с целью выявления объектов, направлений и форм проявления повышенного риска для принятия мер по линии ПОД/ФТ 3. Подготовка экспертно-оценочных материалов, содержащих информацию об участниках финансовых операций (сделок), признаках подозрительности и вопросах, подлежащих выяснению в ходе проведения проверок и финансовых расследований в целях ПОД/ФТ 4. Формулирование выводов и рекомендаций по результатам проведенного анализа для принятия мер по линии ПОД/ФТ 5. Методическое обеспечение работ по выявлению новых типологических проявлений в противоправной деятельности участников финансовых операций (сделок) 6. Сбор, обобщение и закрепление ранее выявленных типологий подозрительной деятельности в целях ПОД/ФТ 7. Ведение базы данных типологий подозрительной деятельности в целях ПОД/ФТ 8. Доведение аналитических материалов до заинтересованных структурных подразделений организации 9. Выявление и систематизация в целях ПОД/ФТ пробелов действующего законодательства и практики его применения, вследствие которых возможно функционирование типовых схем подозрительной деятельности 10. Классификация выявленных пробелов законодательства и практики его применения в целях ПОД/ФТ 11. Разработка предложений по устранению пробелов в законодательстве в целях ПОД/ФТ 12. Организация обсуждения разработанных предложений по устранению пробелов в законодательстве в целях ПОД/ФТ в профессиональном сообществе 13. Доработка предложений по устранению пробелов в законодательстве в целях ПОД/ФТ по результатам обсуждения 14. Оформление и представление в установленном порядке предложений по устранению пробелов в законодательстве в целях ПОД/ФТ

ОТФ Организация финансового мониторинга в целях ПОД/ФТ в организации (С) Организация разработки правил внутреннего контроля в целях ПОД/ФТ в организации ТФ С/01.8 Организация контроля реализации работниками организации правил внутреннего контроля в целях ПОД/ФТ ТФ С/04.8		**На уровне знаний:** **Знать:** 1. Законодательство Российской Федерации, нормативные правовые акты, международные акты и стандарты, регулирующие отношения в сфере ПОД/ФТ 2. Методы стратегического управления и планирования 3. Компетенции уполномоченного органа в сфере ПОД/ФТ 4. Виды деятельности и отчетность работника, ответственного за ПОД/ФТ 5. Цели и структура сектора финансовых услуг 6. Основные виды финансовых услуг и продуктов в профильном секторе, их функции и назначение 7. Услуги и продукты, которые предоставляет организация 8. Методы и формы контроля деятельности работников
		На уровне умений: **Уметь:** 1. Осуществлять планирование деятельности в рамках выполняемых задач 2. Организовывать и координировать работу работников, находящихся в подчинении, для решения поставленных задач 3. Оценивать и контролировать деятельность работников, находящихся в подчинении 4. Планировать перспективную потребность в кадрах 5. Разрабатывать предложения по организации и проведению обучения и профессиональной подготовки работников 6. Применять законодательство в сфере ПОД/ФТ, нормативные правовые акты и правила внутреннего контроля 7. Разрабатывать документы, рекомендации, методические материалы по направлению деятельности подразделения 8. Подготавливать отчетные материалы по установленной форме 9. Разрабатывать должностные обязанности работника (работников), отвечающего за недопущение ОД/ФТ и предоставление отчетности по ПОД/ФТ 10. Позиционировать деятельность в целях ПОД/ФТ в качестве приоритетного направления работы 11. Формулировать задачи и контролировать их исполнение
		На уровне навыков:

