Федеральное государственное образовательное бюджетное учреждение
высшего образования

**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)**

Кафедра «Информационная безопасность»

С.А.Борисов

Информационная безопасность

Рабочая программа дисциплины

для студентов, обучающихся по направлению подготовки
38.03.01 «Экономика»
Профиль
«Экономическая безопасность хозяйствующих субъектов»

Москва
2019

Федеральное государственное образовательное бюджетное учреждение
высшего образования
**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**
(Финансовый университет)

Кафедра «Информационная безопасность»

УТВЕРЖДАЮ
Проректор по развитию
образовательных программ
_____Е.А. Каменева
«18» января 2019 г.

С.А.Борисов

Информационная безопасность

Рабочая программа дисциплины

для студентов, обучающихся по направлению подготовки
38.03.01 «Экономика»
Профиль
«Экономическая безопасность хозяйствующих субъектов»

Одобрено кафедрой «Информационная безопасность»
(протокол №9 от 10.01.2019 г.)

Рекомендовано Ученым советом факультета
«Прикладной математики и информационных технологий»
(протокол №11 от 15.01.2019 г.)

Москва 2019

УДК 004.451(073)
ББК 32.973я73
С12

Рецензент: **д.ф.-м.н., профессор Фомичев В.М. –** профессор кафедры «Информационная безопасность»

С12 **С.А.Борисов «Информационная безопасность».** Рабочая программа дисциплины для студентов, обучающихся по направлению подготовки 38.03.01 Экономика, профиль «Экономическая безопасность хозяйствующих субъектов» (очная форма обучения) – М.: Финансовый университет, кафедра «Информационная безопасность», 2019 – 30 с.

Рабочая программа дисциплины содержит требования к результатам освоения дисциплины, содержание дисциплины, тематику практических занятий и технологии их проведения, формы самостоятельной работы, контрольные вопросы и систему оценивания, учебно-методическое и информационное обеспечение дисциплины.

УДК 004.451(073)

ББК 32.973я73

Учебное издание

Борисов Сергей Александрович

Информационная безопасность

Рабочая программа дисциплины

Компьютерный набор, верстка С.А.Борисов

Формат 60x90/16. Гарнитура *Times New Roman*
Усл. п.л. 2,0625. Изд. № _____. – 2019. Тираж - 25 экз.

Заказ № _____

Отпечатано в Финансовом университете

СОДЕРЖАНИЕ

1 Наименование дисциплины

«Информационная безопасность».

2 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 1.

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	**Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции**
ПКП- 4	Способность разрабатывать правила внутреннего контроля в организации в целях обеспечения экономической безопасности	-	**Знать** принципы и подходы, лежащие в основе организации и проведении контроля обеспечения информационной безопасности хозяйствующего субъекта **Уметь** выполнять процедуры по контролю обеспечения информационной безопасности хозяйствующего субъекта **Владеть** навыками организации мероприятия по контролю обеспечения информационной безопасности хозяйствующего субъекта

3 Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» является дисциплиной по выбору профильного блока направления подготовки бакалавров 38.03.01 Экономика, профиль «Экономическая безопасность хозяйствующих субъектов».

4 Объем дисциплины в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся (в семестре, в сессию)

Общая трудоёмкость дисциплины составляет 3 ЗЕ (108 часов).

Вид промежуточной аттестации – зачет в пятом семестре.

Таблица 2

Вид учебной работы по дисциплине	**Всего (в з/е и часах)**	**Семестр 5 (в часах)**
Общая трудоёмкость дисциплины	3 з\е, 108 ч.	108
Контактная работа - Аудиторные занятия	36	36
Лекции	18	18
Семинары, практические занятия	18	18
Самостоятельная работа	72	72
Вид текущего контроля	Эссе	Эссе
Вид промежуточной аттестации	Зачет	Зачет

5 Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий

5.1 Содержание тем дисциплины

Тема 1. Информационная безопасность в системе национальной безопасности

Понятийный аппарат и основы терминологии информационной и национальной безопасности. Виды национальной безопасности и их краткая характеристика. Системные связи информационной безопасности с другими видами национальной безопасности.

Тема 2. Информационные уязвимости объектов

Антропогенные информационные уязвимости. Техногенные информационные уязвимости. Организационно-правовые и комбинированные информационные уязвимости.

Тема 3. Угрозы информационной безопасности и их источники

Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация. Угрозы конфиденциальности, целостности и доступности информации. Системная классификация угроз. Информационная война как высшая форма угрозы информационной безопасности.

