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, очно-заочная, заочная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2023

Информационная безопасность

Рабочая программа дисциплины

Составитель:
доцент *С.В. Никифоров*
……
Ответственный редактор

……

УТВЕРЖДЕНО
Протокол заседания кафедры

№ 6 от 13 апреля 2023 года

УТВЕРЖДАЮ

Руководитель ООП ВПО

_____
(название)

_____
(подпись, ф.и.о.)

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 обязательной части, формируемой участниками образовательных отношений блока 1 дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик:

«Менеджмент», «Эконометрика», «Теория вероятностей и математическая статистика», «Правовое обеспечение экономической безопасности», «Финансовая безопасность организации».

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:

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

Объем дисциплины в форме самостоятельной работы обучающихся составляет

48_ академических часов, контроль (экзамен) 18 час.

Структура дисциплины для очно-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:

Семестр	Тип учебных занятий	Количество часов
6	Лекции	**8**
6	Семинары	**14**
	Всего:	**22**

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет _68_ академических часа, контроль (экзамен) 18 час.

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:

Семестр	Тип учебных занятий	Количество часов
	Лекции	**4**
	Семинары/лабораторные работы	**8**
	Всего:	**12**

Объем дисциплины в форме самостоятельной работы обучающихся составляет _87_ академических часов контроль (экзамен) 9 час.

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 компьютерных системах	Понятие концепции и политик информационной 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

В процессе изучения дисциплины проводится рейтинговый контроль знаний undefined в соответствии с Положением РГГУ о его проведении. Он предполагает учет результатов написания контрольной работы и выполнения заданий 1,2,3 на основе компьютерных технологий (практические занятия 5,6,7), результатов самостоятельной работы по выполнению домашних заданий, а также степени участия бакалавров в дискуссиях, при обсуждении проблемных вопросов на практических занятиях.

Критерии, используемые при проведении рейтингового контроля для студентов, изучающих дисциплину «Теория вероятностей и математическая статистика», представлены в таблице:

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		
- устный блиц-опрос и участие в дискуссии на семинаре	2,5 балла	10 баллов
- контрольная работа	20 баллов	20 баллов
- задание 1	10 баллов	10 баллов
- задание 2 - задание 3	10 баллов 10 баллов	10 баллов 10 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 профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		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.

При оценивании устного блиц-опроса и участия в дискуссии на практическом занятии учитываются:
- степень раскрытия темы выступления (0-2,5 баллов);

- знание содержания обсуждаемых проблем, умение использовать ранее изученный теоретический материал и терминологию научных исследований (0-2 балла).
При оценке контрольной работы учитывается:
- полнота и правильность решения задания (0-2 балла) (для заданий 1,2,3,4);
- полнота и правильность решения задания (0-3 балла) (для заданий 5,6,7,8);
При оценке заданий 1,2,3 на основе компьютерных технологий учитывается:
- полнота и точность выполненной работы (0-4 балла);
- оформление работы (0-2 балла);
- - полнота и точность ответов на контрольные вопросы (0-4 балла).

Промежуточная аттестация (зачет)

При проведении промежуточной аттестации студент должен ответить на 2 вопроса (теоретического и практического характера).
При оценивании ответа на вопрос теоретического характера учитывается:
- теоретическое содержание освоено не полностью, знание материала носит фрагментарный характер, имеются явные ошибки в ответе (до 5 баллов);
- теоретическое содержание освоено частично, допущено не более двух-трех недочетов (до 10 баллов);
- теоретическое содержание освоено почти полностью, допущено не более одного-двух недочетов (до 15 баллов);
- теоретическое содержание освоено полностью, (20 баллов).
При оценивании ответа на вопрос практического характера учитывается:
- ответ содержит менее 30% правильного решения (0-5 баллов);
- ответ содержит 31-79 % правильного решения (6-15 баллов);
- ответ содержит 80% и более правильного решения (15- 20 баллов).

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности.

Контрольная и задания на основе компьютерных технологий (текущий контроль) содержат типовые задания по ключевым практическим аспектам укрупненных тематик дисциплины и проводятся в течение семестра после их изучения. Итоговые контрольные работы (промежуточный контроль) содержат теоретические вопросы курса, базовые понятия, теоремы и практические задания, не включенные в текущий контроль успеваемости, по укрупненным тематическим разделам. Каждый студент получает индивидуальный вариант работы. Для каждого укрупненного тематического раздела приведены ссылки на основную рекомендуемую литературу с указание параграфов.