		Владеть навыками: 1. Определение нормативных правовых актов и нормативных документов в сфере ПОД/ФТ для разработки правил внутреннего контроля в целях ПОД/ФТ в организации 2. Определение области применения правил внутреннего контроля в целях ПОД/ФТ в организации 3. Определение порядка взаимодействия с уполномоченным органом, принимающим меры по ПОД/ФТ 4. Определение порядка обеспечения конфиденциальности клиентской информации при направлении сообщений, касающихся ОД/ФТ 5. Определение ответственности и отчетности работников организации в вопросах недопущения (предотвращения) ОД/ФТ 6. Определение процедуры оценки рисков ОД/ФТ и реализации мер по надлежащей оценке клиента ("знай своего клиента") при установлении деловых отношений с клиентами 7. Определение методов и мер по контролю и оценке эффективности реализации правил внутреннего контроля в целях ПОД/ФТ 8. Определение мер реагирования организации на несоблюдение правил внутреннего контроля в целях ПОД/ФТ 9. Утверждение графика (сроков) разработки программ внутреннего контроля в целях ПОД/ФТ 10. Руководство разработкой программ внутреннего контроля в целях ПОД/ФТ 11. Определение функций и обязанностей подразделений и работников организации по обеспечению выполнения правил внутреннего контроля в целях ПОД/ФТ 12. Организация разработки и актуализации правил внутреннего контроля в целях ПОД/ФТ 13. Представление на утверждение руководству организации правил внутреннего контроля в целях ПОД/ФТ 14. Организация мероприятий по устранению выявленных нарушений в целях ПОД/ФТ в организации 15. Контроль мероприятий по устранению выявленных нарушений в целях ПОД/ФТ в организации

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Дисциплина Б1.В.16 «Корпоративная и финансовая кибербезопасность» составляет 2 зачетные единицы, т.е. 72 академических часа.

Для студентов очной и очно-заочной формы обучения на контактную работу с преподавателем выделено 20 часов, из них 8 часов лекций и 12 часов практических занятий, на самостоятельную работу обучающихся выделено 52 часа. Для студентов заочной формы обучения на контактную работу с преподавателем выделено 12 часов, из них 4 часа лекций и 8 часов практических занятий, на самостоятельную работу обучающихся выделено 58 часов.

Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.16 «Корпоративная и финансовая кибербезопасность» изучается на 2 курсе, в 4 семестре студентами очной и очно-заочной формы обучения; студентами заочной формы обучения изучается на 2 курсе.

Дисциплина Б1.В.16 «Корпоративная и финансовая кибербезопасность» реализуется после базового курса «Мировая экономика», полученного студентами в рамках бакалавриата.

Форма промежуточной аттестации в соответствии с учебным планом: зачет в устной форме.

3. Содержание и структура дисциплины

Очная форма обучения

№ п/п	Наименование тем (разделов)	Объем дисциплины , час.						Форма текущего контроля успеваемости**, промежуточной аттестации***
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Раздел 1.	Вычислительные концепции и проблемы безопасности	18	2		2		14	*Т*
Раздел 2.	Криптография	10	2		2		6	*Т*
Раздел 3.	Сеть	18	2		2		14	*Т*

№ п/п	Наименование тем (разделов)	Объем дисциплины , час.						Форма текущего контроля успеваемости**, промежуточной аттестации***
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Раздел 4.	Системное администрирование	10	2		2		6	*Т*
Раздел 5.	Обнаружение и предотвращение	8			2		6	*Т*
Раздел 6.	Вредоносное ПО и криминалистическая экспертиза завершены	8			2		6	*Т*
Промежуточная аттестация								*За*
Всего по курсу:		**72**	**8**		**12**		**52**	

Очно-заочная форма обучения

№ п/п	Наименование тем (разделов)	Объем дисциплины , час.						Форма текущего контроля успеваемости**, промежуточной аттестации***
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Раздел 1.	Вычислительные концепции и проблемы безопасности	18	2		2		14	*Т*
Раздел 2.	Криптография	10	2		2		6	*Т*
Раздел 3.	Сеть	18	2		2		14	*Т*
Раздел 4.	Системное администрирование	10	2		2		6	*Т*
Раздел 5.	Обнаружение и предотвращение	8			2		6	*Т*
Раздел 6.	Вредоносное ПО и криминалистическая экспертиза завершены	8			2		6	*Т*
Промежуточная аттестация								*За*
Всего по курсу:		**72**	**8**		**12**		**52**	

Заочная форма обучения

№ п/п	Наименование тем (разделов)	Объем дисциплины , час.						Форма текущего контроля успеваемости**, промежуточной аттестации***
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Раздел 1.	Вычислительные концепции и проблемы безопасности	16	2				14	*Т*
Раздел 2.	Криптография	8	2				6	*Т*
Раздел 3.	Сеть	16			2		14	*Т*
Раздел 4.	Системное администрирование	8			2		6	*Т*
Раздел 5.	Обнаружение и предотвращение	12			2		10	*Т*
Раздел 6.	Вредоносное ПО и криминалистическая экспертиза завершены	10			2		8	*Т*
Промежуточная аттестация		2						*За*
Всего по курсу:		**72**	**4**		**8**		**58**	