Тема 4. Средства обеспечения информационной безопасности

Организационно-правовые средства обеспечения информационной безопасности, категорирование информации, допуск и доступ к информационным ресурсам. Программно-аппаратные, криптографические и стеганографические средства обеспечения информационной безопасности. Пассивные и активные средства противодействия техническим разведкам. Защита информации от утечки по техническим каналам.

Тема 5. Риски информационной безопасности и проблема построения комплексной системы защиты информации

Стратегия и концепция защиты информации. Формирование политики обеспечения информационной безопасности. Проблема равнопрочного распределения ограниченных средств обеспечения информационной безопасности по информационным уязвимостям, методы и критерии ее решения. Построение комплексной оптимальной системы защиты. Оценка рисков и организация управления процессом защиты информации.

Тема 6. Обработка и передача информации в вычислительных и управляющих системах и сетях связи, вопросы информационной безопасности и защиты информации для вычислительных и управляющих систем и сетей

Человек и информация; сообщения, сигналы; обобщенная структурная схема систем электросвязи. Компьютерная информация; системное, прикладное и специальное программное обеспечение; понятие «открытой» системы; модель взаимодействия элементов «открытых» систем, информационно-вычислительная система. Виды защищаемой информации: семантическая и

признаковая. Исторический аспект развития проблемы защиты информации. Развитие идей и концепций защиты информации.

5.2 Учебно-тематический план

Таблица 3

№ п/п	Наименование темы дисциплины	Трудоемкость в часах						Формы текущего контроля успеваемости
		Всего часов	Аудиторная работа				Самостоятельная работа	
			Общая	Лекции	Семинары, практические занятия	Занятия в интерактивной форме		
1.	Информационная безопасность в системе национальной безопасности	18	4	2	2		14	доклады рефераты презентации дискуссии
2.	Информационные уязвимости объектов	18	4	2	2	2	14	доклады рефераты презентации дискуссии
3.	Угрозы информационной безопасности и их источники	18	4	2	2	2	14	доклады рефераты презентации дискуссии
4.	Средства обеспечения информационной безопасности	18	8	4	4	4	10	доклады рефераты презентации дискуссии
5.	Риски информационной безопасности и проблема построения комплексной системы защиты информации	18	8	4	4	4	10	доклады рефераты презентации дискуссии
6.	Обработка и передача информации в вычислительных и управляющих системах и сетях связи, вопросы информационной безопасности и защиты информации для вычислительных и управляющих систем и сетей	18	8	4	4	4	10	доклады рефераты презентации дискуссии
	В целом по дисциплине	108	36	18	18	16	72	Эссе
	Итого в %					44%		

5.3 Содержание семинарских занятий

Таблица 4

Наименование тем (разделов) дисциплины	**Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 8,9 (указывается раздел и порядковый номер источника)**	**Формы проведения занятий**
Понятийный аппарат и основы терминологии информационной и национальной безопасности. Методики составления обзоров по вопросам обеспечения информационной безопасности по профилю своей деятельности.	• Понятийный аппарат и основы терминологии информационной и национальной безопасности. • Виды национальной безопасности и их краткая характеристика. • Системные связи информационной безопасности с другими видами национальной безопасности. Источники: 8.1, 8.2, 8.3, 8.9, 8.10, 8.13	Доклады, презентации, обсуждение в группе, опрос, решение ситуационной задачи Учебное практическое задание: оформление перечня мероприятий по организации эксплуатации СКЗИ в финансово-банковских организациях Разработка приказа о перечне пользователей СКЗИ, оформление аппаратного журнала, журнала учета СКЗИ для обладателя, журнала учета СКЗИ для органа
Организационно-правовые и комбинированные информационные уязвимости.	• Антропогенные информационные уязвимости. • Техногенные информационные уязвимости. • Организационно-правовые и комбинированные информационные уязвимости. Источники: 8.9, 8.10, 8.11, 8.12, 8.14	Доклады, презентации, обсуждение в группе, опрос, решение ситуационной задачи Обсуждение особенностей криптографических алгоритмов. Ситуационная задача: выбор предпочтительного алгоритма криптографической защиты
Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация.	• Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация. • Угрозы конфиденциальности, целостности и доступности информации. • Системная классификация угроз. • Информационная война как	Доклады, презентации, обсуждение в группе, опрос, решение ситуационной задачи Учебное практическое задание (лабораторная работа) установка удостоверяющего центра на примере VipNet Administrator УКЦ Учебное практическое задание (лабораторная работа)