Задания для текущего контроля успеваемости
Контрольные вопросы по курсу.

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).

1.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Конституция Российской Федерации. Официальное издание. - М., Изд. «Юридическая литература», Администрация Президента РФ, 1997. - 64 с.

Доктрина информационной безопасности РФ. Утверждена Президентом Российской Федерации 9.09.2000 г. № Пр-1895 // Рос. газ. Федер. вып. № 187 (2551). – 2000. – 28 сент.

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.

Федеральный закон РФ от 27 июля 2006 № 152-ФЗ «О персональных данных» // Рос. газ. Федер. вып. № 165 (4131). – 2006. – 29 июля.

Руководящий документ Гостехкомиссии России. Термины и определения в области защиты от НСД к информации. - М.: ГТК РФ, 1992.

Руководящий документ Гостехкомиссии России. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. - М.: ГТК РФ, 1992.

Руководящий документ Гостехкомиссии России. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. - М.: ГТК РФ, 1992.

Руководящий документ Гостехкомиссии России. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. - М.: ГТК РФ, 1992.

Руководящий документ Гостехкомиссии России. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. - М.: ГТК РФ, 1997.

Стандарт международный ISO/IEC 15408. Общие критерии оценки безопасности информационных технологий. - М.: GlobalTrust, 2005.

Дополнительные

Закон Российской Федерации от 5 марта 1992 № 2446-I «О безопасности» (в ред. Закона РФ от 25.12.1992 № 4235-1, Указа Президента РФ от 24.12.1993 № 2288, Федеральных законов от 25.07.2002 № 116-ФЗ, от 07.03.2005 № 15-ФЗ, от 25.07.2006 № 128-ФЗ, от 02.03.2007 № 24-ФЗ, от 26.06.2008 №103-ФЗ) / Ведомости Съезда народных депутатов РФ и Верховного Совета РФ. - 1992. - № 15 // Рос. газ. – 1992. - 6 мая.

Закон РФ от 21 июля 1993 № 5485-1 «О государственной тайне» (в ред. Федерального закона от 06.10.97 № 131-ФЗ) // Собр. Законодательства РФ. – 1997. - № 41. – 2004. - № 35 / Рос. Газ. – 1993. - 21 сентября.

Федеральный закон рф от 29 июля 2004 № 98-фз «о коммерческой тайне» / рос. Газ. Федер. Вып. № 3543. – 2004. - 5 августа.

Федеральный закон рф от 1 декабря 2007 № 294-фз «о внесении изменений в статьи 4 и 18 закона рф «о государственной тайне»" / рос. Газ. Федер. Вып. № 4534. – 2007. - 4 декабря.

Постановление Правительства РФ от 5 декабря 1991 № 35 «О перечне сведений, которые не могут составлять коммерческую тайну» (ред. Постановления Правительства РФ от 03.10.2002 № 731, в части, не против. ст. 5 ФЗ от 29.07.2004 № 98-ФЗ «О коммерческой тайне») / Собр. постановлений Правительства РСФСР. - 1992. - № 1-2.

Постановление Правительства РФ от 27 мая 2002 № 348 «Об утверждении положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации» / Собр. законодательства РФ. - 2002. - № 23 (утратил силу с введ. Постановления Правительства РФ от 31 августа 2006 № 532).

Стандарт Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” СТО БР ИББС-1.0-2006 / Вестник Банка России. - № 6. - М. 2006.

Стандарт международный Cobit 4.0. Задачи управления (Control Objectives). Руководство по менеджменту (Management Guidelines). – М.: GlobalTrust, Алмитек, 2000.

Учебники и учебные пособия

Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с.

Вострецова Е.В. Основы информационной безопасности: Учебное пособие / Вострецова Е.В. – Екатеринбург, издательство «Урал. Ун-та», 2019 – 204 с.

Основы информационной безопасности. Курс лекций. Учебное пособие /Издание второе, исправленное / Галатенко В.А. Под редакцией чл-корр. РАН В.Б. Бетелина, М.: ИНТУИТ.РУ «Интернет университет информационных технологий», 2004. – 264 с.

Основная литература

Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2016. — 280 с.

Лопатин В. Н. Информационная безопасность России: Человек. Общество. Государство / В. Н. Лопатин. МВД России, СПб. ун-т. - СПб.: Фонд «Ун-т», 2000.

Ярочкин В.И. Информационная безопасность: учебник для вузов. - [4-е изд.]. - М.: Акад. проект, 2006.

Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2017. — 336 с.

Дополнительная литература

Алексенцев А.И. Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность» // Безопасность информационных технологий. - 1999. - № 1.

Баранович А.Е. Дидактические материалы к специальному курсу «Введение в информациологию и ее специальные приложения»: учеб. пособие. - М.: Российск. гос. гуманит. ун-т, 2009.

Грушо А.А., Применко Э.А., Тимонина Е.Е. Анализ и синтез криптоалгоритмов : Курс лекций. - Йошкар-Ола : Марийский фил. Моск. открытого соц. ун-та, 2000.

Расторгуев С.А. Программные методы защиты информации в компьютерах и сетях. - М.: Яхтсмен, 1993.

Скиба В., Курбатов В. Руководство по защите от внутренних угроз информационной безопасности. - Спб.: Питер, 2008.

Тихонов В. А., Райх В. В. Информационная безопасность. Концептуальные, правовые, организационные и технические аспекты. - М.: Гелиос АРВ, 2006.

Торокин А. А. Инженерно-техническая защита информации. - М.: Гелиос АРВ, 2005.

Фергюсон Н., Шнайер Б. Практическая криптография. - М.: Вильямс, 2005.

Черней Г.А. Оценка угроз безопасности автоматизированным информационным системам // НТИ. Сер. 2. Информационные процессы и системы. - 1997. - № 10.

Шанкин Г.П. Ценность информации. Вопросы теории и приложений. - М.: Филоматис, 2004.

Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие для студентов учреждений сред. проф. образования, обучающихся по группе специальностей 2200 «Информатика и вычислительная техника». - М.: Форум - Инфра-М, 2008.

Шеннон К. Работы по теории информации и кибернетике: Пер. с англ. - М.: Иностр. лит-ра, 1963.

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса лицам с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого от студента требуется представить заключение психолого-медико-педагогической комиссии (ПМПК) и личное заявление (заявление законного представителя).

В заключении ПМПК должно быть прописано:
- рекомендуемая учебная нагрузка на обучающегося (количество дней в неделю, часов в день);
- оборудование технических условий (при необходимости);
- сопровождение и (или) присутствие родителей (законных представителей) во время учебного процесса (при необходимости);
- организация психолого-педагогического сопровождение обучающегося с указанием специалистов и допустимой нагрузки (количества часов в неделю).

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся, при необходимости могут быть созданы фонды оценочных средств, адаптированные для лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе.
Форма проведения текущей и итоговой аттестации для лиц с ограниченными возможностями здоровья устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно (на бумаге, на компьютере), в форме тестирования и т.п.). При необходимости студенту предоставляется дополнительное время для подготовки ответа на зачете или экзамене.

9. Методические материалы
9.1. Планы практических занятий

Цель практических занятий — помочь студентам применять полученные на лекциях знания как в процессе обучения, так и в будущей самостоятельной работе.

На практических занятиях отрабатываются наиболее важные моменты курса. Выбор темы практического занятия определяется, во-первых, последовательностью материала, читаемого на лекциях в соответствии с программой курса, а во-вторых, важностью темы, затрагивающей ключевые или узловые проблемы изучаемой дисциплины.

Практические занятия проводятся в форме обсуждения заданных планом вопросов и разбора решений типовых задач. В ходе проведения занятий студенты приобретают навыки построения вероятностных моделей, вычисления вероятностей случайных событий, применения наиболее важных законов распределения случайных величин. При подготовке к занятию студент должен ознакомиться с планом практического занятия, изучить выносимые на практическое занятие темы и вопросы на основании конспектов лекций и рекомендуемой литературы. В последнем случае особое внимание следует уделить методам решения типовых задач, излагаемым в перечисленных учебниках и задачниках.

В течение семестра студенты должны выполнить три практических занятия с использованием компьютерных технологий.

Цель практических занятий с использованием компьютерных технологий– помочь студентам овладеть методами математической статистики и применять полученные знания для решения конкретных задач в будущей самостоятельной работе.

Особенностью практических занятий с использованием компьютерных технологий является их компьютерная направленность. В качестве программной среды используются средства Microsoft Excel (электронные таблицы MS Office).

Выполнив все практические занятия с использованием компьютерных технологий, студент должен уметь:

- выделить проблему, исследование которой может быть связано со статистическим анализом
- определить генеральную совокупность и исследуемую случайную величину;
- сформулировать математическую постановку задачи собрать экспериментальный материал и сформировать выборку;
- с учетом поставленной задачи, используя методы математической статистики, провести обработку и анализ данных
- использовать вычислительную технику при выполнении статистических расчетов

Перед выполнением практического занятия с использованием компьютерных технологий студент должен проработать относящийся к ней теоретический материал.

Выполнение каждого практическго занятия с использованием компьютерных технологий протекает в несколько этапов. Сначала студент ознакомится с основными положениями и общей постановкой задачи. Затем под руководством преподавателя решает общую конкретную задачу, на примере которой осваивает методы математической статистики и проводит анализ полученных результатов.

По каждому практическому занятию с использованием компьютерных технологий студент получает индивидуальное задание, которое выполняется и оформляется в виде отчета.

Преподаватель проверяет правильность и понимание студентом полученных результатов и засчитывает студенту задание только после его ответов на контрольные вопросы.

Ниже подробно раскрывается содержание практических занятитий с использованием компьютерных технологий.

Приведены:

1) количество аудиторных часов;

2) вопросы для обсуждения, которые отражают ключевые теоретические аспекты курса и методики решения типовых математических задач, а также возможность их использования в предметной области;

Для эффективного обучения студенты должны выполнить домашнее задание, выдаваемое после каждого практического занятия, содержание которого соответствует пройденному теоретическому и практическому материалу.

Ниже подробно раскрывается содержание практических занятий. Приведены:

1) количество аудиторных часов;

2) вопросы для обсуждения, которые отражают ключевые теоретические аспекты курса и методики решения типовых математических задач, а также возможность их использования в предметной области;

На практичкские занятия по программе дисциплины «Теория вероятностей и математическая статистика» отведено 24 часа.

Практическое занятие 1

Количество часов – 4 часа.

Тема 1 Составляющие информационной безопасности
Тема 2 Законодательный уровень обеспечения информационной безопасности

Тема 1. 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

Количество часов –4 часа.

Тема 3. 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

Количество часов – 4 часа.

Тема 4. 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

Количество часов – 4 часа.

Тема 5. Управление рисками
Тема 6. 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.

Количество часов – 4 часа.

Темы 7. Основные программно-технические меры

Тема 8. 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.

Тема 9. Экранирование, анализ защищенности

Тема 10. Обеспечение высокой доступности

Тема 11. 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 обязательной части, формируемой участниками образовательных отношений блока 1 дисциплин учебного плана.

Дисциплина реализуется кафедрой моделирования в экономике и управлении факультета управления Института экономики, управления и права.

Цель дисциплины:

Предметом курса является рассмотрение средств и методов защиты информации и обеспечение информационной безопасности в автоматизированные информационные

системы . Во вводной части курса приводится рассмотрение основных угроз информации и их причин, также источников возможной потери информации в автоматизированных информационных системах .

Целью курса является формирование у студентов представления о месте и роли информационной безопасности в экономической безопасности, ознакомление обучаемых с основами обеспечения информационной безопасности, основными средствами и методами защиты информации.

Задачи:

- показать основные причины нарушения информации

- ознакомить студентов с основными принципами и методами обеспечения информационной безопасности.

-сформировать у студентов практические навыки по использованию средств обеспечения информационной безопасности;

Дисциплина направлена на формирование следующих компетенций*:*

Профессиональных (ПК)

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-4 Способен проводить мониторинг и контроль основных показателей бизнес-среды для выявления угроз экономической безопасности хозяйствующего субъектв и обеспечения текущей деятельности

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;
- анализировать особенности нарушения информационной безопасности с целью выбора для защиты информации наиболее подходящей технологии;
- на основе полученных знаний применять необходимые средства и методы при практической реализации защищенных информационных систем и технологий в различных прикладных сферах

владеть:

- набором инструментов, средств, методов и мероприятий по организации комплекса средств защиты информации в компьютерных технологиях;

- методологией организации, планирования и контроля функционирования комплекса средств защиты информации;

- инструментарием практического применения технических, программных и программно-аппаратных средств и методов защиты информации в компьютерных технологиях;

- инструментарием организации системы управления контролем доступа в сетевых компьютерных технологиях и оценку их информационной безопасности.

Промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы, 108 часов.