МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙГУМАНИТАРНЫЙ УНИВЕРСИТЕТ»
(РГГУ)

ИНСТИТУТ ЭКОНОМИКИ, УПРАВЛЕНИЯ И ПРАВА

ФАКУЛЬТЕТ УПРАВЛЕНИЯ

КАФЕДРА МОДЕЛИРОВАНИЯ В ЭКОНОМИКЕ И УПРАВЛЕНИИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

38.05.01 Экономическая безопасность

Код и наименование направления подготовки/специальности

«Экономическая безопасность хозяйствующего субъекта»

Наименование специализации

Уровень высшего образования: специалитет

Форма обучения: очная, заочная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2024

Информационная безопасность

Рабочая программа дисциплины

Составитель:
доцент *С.В. Никифоров*

Протокол заседания кафедры
№ 3 от 24.03.2024 г.

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель курса – сформировать у студентов представление о месте и роли информационной безопасности в экономике, ознакомить обучаемых с основами обеспечения информационной безопасности, основными средствами и методами защиты информации.

Задачи курса

–формирование практических навыков по использованию средств обеспечения информационной безопасности;

- ознакомление с основными принципами и методами обеспечения информационной безопасности.

1.2 . Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-2 Способен использовать информацию разного уровня для мониторинга факторов, анализа финансово-экономических показателей деятельности хозяйствующих субъектов, оценки угроз и рисков экономической безопасности, готовить аналитические материалы для принятия решений в сфере экономической безопасности, в том числе с использованием современных информационных технологий	ПК-2.2 Осуществляет подготовку аналитических материалов, в т.ч с применением информационных технологий;	*Знать:* -основные причины потери или искажения информации -наиболее значимые для практики вопросы создания политики защиты *Уметь:* формулировать задачи в соответствующей области деятельности по обеспечению защиты информации *Владеть:* методами и программными средствами обработки деловой информации, способностью взаимодействовать со службами информационных технологий и эффективно использовать корпоративные информационные системы
	ПК-2.3 Анализирует и применяет нормативно-правовые акты в целях обеспечения экономической безопасности хозяйствующих субъектов	*Знать:* принципы обеспечения информационной безопасности в свете положений Доктрины информационной безопасности Российской Федерации - основные нормативные и руководящие документы в области информационной безопасности *Уметь:* на основе полученных знаний применять необходимые средства и методы при практической

		реализации защищенных информационных систем и технологий в различных прикладных сферах *Владеть:* Методикой применения справочно-правовых систем
ПК-4 Способен проводить мониторинг и контроль основных показателей бизнес-среды для выявления угроз экономической безопасности хозяйствующего субъектв и обеспечения текущей деятельности	ПК-4.3 Разрабатывает меры, план мероприятий по устранению негативных воздействий на экономическую безопасность хозяйствующего субъекта	*Знать:* принципы системного анализа и классификации угроз информационной безопасности *Уметь:* на основе полученных знаний применять необходимые средства и методы при практической реализации защищенных информационных систем и технологий в экономической деятельности *Владеть:* способностью взаимодействовать со службами информационных технологий и эффективно использовать корпоративные информационные системы.

1.3. Место дисциплины в структуре основной образовательной программы

Дисциплина «Информационная безопасность» относится к части, формируемой участниками образовательных отношений блока 1 дисциплин учебного плана.

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 з.е., 108 академических часов.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Курс	Тип учебных занятий	Количество часов
6	Лекции	**16**
6	Семинары	**26**
	Всего:	**42**

Объем дисциплины в форме самостоятельной работы обучающихся составляет 48 академических часов.

Структура дисциплины для заочной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Курс	Тип учебных занятий	Количество часов

6	Лекции	**4**
6	Семинары	**8**
	Всего:	**12**

Объем дисциплины в форме самостоятельной работы обучающихся составляет 96 академических часов.

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	Тема 1 Терминологические основы информационной безопасности. Основные понятия и определения	Информационные процессы, информационная сфера, информационная безопасность. Информационные войны, информационное оружие и информационный терроризм. Объективная необходимость и общественная потребность в защите информации. Информация как объект правовой защиты. Сущность, общее содержание и цели защиты информации. Правовое регулирование вопросов защиты информации
2	Тема 2 Информационная безопасность РФ, ее место в национальной безопасности.	Информационная безопасность в условиях функционирования в России глобальных сетей. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Место информационной безопасности информационных систем в национальной безопасности страны. Составляющие национальных интересов РФ в информационной сфере. Доктрина информационной безопасности РФ. Доктрина информационной безопасности РФ. Отечественные нормативные и руководящие документы, связанные с информационной безопасностью. Руководящие документы Гостехкомиссии РФ.
3	Тема 3. Основные положения теории информационной безопасности информационных систем.	Виды, происхождение, предпосылки появления и источники угроз информационной безопасности. Последствия таких угроз. Случайные угрозы: отказы, сбои, ошибки, аварийные ситуации, побочные влияния внешней среды. Преднамеренные угрозы, злоумышленные действия людей.
4	Тема 4 Методы нарушения конфиденциальности, целостности и доступности.	Регистрация нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Примеры. Стратегии защиты информации. Анализ способов нарушений информационной безопасности.
5	Тема 5. Защита информации в	Понятие концепции и политик информационной

	компьютерных системах	безопасности. Организационные мероприятия по защите информации.. Противодействие программным и аппаратным закладкам на этапах разработки и производства систем. Разграничение доступа. Контроль целостности программ и данных .путем использования контрольного суммирования и циклических кодов. Защита информации в компьютерных системах от случайных угроз. Контроль сбоев и отказов в работе оборудования. Резервирование технических средств. Концепция комплексной системы защиты информации (КСЗИ). Отдельно рассмотрены все методы разграничения доступа к данным в АИС и средства шифрования для сохранения секретных данных в АИС и при передаче по сетям связи.
6	Тема 6. Криптографические методы защиты.	Криптография и криптоанализ. Понятие криптостойкости системы защиты информации. Шифрование как метод криптографического преобразования. Ключи и алгоритмы шифрования. Системы блочного шифрования на основе отечественного ГОСТа и стандарта DES (США). Электронная цифровая подпись на основе криптографического преобразования. Особенности стандартизации и сертификации криптографических средств.
7	Тема 7. Компьютерные вирусы и антивирусные программные средства	Компьютерные вирусы как специальный класс саморепродуцирующихся вредительских программ. Вирусные атаки. Модели распространения вирусных программ. Классификация компьютерных вирусов. Методы и средства антивирусной защиты.

4. Образовательные технологии

Для проведения учебных занятий по дисциплине используются различные образовательные технологии. Для организации учебного процесса может быть использовано электронное обучение и (или) дистанционные образовательные технологии.

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		

- устный опрос	10 баллов	60 баллов
Промежуточная аттестация (*экзамен*)		40 баллов
Итого за семестр		100 баллов

Полученный совокупный результат (максимум 100 баллов) конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5,2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	«удовлетвори-тельно»/ «зачтено (удовлетвори-тельно)»/ «зачтено»	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворите льно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине.

Текущая аттестация

При оценивании устного опроса на практическом занятии учитываются:
- степень раскрытия темы выступления (0-6 баллов);
- знание содержания обсуждаемых проблем, умение использовать ранее изученный теоретический материал и терминологию научных исследований (0-4 балла).
Вопросы приведены в п. 9.1

Промежуточная аттестация

Перечень вопросов к экзамену

1. Понятие информационной безопасности. Информационная безопасность личности, общества и государства. Конфиденциальная информация.
2. Информационная безопасность как составляющая национальной безопасности. Задачи государства в этой области. Информационное оружие, информационные войны и терроризм. Государственные органы РФ, реализующие функции обеспечения информационной безопасности.
3. Компьютерная система (КС) как объект защиты информации. Угрозы информационной безопасности в КС. Классификация угроз.
4. Общая характеристика угроз доступности.
5. Общая характеристика угроз целостности.
6. Общая характеристика угроз конфиденциальности.
7. Обобщенные модели системы защиты информации в КС. Одноуровневые и многоуровневые модели. Общая характеристика средств и методов защиты информации в КС.
8. Общая характеристика организационных мероприятий, обеспечивающих информационную безопасность КС. Основные задачи службы безопасности.
9. Отечественное законодательство в области информации и защиты информации.
10. Минимизация ущерба, наносимого КС авариями и стихийными бедствиями. Дублирование информации. Технология RAID. Резервирование технических средств.
11. Общая характеристика технических каналов утечки информации в КС.
12. Базовые принципы, лежащие в основе моделей политики безопасности в КС. Матричная (дискреционная) модель и мандатная (полномочная) модель управления доступом к ресурсам КС.
13. Средства и методы разграничения доступа к ресурсам КС.
14. Защита программных средств КС от несанкционированного копирования и исследования.
15. Общие понятия, история развития и классификация криптографических средств.
16. Общая характеристика различных методов шифрования. Криптостойкость. Шифрование с симметричным и несимметричным ключами.
17. Различные методы шифрования.
18. Отечественные и зарубежные стандарты шифрования.
19. Общая характеристика и классификация компьютерных вирусов.
20. Механизм заражения файловыми и загрузочными вирусами. Особенности макровирусов.
21. Средства, используемые для обнаружения компьютерных вирусов.
22. Профилактика заражения компьютерными вирусами.
23. Антивирусные средства для лечения и удаления компьютерных вирусов. Программы-полифаги. Эвристические анализаторы.
24. Содержательный смысл понятия комплексной системы защиты информации (КСЗИ) в компьютерных системах. Основные принципы и положения, реализующие системный подход к построению КСЗИ.
25. Основные технологические этапы разработки КСЗИ.

26. Организационно-технические мероприятия, проводимые в процессе эксплуатации КСЗИ.

27. Задачи, решаемые подсистемой аудита в составе защищенных КС.

28. Международные стандарты в области информационной безопасности. Основные положения. Основные положения РД Гостехкомиссии РФ (Пятикнижие).

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники

Основные

Конституция Российской Федерации от 12.12.1993 г. http://www.consultant.ru

Доктрина информационной безопасности РФ. Утверждена Указом Президента Российской Федерации от 05.12.2016 г. № 646. http://www.consultant.ru

Федеральный закон РФ от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». http://www.consultant.ru

Федеральный закон РФ от 27 июля 2006 № 152-ФЗ «О персональных данных». http://www.consultant.ru

Дополнительные

Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности». http://www.consultant.ru

Закон РФ от 21 июля 1993 № 5485-1 «О государственной тайне» http://www.consultant.ru

Федеральный закон рф от 29 июля 2004 № 98-фз «О коммерческой тайне». http://www.consultant.ru

Литература

Основная

Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544290

Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544029

Дополнительная

Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 327 с. — (Высшее образование). — ISBN 978-5-534-16772-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542739

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ru www.grebennikon.ru

6.3. Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения: учебные аудитории, оснащённые компьютером и проектором для демонстрации учебных материалов.

Состав программного обеспечения:
1. Windows
2. Microsoft Office
3. ПО Kaspersky Endpoint Security

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий

Практическое занятие 1. Составляющие информационной безопасности. Законодательный уровень обеспечения информационной безопасности

Вопросы для обсуждения

1. Понятие доступности
2. Понятие целостности
3. Понятие конфиденциальности
4. Федеральный закон РФ от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» / Рос. газ. Федер. вып. № 165 (4131). – 2006. – 29 июля
5. Другие законы и нормативные акты.

Практическое занятие 2 Нормативный уровень обеспечения ниформационной безопасности

Вопросы для обсуждения

1. Руководящий документ Гостехкомиссии России. Термины и определения в области защиты от НСД к информации.
2. Руководящий документ Гостехкомиссии России. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.
3. Руководящий документ Гостехкомиссии России. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации.

4. Руководящий документ Гостехкомиссии России. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
5. Руководящий документ Гостехкомиссии России. Средства вычислительной техники, Межсетевые экраны. Защита от несанкционированного доступа к информации
6. Стандарт международный ISO/IEC 15408. Общие критерии оценки безопасности информационных технологий. - М.: GlobalTrust, 2005

Практическое занятие 3 Административный уровень информационной безопасности

Вопросы для обсуждения

1. Политика безопасности
2. Программа Безопасности
3. Синхронизация программы безопасности с жизненным циклом систем
4. Предельный переход биномиального закона в закон Пуассона.

Практическое занятие 4. Управление рисками. Процедурный уровень информационной безопасности

Вопросы для обсуждения

1. Подготовительные этапы управления рисками.
2. Основные этапы управления рисками
3. Основные классы мер процедурного уровня
4. Управление персоналом как основной группой риска
5. Фиическая защита
6. Поддержание работоспособности
7. Реагирование на нарушение режима безопасности
8. Планирование восстановительных работ

Практическое занятие 5. Основные программно-технические меры. Протоколирование и аудит, шифрование, контроль целостности.

Вопросы для обсуждения:

1. Основные понятия программно-технического уровня информационной безопасности
2. Особенности современных информационных систем, существенные с точки зрения информационной безопасности
3. Архитектурная безопасность
4. Активный аудит
5. Функциональные компоненты и архитектура
6. Шифрование
7. Цифровые сертификаты

Практическое занятие 6. Экранирование, анализ защищенности. Обеспечение высокой доступности. Туннелирование и управление.

Вопросы для обсуждения.

1. Классификация межсетевых экранов.
2. Анализ защищенности
3. Основы мер обеспечения высокой лоступности
4. Отказоустойчивость и зона риска
5. Программное обеспечение промежуточного слоя
6. Обеспечение обслуживаемости
7. Туннелирование

8. Управление
9. Возможности типичных систем

Приложение 1

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность» относится к части, формируемой участниками образовательных отношений блока 1 дисциплин учебного плана.

Цель курса – сформировать у студентов представление о месте и роли информационной безопасности в экономике, ознакомить обучаемых с основами обеспечения информационной безопасности, основными средствами и методами защиты информации.

Задачи курса

–формирование практических навыков по использованию средств обеспечения информационной безопасности;

- ознакомление с основными принципами и методами обеспечения информационной безопасности.

В результате освоения дисциплины обучающийся должен:

Знать: основные причины потери или искажения информации; наиболее значимые для практики вопросы создания политики защиты; принципы обеспечения информационной безопасности в свете положений Доктрины информационной безопасности Российской Федерации; основные нормативные и руководящие документы в области информационной безопасности; принципы системного анализа и классификации угроз информационной безопасности

Уметь: формулировать задачи в соответствующей области деятельности по обеспечению защиты информации; на основе полученных знаний применять необходимые средства и методы при практической реализации защищенных информационных систем и технологий в различных прикладных сферах; на основе полученных знаний применять необходимые средства и методы при практической реализации защищенных информационных систем и технологий в экономической деятельности.

Владеть: методами и программными средствами обработки деловой информации, способностью взаимодействовать со службами информационных технологий и эффективно использовать корпоративные информационные системы; методикой применения справочно-правовых систем; способностью взаимодействовать со службами информационных технологий и эффективно использовать корпоративные информационные системы.