	высшая форма угрозы информационной безопасности. Источники: 8.9, 8.10, 8.11, 8.12, 8.14	функции и интерфейс удостоверяющего центра на примере VipNet Administrator УКЦ
Программно-аппаратные, криптографические и стеганографические средства защиты информации.	• Организационно-правовые средства обеспечения информационной безопасности, категорирование информации, допуск и доступ к информационным ресурсам. • Программно-аппаратные, криптографические и стеганографические средства обеспечения информационной безопасности. • Пассивные и активные средства противодействия техническим разведкам. • Защита информации от утечки по техническим каналам. Источники: 8.9, 8.10, 8.11, 8.12, 8.14	Доклады, презентации, обсуждение в группе, опрос, решение ситуационной задачи Учебное практическое задание (лабораторная работа) создание мастер-ключей и ключей для объектов VPN-сети Учебное практическое задание (лабораторная работа) управление ключевой структурой сети VipNet Учебное практическое задание (лабораторная работа) работа с сертификатами на примере удостоверяющего центра VipNet
Оценка рисков и организация управления процессом защиты информации.	• Стратегия и концепция защиты информации. • Формирование политики обеспечения информационной безопасности. • Проблема равнопрочного распределения ограниченных средств обеспечения информационной безопасности по информационным уязвимостям, методы и критерии ее решения. • Построение комплексной оптимальной системы защиты. • Оценка рисков и организация управления процессом защиты информации.	Доклады, презентации, обсуждение в группе, опрос, решение ситуационной задачи Учебное практическое задание (лабораторная работа) настройка резервного копирования и восстановления данных

	Источники: 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.12	
Актуальность проблемы; угрозы безопасности информации, обрабатываемой в компьютерных системах.	• Человек и информация; сообщения, сигналы; обобщенная структурная схема систем электросвязи. • Компьютерная информация; системное, прикладное и специальное программное обеспечение; понятие «открытой» системы; модель взаимодействия элементов «открытых» систем, информационно-вычислительная система. • Виды защищаемой информации: семантическая и признаковая. Исторический аспект развития проблемы защиты информации. • Развитие идей и концепций защиты информации. Источники: 8.9, 8.10, 8.11, 8.12	Доклады, презентации, обсуждение в группе, опрос, решение ситуационной задачи Эссе Учебное практическое задание (лабораторная работа) настройка резервного копирования и восстановления данных

6 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1 Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Информационная безопасность в системе национальной безопасности	• Виды национальной безопасности и их краткая характеристика.	• работа с учебной, научной и справочной литературой; • конспект; • подготовка докладов по теме; • подготовка презентаций по теме;

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
		• выполнение учебного задания
Информационные уязвимости объектов	• Антропогенные информационные уязвимости. • Техногенные информационные уязвимости. • Организационно-правовые и комбинированные информационные уязвимости.	• работа с учебной, научной и справочной литературой; • конспект; • подготовка докладов по теме; • подготовка презентаций по теме; • выполнение учебного задания
Угрозы информационной безопасности и их источники	• Угрозы конфиденциальности, целостности и доступности информации. • Информационная война как высшая форма угрозы информационной безопасности.	• работа с учебной, научной и справочной литературой; • конспект; • подготовка докладов по теме; • подготовка презентаций по теме; • выполнение учебного задания
Средства обеспечения информационной безопасности	• Организационно-правовые средства обеспечения информационной безопасности, категорирование информации, допуск и доступ к информационным ресурсам. • Защита информации от утечки по техническим каналам.	• работа с учебной, научной и справочной литературой; • конспект; • подготовка докладов по теме; • подготовка презентаций по теме; • выполнение учебного задания
Риски информационной безопасности и проблема построения комплексной системы защиты информации	• Оценка рисков и организация управления процессом защиты информации.	• работа с учебной, научной и справочной литературой; • конспект; • подготовка докладов по теме; • подготовка презентаций по теме; • выполнение учебного задания
Обработка и передача информации в вычислительных и управляющих системах и	• Уязвимые места информационно-вычислительных и управляющих систем	• работа с учебной, научной и справочной литературой; • конспект; • подготовка докладов по теме;

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
сетях связи, вопросы информационной безопасности и защиты информации для вычислительных и управляющих систем и сетей	на предприятии.	• подготовка презентаций по теме; • выполнение учебного задания

6.2 Перечень вопросов, заданий, тем для подготовки к текущему контролю

Основные формы текущего контроля знаний:

- участие в дискуссиях по проблемным темам дисциплины;
- выступление с докладом по проблемным темам дисциплины;
- собеседование по теоретическим вопросам;
- решение ситуационных задач;
- выполнение учебных практических заданий (лабораторных работ);
- выполнение аудиторных самостоятельных работ, контрольных работ, обсуждение и анализ их результатов.

Перечень тем для подготовки эссе

1. Государственная система защиты информации в России
2. Стратегия национальной безопасности Российской Федерации
3. Современная защита информационной безопасности в России: проблемы и направления её развития
4. Государственная система защиты информации в России
5. Содержание правового режима информации
6. Понятие правового режима информации
7. Соотношение государственной и служебной тайн
8. Правовое регулирование международного информационного обмена

9. Преступления в информационной сфере
10. Соотношение служебной и коммерческой тайн
11. Правовое регулирование использования аналогов собственноручной подписи
12. Информационная безопасность общества
13. Информационная безопасность личности
14. Информационная безопасность государства
15. Правовой режим коммерческой тайны
16. Правовой режим персональных данных
17. Административно-правовая ответственность в информационной сфере
18. Уголовно-правовая ответственность в информационной сфере
19. Гражданско-правовая ответственность в информационной сфере
20. Правовая защита информации
21. Право граждан на доступ к информации
22. Право юридических лиц на получение информации
23. Информационная открытость органов государственной власти
24. Информационное обеспечение деятельности органов государственной власти
25. Правовой режим информации, составляющей государственную тайну
26. Информационное обеспечение деятельности правоохранительных органов
27. Защита коммерческой тайны фирмы
28. География киберпреступности: преступление и наказание
29. Особенности нормативно-правовой защиты кибернетической информации в нашей стране
30. Информационное противоборство в бизнесе: кто же реально управляет предприятием?
31. Защита информационной среды бизнеса от киберпреступлений

32. Что же защищает информационная безопасность в компании, или какие тайны страшнее
33. Безопасность как социальное явление: сущность и содержание
34. Можно ли говорить о том, что в РФ созданы безопасные условия для бизнеса?
35. Облачные вычисления: условия применения, проблемы внедрения и сопровождения
36. Обосновать критерии построения безопасного информационного общества
37. Профессиональная и служебная тайна в РФ
38. Wikileaks война с секретами
39. Загадочный биткоин: благо или всемирная угроза?
40. Меры государственного контроля в области обеспечения безопасности кибернетической информации
41. Что же защищает информационная безопасность в компании, или какие тайны страшнее
42. Импортозамещение и информационная безопасность бизнеса
43. Особенности нормативно-правовой защиты кибернетической информации в нашей стране
44. Информационная безопасность в социальных сетях
45. Специфика системы обеспечения экономической безопасности в Южной Корее и возможности использования зарубежного
46. Обеспечение безопасности промышленной среды с помощью Kaspersky Industrial Cybersecurity
47. В чем отличия обеспечения информационной безопасности в Российской Федерации от других стран
48. Источники угроз безопасности персональных данных
49. Понятия информации и информационных ресурсов в законодательстве

50. Место информационной безопасности в стратегии национальной безопасности Российской Федерации

Примерные тематики для дискуссий:

1. Информационная война как высшая форма угрозы информационной безопасности.
2. Антропогенные информационные уязвимости.
3. Техногенные информационные уязвимости.
4. Организационно-правовые и комбинированные информационные уязвимости.
5. Уязвимые места информационно-вычислительных и управляющих систем на предприятии.
6. Оценка рисков и организация управления процессом защиты информации.
7. Защита информации от утечки по техническим каналам.
8. Обеспечение информационной безопасности средствами антивирусной защиты.
9. Обеспечение информационной безопасности при использовании ресурсов сети Интернет.
10. Обеспечение информационной безопасности при использовании средств криптографической защиты информации.
11. Обеспечение информационной безопасности информационных технологических процессов.
12. Угрозы конфиденциальности, целостности и доступности информации.
13. Обработка персональных данных в организации.
14. Организация и функционирование службы информационной безопасности организации.

15. Организация реализации планов внедрения системы обеспечения информационной безопасности.
16. Организация обнаружения и реагирования на инциденты информационной безопасности.
17. Организация обеспечения непрерывности бизнеса и его восстановления после прерываний
18. Мониторинг информационной безопасности и контроль защитных мер.
19. Проведение аудита информационной безопасности.
20. Подходы к оценке рисков нарушения информационной безопасности.
21. Процедуры оценки рисков нарушения информационной безопасности.
22. Оценка рисков нарушения информационной безопасности
23. Основные задачи и функции службы информационной безопасности организаций
24. Расчет ресурсов информационной безопасности организации.
25. Основы определения затрат на информационную безопасность.
26. Определение размера целесообразных затрат на обеспечение безопасности информации.
27. Модель определения зон и средств защиты предприятия от угроз.
28. Модель распределения работы службы безопасности предприятия.
29. Прикладной информационный анализ.
30. Потребительский индекс.
31. Добавленная экономическая стоимость.
32. Исходная экономическая стоимость.
33. Управление портфелем активов.
34. Оценка действительных возможностей.
35. Метод жизненного цикла искусственных систем.
36. Функционально-стоимостной анализ.

37. