МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий

_____ Филиппович А.Ю.

"01" сентября 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Противодействие киберпреступности»

Направление подготовки

10.05.03 «Информационная безопасность автоматизированных систем»

Образовательная программа (профиль)

«Обеспечение информационной безопасности распределенных информационных систем»

Квалификация (степень) выпускника

Специалист

Форма обучения

Очная

Год приема - 2019

Москва 2019 г.

1. Цели освоения дисциплины

К **основным целям** освоения дисциплины «Противодействие киберпреступности» следует отнести:

- овладение проблемами киберпреступности, ее криминологических главных принципов, нужных для оценки меры общественной опасности этого явления;
- анализ способов уголовно-правовой борьбы с ним и формирование предложений, направленных на повышение эффективности уголовно-правового установления борьбы с киберпреступностью;
- оценивание уровня безопасности компьютерных систем и сетей

К **основным задачам** освоения дисциплины «Противодействие киберпреступности» следует отнести:

- выработка навыков совершения криминологический анализ состояния, состава, динамики киберпреступности в мировом масштабе;
- выработка навыков совершить анализ правового опыта противодействия киберпреступности на двух рангах международном и национальном, в том числе совершить сравнительный анализ законодательства заграничных государств;
- выработка навыков проведения инструментального мониторинга защищенности компьютерных систем и сетей.

2. Место дисциплины в структуре ООП

Дисциплина «Противодействие киберпреступности» относится к числу профессиональных учебных дисциплин базовой части цикла (Б1) основной образовательной программы (Б.1.1.44).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Аудит информационной безопасности (ISACA)», «Основы управления информационной безопасностью», «Программно-аппаратные средства защиты информации».

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

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по дисциплине**
ОПК-6	Способность применять нормативные правовые акты в профессиональной деятельности	**знать:** • национальные, межгосударственные и международные стандарты в области

		защиты информации; • нормативные правовые акты в области защиты информации; • уголовно-правовой анализ преступлений в сфере информационных технологий; **уметь:** • оценивать события и явления общественной жизни с позиций закона и действовать в соответствии с его нормами; • применять теоретические знания о преступлениях и преступности в сфере информационных технологий по российскому законодательству. **владеть:** • применять инструментальные средства проведения сертификационных испытаний; • составлять и оформлять аналитический отчет по проведенным сертификационным испытаниям;
ПК-17	Способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	**знать**: • принципы построения компьютерных систем и сетей; • уязвимости компьютерных систем и сетей; • криптографические методы защиты информации; **уметь**: • прогнозировать возможные пути развития действий нарушителя информационной безопасности; • производить анализ политики безопасности на предмет адекватности; • составлять и оформлять аналитический отчет по результатам

		проведенного анализа • разрабатывать предложения по устранению выявленных уязвимостей; **владеть**: • применять программно-аппаратные средства защиты информации в компьютерных сетях; • анализировать компьютерную систему с целью определения уровня защищенности и доверия; • проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в компьютерных сетях; • формулировать предложения по применению программно-аппаратных; средств защиты информации в компьютерных сетях.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единицы, т.е. **108** академических часов (лекции – 18 час, лабораторные занятия – 36 час, самостоятельная работа - 54 часов, форма контроля – зачет) в 8 семестре.

Структура и содержание дисциплины «Противодействие киберпреступности» по срокам и видам работы отражены в приложении.

5. Образовательные технологии

Методика преподавания дисциплины «Противодействие киберпреступности» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков у обучающихся:

- выполнение лабораторных работ в лабораториях вуза;
- индивидуальные и групповые консультации студентов преподавателем, в том числе в виде защиты выполненных заданий в рамках самостоятельной работы;
- посещение профильных конференций и работа на мастер-классах экспертов и специалистов индустрии;
- посещение лекций.

Самостоятельная внеаудиторная работа студентов составляет 50% от общего объема дисциплины и состоит из:

- подготовки к выполнению и подготовки к защите лабораторных работ;
- чтения литературы и освоения дополнительного материала в рамках тематики дисциплины;
- подготовки к текущей аттестации;
- подготовки к промежуточной аттестации.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- зачет.

Образцы вопросов к зачету приведены в приложении.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

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

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ОПК-6	Способность применять нормативные правовые акты в профессиональной деятельности
ПК-17	Способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю):

ОПК-6 Способность применять нормативные правовые акты в профессиональной деятельности				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
ЗНАТЬ	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенными знаниями.
УМЕТЬ	Обучающийся не умеет или в недостаточной степени умеет выполнять действия, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3).	Обучающийся демонстрирует неполное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании умениями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся демонстрирует полное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.

ВЛАДЕТЬ	Обучающийся не владеет или в недостаточной степени владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3).	Обучающийся в неполном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей. Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях.	Обучающийся частично владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Свободно применяет полученные навыки в ситуациях повышенной сложности.

ПК-17 Способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
ЗНАТЬ	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенными знаниями.

УМЕТЬ	Обучающийся не умеет или в недостаточной степени умеет выполнять действия, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3).	Обучающийся демонстрирует неполное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании умениями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся демонстрирует полное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
ВЛАДЕТЬ	Обучающийся не владеет или в недостаточной степени владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3).	Обучающийся в неполном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей. Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях.	Обучающийся частично владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Свободно применяет полученные навыки в ситуациях повышенной сложности.

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: зачет.

Промежуточная аттестация обучающихся в форме зачёта проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов

обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «зачтено» или «не зачтено».

Шкала оценивания	Описание
Зачтено	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Не зачтено	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Фонды оценочных средствпредставлены в приложении к рабочей программе

7. Учебно-методическое и информационное обеспечение дисциплины

1. **Основная литература:**
   - Особенности противодействия киберпреступности подразделениями уголовного розыска : учебно-методическое пособие / ред. П.Б. Михайлов, Е.Н. Хазов. – Москва : Юнити-Дана : Закон и право, 2016. – 151 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=439600 (дата обращения: 19.08.2019). – Библиогр.: с. 134-138. – ISBN 978-5-238-02760-9. – Текст : электронный.

2. **Дополнительная литература:**
   - Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк ; Национальный исследовательский университет – Высшая школа экономики. – Москва : Издательский дом Высшей школы экономики, 2015. – 574 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=440285 (дата обращения: 19.08.2019). – Библиогр. в кн. – ISBN 978-5-7598-0698-1. – Текст : электронный.

8. Материально-техническое обеспечение дисциплины

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерных классов, оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

Оборудование и аппаратура:

1. Операционная система Microsoft Windows.
2. Веб-браузер Chrome.

9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к зачету, а также самостоятельно изучают отдельные темы учебной программы.

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки **10.05.03 «Информационная безопасность автоматизированных систем»**.

Программу составил:

Программа утверждена на заседании кафедры “Информационная безопасность” «29» августа 2019 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

Приложение

Структура и содержание дисциплины «Противодействие киберпреступности»
по направлению подготовки
10.05.03 «Информационная безопасность автоматизированных систем»
(специалист)

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб	СРС	КСР	К.Р.	К.П.	ДЗ	Реферат	К/р	Э	З
	8 семестр														
1	Исследование состояния компьютерно-технической экспертизы	8	1	1		2	2								
2	Понятие судебной экспертизы		2	1		2	2								
3	Понятие компьютерно-технической экспертизы		3	1		2	2								
4	Понятие экспертной методики		4	1		2	2								
5	Требования законодательства к методике (и методам) производства экспертизы		5	1		2	2								
6	Результаты анализа методик производства КТЭ		6	1		2	2								
7	Анализ методик производства КТЭ		7	1		2	2								
8	Классификация методик и построение модели методики производства КТЭ		8	1		2	4								
9	Базовые критерии классификации методик КТЭ		9	1		2	4								
10	Содержание модели методики производства КТЭ		10	1		2	4								

11	Применение методов КТЭ		11	2		2	6								
12	Оценка трудозатрат при производстве комплексной экспертизы		12	2		2	6								
13	Унифицированная методика производства компьютерно-технических экспертиз		15	2		6	8								
14	Практическое применение разработанной методики производства КТЭ		18	2		6	8								
	Форма аттестации	8	19-21							.					З
	Всего часов по дисциплине во восьмом семестре			18		36	54								
	Всего часов по дисциплине			18		36	54								

Приложение к
рабочей программе

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗРВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем»

ОП (профиль): «Обеспечение информационной безопасности распределенных информационных систем»

Форма обучения: очная

Вид профессиональной деятельности: эксплуатационная; проектно-технологическая; экспериментально-исследовательская; организационно-управленческая

.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Противодействие киберпреступности»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

список вопросов к зачету.

Составители:

Москва, 2019 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Противодействие киберпреступности					
ФГОС ВО **10.05.03 «Информационная безопасность автоматизированных систем»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетен**	**Форма оценоч-ного**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ОПК-6	Способность применять нормативные правовые акты в профессиональной деятельности	**знать:** • национальные, межгосударственные и международные стандарты в области нормативные правовые акты в области защиты информации; • нормативные правовые акты в области защиты информации; • уголовно-правовой анализ преступлений в сфере информационных технологий; **уметь:** • оценивать события и явления общественной жизни с позиций закона и действовать в соответствии с его нормами; • применять теоретические знания о преступлениях и преступности в сфере информационных технологий по российскому законодательству. **владеть:** • применять инструментальные средства проведения сертификационных испытаний; • составлять и оформлять аналитический отчет по проведенным сертификационным испытаниям;	самостоятельная работа, лабораторные занятия, лекции	зачет	**Базовый уровень:** **знать:** нормативные правовые акты в области защиты информации; **уметь**: оценивать события и явления общественной жизни с позиций закона и действовать в соответствии с его нормами; **владеть**: анализировать компьютерную систему с целью определения уровня защищенности и доверия; **Повышенный уровень**: национальные, межгосударственные и международные стандарты в области защиты информации; составлять и оформлять аналитический отчет по проведенным сертификационным испытаниям;

ПК-17	Способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	**знать**: • принципы построения компьютерных систем и сетей; • уязвимости компьютерных систем и сетей; • криптографические методы защиты информации; **уметь**: • прогнозировать возможные пути развития действий нарушителя информационной безопасности; • производить анализ политики безопасности на предмет адекватности; • составлять и оформлять аналитический отчет по результатам проведенного анализа • разрабатывать предложения по устранению выявленных уязвимостей; **владеть**: • применять программно-аппаратные средства защиты информации в компьютерных сетях; • анализировать компьютерную систему с целью определения уровня защищенности и доверия; • проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в компьютерных сетях; • формулировать предложения по применению программно-аппаратных; средств защиты информации в компьютерных сетях.	самостоятельная работа, лабораторные занятия, лекции	зачет	**Базовый уровень**: **знать**: принципы построения компьютерных систем и сетей; **уметь**: производить анализ политики безопасности на предмет адекватности; **владеть**: Применять программно-аппаратные средства защиты информации в компьютерных сетях; **Повышенный уровень:** Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в компьютерных сетях;

Приложение 2
к рабочей программе

Оценочные средства для промежуточной аттестации

Список вопросов к зачету по дисциплине

1. Киберпреступность: суть, виды, угрозы и риски.
2. Международный и национальный аспекты борьбы с киберпреступностью.
3. Угрозы и риски, связанные с киберпреступностью.
4. Анализ политики безопасности на предмет адекватности.
5. Организационная и правовая защита информации как составные части системы комплексного противодействия информационным угрозам.
6. Структура и задачи органов власти и управления, отвечающих за организацию защиты информации в стране.
7. Основные цели и задачи организационного обеспечения информационной безопасности на предприятии.
8. Угрозы информационной безопасности. Виды угроз.
9. Утечка информации. Каналы утечки информации. Разглашение информации. Несанкционированный доступ.
10. Национальные, межгосударственные и международные стандарты в области защиты информации.
11. Порядок засекречивания и рассекречивания сведений, составляющих информацию ограниченного доступа.
12. Порядок учета и хранения сведений, составляющих информацию ограниченного доступа.
13. Нормативные правовые акты в области защиты информации.
14. Принципы построения компьютерных систем и сетей.
15. Уязвимости компьютерных систем и сетей.
16. Криптографические методы защиты информации.
17. Принципы построения систем управления базами данных.
18. Механизмы контроля доступа к ресурсам.
19. Аутентификация в операционных системах.
20. Классификация и перечень факторов, воздействующих на безопасность защищаемой информации (ГОСТ Р51275).
21. Основные задачи менеджмента в сфере информационной безопасности.
22. Понятие безопасной информационной инфраструктуры и ее составляющие.
23. Уровни организационной работы в сфере информационной безопасности.
24. Задачи, роли и методы, используемые на различных уровнях организационной работы в сфере информационной безопасности.
25. Роль международных организаций и объединений в сфере информационной безопасности.
26. Обзор деятельности международных профессиональных объединений и направлений их деятельности в сфере информационной безопасности.
27. Направления организационной работы в сфере информационной безопасности специализированных международных организаций и объединений.
28. Роль и направления деятельности альянсов крупных технологических компаний в сфере информационной безопасности.