Примечание:
*** –формы текущего контроля успеваемости: тестирование (Т).*
**** формы промежуточной аттестации: зачет (За).*

Содержание дисциплины

Раздел 1. Вычислительные концепции и проблемы безопасности

Определение кибербезопасности и обязанностей специалистов по кибербезопасности. Определение типов хакеров и их мотивов. Объяснение как выявляются и устраняются уязвимости. Утечки данных. Модель CIA. Модель AAA: аутентификация. Модель AAA: авторизация. Модель AAA: бухгалтерский учет. Баланс между безопасностью и доступностью. Безопасность и удобство. Агенты угрозы.

Раздел 2. Криптография

Введение в криптографию. Принцип Керкхоффса. Описание процесса шифрования. Типы шифрования. Алгоритм хеширования и защита данных. Демонстрация хеширования. Центр сертификации сайтов. Демонстрация веб-сайта и хеширование.

Раздел 3. Сеть

Введение в сеть. Описание процесса как информация попадает в Интернет. MAC и IP-адреса. Маски подсети. Местная связь. Удаленная связь. Маршрутизация пакета. Описание процесса как MAC- и IP-адреса используются вместе. Привязка IP-адресов к MAC-адресам. Обучение парсингу IP и MAC-адресов. Порты. TCP и UDP. Принципы работы переключателей портов. Описание процесса перемещения данных в сети или автономной системе. Автономные системы. Динамическая маршрутизация.

Раздел 4. Системное администрирование

Принципы работы ключевых сетевых служб, которые подпадают под домен системного администратора. Статическая адресация. RARP. BOOTP. DHCP. DORA DHCP. DNS. Процесс DNS.

Раздел 5. Обнаружение и предотвращение

Принципы работы различных типов межсетевых экранов и примеры их работы. Межсетевые экраны. Методы брандмауэра. Принципы работы систем защищающие сети от внутренних угроз. Системы обнаружения вторжений и системы предотвращения вторжений. Программы для приманок и обмана. Социальная инженерия. Риски атак социальной инженерии.

Раздел 6. Вредоносное ПО и криминалистическая экспертиза завершены

Определение различных категорий вредоносного ПО. Вирус. Червь. Логическая бомба, троянский конь и RAT. Определение различных типов атак социальной инженерии. Руткит, бэкдор, шпионское ПО, рекламное ПО и ПНП. Фишинг, Спеарфишинг, Фарминг, Watering Hole. Программы-вымогатели. Понятие цифровой криминалистики. Доказательства совершения преступлений в цифровой среде. Основные три этапа судебно-медицинских расследований цифровых преступлений согласно мировой практике.

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Текущий контроль успеваемости

4.1.1. Формы текущего контроля успеваемости

№ п/п	Тема (раздел)	Методы текущего контроля успеваемости
1.	Вычислительные концепции и проблемы безопасности	тест
2.	Криптография	тест
3.	Сеть	тест
4.	Системное администрирование	тест
5.	Обнаружение и предотвращение	тест
6.	Вредоносное ПО и криминалистическая экспертиза завершены	тест

4.1.2. Материалы текущего контроля успеваемости обучающихся

Типовые оценочные материалы по теме 1. «Вычислительные концепции и проблемы безопасности»

Пример тестового задания

Для чего предназначены тесты на проникновение?

- Исправить уязвимости
- Выявить только уязвимости
- Выявление и использование уязвимостей
- Используйте только уязвимости

Что всегда будет самым слабым звеном любой системы кибербезопасности?

- Брандмауэры
- Вредоносное ПО
- Люди
- Шифрование

Типовые оценочные материалы по теме 2. «Криптография»

Пример тестового задания

Текстовое сообщение вместе с ключом вводятся в алгоритм для получения на выходе _____.

Типовые оценочные материалы по теме 3. «Сеть»

Пример тестового задания.

Верно или неверно: когда ваш веб-браузер переходит на веб-сайт, исходный порт, который использует ваш браузер, равен 80.

- Правда
- Ложь

Типовые оценочные материалы по теме 4. «Системное администрирование»

Пример тестового задания.

Какой из следующих протоколов не занимается назначением IP-адресов устройствам?

- RARP
- BOOTP
- ARP
- DHCP

Типовые оценочные материалы по теме 5. «Обнаружение и предотвращение»

Пример тестового задания

Какое из этих утверждений верно?

- Одна сторона межсетевого экрана подключена к доверенному внутреннему устройству.
- К доверенному внутреннему устройству подключены две стороны межсетевого экрана.
- Две стороны межсетевого экрана подключены к ненадежной стороне.

Типовые оценочные материалы по теме 6. «Вредоносное ПО и криминалистическая экспертиза завершены»

Пример тестового задания.

Что из следующего является верным (выберите все подходящие варианты)?

- Вирусы могут воспроизводиться сами по себе в сетях.
- Черви могут самостоятельно размножаться в сетях.
- Вирусы могут копироваться в другие файлы на том же компьютере.
- Черви не могут самостоятельно размножаться в сетях.

4.2. Промежуточная аттестация

4.2.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Показатели и критерии оценивания компетенций с учетом этапа их формирования

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-3	Способность проводить самостоятельные исследования в соответствии с разработанной программой	ПК-3.3.1	Способность оценивать и анализировать национальные и международные стандарты кибербезопасности, применяя современные информационные технологии.
ДПК-5	Способность комплексно оценивать эволюцию и современное состояние мировой системы, рассматривать актуальные международно-политические ситуации в контексте более широких тенденций и процессов, и на этой основе формулировать стратегически-ориентированные рекомендации, владеть основами многосторонней и интеграционной дипломатии, понимать логику становления и развития региональных межгосударственных связей и уметь использовать дипломатические возможности для решения региональных проблем, налаживания социально-экономических связей.	ДПК-5.3.1.	Способность рассматривать актуальные международно-политические ситуации в международных организациях, использовать возможности современной кибербезопасности и полученные результаты отражать в исследовательской работе и преддипломной практике при помощи информационных технологий.

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
ПК-3.3.1 Способность оценивать и анализировать национальные и международные стандарты кибербезопасности, применяя современные информационные технологии.	Способность оценивать и анализировать национальные и международные стандарты кибербезопасности, способен исследовать существующие уязвимости.	Оценивает и анализирует национальные и международные стандарты кибербезопасности, способен исследовать существующие уязвимости.
ДПК-5.3.1 Способность рассматривать актуальные международно-политические ситуации в международных организациях, использовать возможности современной кибербезопасности и полученные результаты отражать в исследовательской работе и преддипломной практике при помощи информационных технологий.	Способность на основе кибербезопасности, осуществлять электронную дипломатию, внешнюю политику и бизнес-дипломатию.	Демонстрирует способность на основе кибербезопасности, осуществлять электронную дипломатию, внешнюю политику и бизнес-дипломатию.

4.2.2. Форма и средства (методы) проведения промежуточной аттестации

Зачет проводится с применением следующих методов (средств): устного опроса.

4.2.3 Типовые оценочные средства

Список вопросов для подготовки к зачету:

1. Определение кибербезопасности и обязанностей специалистов по кибербезопасности.
2. Определение типов хакеров и их мотивов. Объяснение как выявляются и

устраняются уязвимости.

3. Утечки данных.
4. Модель CIA.
5. Модель AAA: аутентификация.
6. Модель AAA: авторизация.
7. Модель AAA: учет.
8. Баланс между безопасностью и доступностью.
9. Безопасность и удобство.
10. Агенты угрозы.
11. Введение в криптографию.
12. Принцип Керкхоффса.
13. Описание процесса шифрования.
14. Типы шифрования.
15. Алгоритм хеширования и защита данных.
16. Демонстрация хеширования.
17. Центр сертификации сайтов.
18. Демонстрация веб-сайта и хеширование.
19. Описание процесса как информация попадает в Интернет.
20. MAC и IP-адреса.
21. Маски подсети.
22. Местная связь.
23. Удаленная связь.
24. Маршрутизация пакета.
25. Описание процесса как MAC- и IP-адреса используются вместе.
26. Привязка IP-адресов к MAC-адресам.
27. Обучение парсингу IP и MAC-адресов.
28. Порты. TCP и UDP.
29. Принципы работы переключателей портов.
30. Описание процесса перемещения данных в сети или автономной системе.
31. Автономные системы.
32. Динамическая маршрутизация.
33. Принципы работы ключевых сетевых служб, которые подпадают под домен системного администратора.
34. Статическая адресация.
35. RARP.

36. BOOTP.
37. DORA DHCP.
38. Процесс DNS.
39. Принципы работы различных типов межсетевых экранов и примеры их работы.
40. Межсетевые экраны.
41. Методы брандмауэра.
42. Принципы работы систем защищающие сети от внутренних угроз.
43. Системы обнаружения вторжений и системы предотвращения вторжений.
44. Программы для приманок и обмана.
45. Социальная инженерия.
46. Риски атак социальной инженерии.
47. Определение различных категорий вредоносного ПО.
48. Вирус.
49. Червь.
50. Логическая бомба.
51. Троянский конь
52. RAT.
53. Определение различных типов атак социальной инженерии.
54. Руткит.
55. Бэкдор.
56. Шпионское ПО.
57. Рекламное ПО и ПНП.
58. Фишинг.
59. Спеарфишинг.
60. Фарминг.
61. Watering Hole.
62. Программы-вымогатели.
63. Понятие цифровой криминалистики. Д
64. Доказательства совершения преступлений в цифровой среде.
65. Основные три этапа судебно-медицинских расследований цифровых преступлений согласно мировой практике

4.3. Методические материалы

Процедура проведения зачета

Промежуточная аттестация определяет степень достижения учебных целей и проводится в форме зачета. Зачёт проводится устно по контрольным вопросам в сроки,

предусмотренные учебным планом. При выведении аттестационной отметки обязательно учитываются результаты текущего контроля и самостоятельной работы обучающегося. Текущий контроль успеваемости осуществляется во время проведения семинаров посредством проведения устных опросов учащихся. Содержание оценочного средства- вопросы к зачету. Требования к выполнению- зачет проводится в устной форме путем ответа на вопросы из представленного перечня. Время, отведенное на процедуру – 20 минут. Результаты оглашаются по окончании опроса. Ответ подготавливается в письменной конспективной форме и сдается преподавателю после устного ответа.

Шкала оценивания

Зачет:	Обучающийся оценивает и анализирует национальные и международные стандарты кибербезопасности, способен исследовать существующие уязвимости. Сдал все промежуточные тесты.
Незачет:	Обучающийся не оценивает и анализирует национальные и международные стандарты кибербезопасности, не способен исследовать существующие уязвимости. Не сдал часть промежуточных тестов.

5. Методические указания для обучающихся по освоению дисциплины

Методические рекомендации студентам по изучению дисциплины

Самостоятельная работа – крайне важный элемент подготовки студентов в процессе обучения. Получить всесторонние знания, ограничиваясь при этом только прослушиванием лекций и посещением семинарских занятий, невозможно.

Кроме того, понятийный аппарат курса разнообразен, объемен, что требует специальной работы для их усвоения.

Важным условием успешной самостоятельной работы студентов являются консультации преподавателя и тщательная подготовка к практическим занятиям.

Цель самостоятельной работы студента по изучению учебного материала – формирование навыков самостоятельного отбора и изучения рекомендованных преподавателями кафедры учебной литературы, нормативных актов, материалов периодических изданий, их анализа и осмысления. В результате этой работы студенты должны научиться понимать логику научного исследования, критически анализировать существующие в научной литературе точки зрения и на этой основе формировать собственную позицию по рассматриваемому вопросу.

Самоподготовка к практическим занятиям

При подготовке к практическому занятию необходимо помнить, что та или иная дисциплина тесно связана с ранее изучаемыми курсами. Более того, именно синтез

полученных ранее знаний и текущего материала по курсу делает подготовку результативной и всесторонней.

На семинарских занятиях студент должен уметь последовательно излагать свои мысли и аргументированно их отстаивать.

Для достижения этой цели необходимо:

1) ознакомиться с соответствующей темой программы дисциплины;

2) осмыслить круг изучаемых вопросов и логику их рассмотрения;

3) изучить рекомендованную литературу по данной теме;

4) тщательно изучить лекционный материал;

5) ознакомиться с вопросами очередного семинарского занятия;

6) подготовить краткое выступление по каждому из вынесенных на семинарское занятие вопросу.

Изучение вопросов очередной темы требует глубокого усвоения теоретических основ дисциплины, раскрытия сущности основных экономических категорий, проблемных аспектов темы и анализа фактического материала.

При презентации материала на семинарском занятии можно воспользоваться следующим алгоритмом изложения темы: определение и характеристика основных категорий, эволюция предмета исследования, оценка его современного состояния, существующие проблемы, перспективы развития.

Тестовые задания

Решение тестовых заданий проводится в течение изучения дисциплины.

Преподаватель должен определить студентам исходные данные для подготовки к тестированию: назвать разделы (темы, вопросы), по которым будут задания в тестовой форме, нормативные акты и теоретические источники для подготовки.

Каждому студенту отводится на тестирование время, соответствующее количеству тестовых заданий. До окончания теста студент может еще раз просмотреть все свои ответы на задания и при необходимости внести коррективы.

При прохождении тестирования пользоваться конспектами лекций, учебниками, и иными материалами не разрешено.

Методические рекомендации по подготовке к промежуточной аттестации

При подготовке к промежуточной аттестации ознакомьтесь со списком представленных вопросов. Формулируйте ответ с точки зрения применения различных методов анализа данных. Необходимо дать аргументированный ответ, подтверждающий уровень освоения компетенции.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

6.1. Основная литература

1. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. — Москва, Вологда : Инфра-Инженерия, 2020. — 692 с. — ISBN 978-5-9729-0486-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/98349.html

6.2. Дополнительная литература

1. Овчинский, В. С. Криминология цифрового мира: учебник для магистратуры / В. С. Овчинский. - Москва : Норма : ИНФРА-М, 2020. -352 с. - ISBN 978-5-91768-896-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1059377

6.3. Учебно-методическое обеспечение самостоятельной работы

Не предусмотрено.

6.4. Нормативные правовые документы.

Не предусмотрено.

6.5. Интернет-ресурсы.

https://www.securitylab.ru

6.6. Иные источники.

1.World's Biggest Data Breaches, Information is Beautiful

2.11 Steps Attackers Took to Crack Target, CIO.com

3.Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid, Wired

4.2017 Cyber Risks to Intensify as Hackers Become More Cunning: Report, Energi

5.The Security Mindset, Schneier on Security

6.Cybersecurity unemployment rate at zero, SC Media

7.Network live IP video cameras directory, Insecam.org

8.Hackers Remotely Kill a Jeep on the Highway—With Me in It, Andy Greenberg, Wired

9.With 'recall,' Fiat Chrysler makes its car hack worse, Colin Neagle, Network World

10. Florida man wins over 1 million miles for hacking United Airlines, Jack Corrigan, WGN TV

11. Computer hackers can now hijack toilets, Sarah Griffiths, Daily Mail
12. Baby monitor hacker delivers creepy message to child, CBS News
13. It's Insanely Easy to Hack Hospital Equipment, Kim Zeller, Wired
14. It's Way Too Easy to Hack the Hospital, Monte Reel and Jordan Robertson, Bloomberg
15. Here's What We Know About the Massive Cyber Attack That Took Down the Internet on Friday, Peter Dockrill, Science Alert
16. How the Dyn DDoS attack unfolded, Tim Greene, Network World
17. MEECES to pieces, Deborah Radcliff, Network World
18. 'Bob' outsources tech job to China; watches cat videos at work, Jaikumar Vijayan, Computerworld
19. 10 Reasons Why Biometrics Won't Replace Passwords Anytime Soon, Tom, Dashlane
20. NIST declares the age of SMS-based 2-factor authentication over, Devin Coldewey, TC's Crunchboard
21. NIST Denounces SMS 2FA - What are the Alternatives?, Kevin Townsend, Security Week
22. Standards body warned SMS 2FA is insecure and nobody listened, Darren Pauli, The Register
23. Microsoft Security Bulletin MS08-067 – Critical: Vulnerability in Server Service Could Allow Remote Code Execution (958644), Microsoft
24. The Inside Story Behind MS08-067, John Lambert, Microsoft
25. Squirrels outrank hackers as threat to U.S. electrical grid, Martin Anderson, The Stack
26. Grid Confronts a Threat from Mother Nature, Matthew L. Wald, The New York Times
27. Power grid cyber security 'in chaos' | State ponders ways to guard against attacks by humans as well as Mother Nature, Hartford Business Journal
28. Heartbleed Explanation, xkcd
29. Heartbleed, xkcd
30. What should you do about "HeartBleed?," LegacyTalk
31. Who your browser trusts, and how to control it., CertSimple
32. Types and Sizes of Networks
33. Backgrounder: Data Representation and the Mathematics of Computing
34. OSI Reference Model Layer Mnemonics
35. OSI Reference Model Layer Summary
36. TCP/IP Protocol Suite and Architecture
37. Private Addressing
38. Subnetting

39. NAT
40. IPv6
41. Cisco IOS Switching Services Configuration Guide, Routing Between VLANs Overview
42. AlliedWare Plus™ OS, Overview of VLANs (Virtual LANs)
43. Firewll.cx, The VLAN Concept - Introduction to VLANs
44. Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide, Release 4.1.x, Chapter 6, Configuring STP and RSTP
45. Cisco, Understanding Rapid Spanning Tree Protocol (802.1w)
46. THE TCP/IP GUIDE: TCP/IP DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)
47. DHCP Overview, Motivation, History and Standards
48. DHCP Address Assignment and Dynamic Address Allocation and Management
49. DHCP Configuration and Operation
50. DHCP Messaging, Message Types and Formats
51. DHCP Client/Server Implementation, Features and Issues
52. DHCP For IP Version 6 (DHCPv6)
53. THE TCP/IP GUIDE: DNS
54. DNS Overview, Functions and Characteristics
55. DNS Name Space, Architecture and Terminology
56. DNS Name Registration, Public Administration, Zones and Authorities
57. DNS Name Servers and Name Resolution
58. DNS Changes To Support IP Version 6
59. Why There Are Only 13 DNS Root Name Servers, Bradley Mitchell, Lifewire
60. Why 13 DNS root servers?, Miek Gieben
61. Hosts file hijacks, Pieter Arntz, Malwarebytes
62. 6 Surprising Uses for the Windows Hosts File, Chris Hoffman, MakeUseOf
63. how to make the internet not suck (as much), Dan Pollock, someonewhocares.org
64. The Hosts File and what it can do for you, Lawrence Abrams, BleepingComputer
65. What are these 127.0.0.1 entries in my system hosts file?, Leo A. Notenboom, Ask Leo!
66. How to effectively prevent Malware by using a HOSTS file, Shanmuga, Malware Help
67. Google Public DNS: Get Started, Google Developers Guide
68. How to Switch to OpenDNS or Google DNS to Speed Up Web Browsing, Taylor Gibb, How-To Geek
69. Google DNS: 8.8.8.8 and 8.8.4.4. Benefits and how to use, Tunecomp
70. Understanding Social Engineering Attacks, Wordfence

71. Top 5 Social Engineering Exploit Techniques, Jamey Heary, PCWorld
72. Phone scammers call the wrong guy, get mad and trash PC, Jérôme Segura, Malwarebytes.

7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Базы данных, информационно-справочные и поисковые системы

1. www.biblio-online.ru –Электронно-библиотечная система [ЭБС] Юрайт;
2. http://www.iprbookshop.ru – Электронно-библиотечная система [ЭБС] «Iprbooks»
3. https://e.lanbook.com - Электронно-библиотечная система [ЭБС] «Лань».
4. http://elibrary.ru/ - Научная электронная библиотека Elibrary.ru.
5. https://new.znanium.com Электронно-библиотечная система [ЭБС] «Znanium.com».
6. https://dlib.eastview.com – Информационный сервис «East View».
7. https://www.jstor.org - Jstor. Полные тексты научных журналов и книг зарубежных издательств.
8. https://elibrary.worldbank.org - Электронная библиотека Всемирного Банка.
9. https://link.springer.com - Полнотекстовые политематические базы академических журналов и книг издательства Springer.
10. https://ebookcentral.proquest.com - Ebook Central. Полные тексты книг зарубежных научных издательств.
11. https://www.oxfordhandbooks.com - Доступ к полным текстам справочников Handbooks издательства Oxford по предметным областям: экономика и финансы, право, бизнес и управление.
12. https://journals.sagepub.com - Полнотекстовая база научных журналов академического издательства Sage.
13. Справочно-правовая система «Консультант».
14. Электронный периодический справочник «Гарант».

Программные, технические и электронные средства обучения и контроля знаний.

Аудитории оснащены компьютером с выходом в интернет.

- программный продукт Microsoft Office и др.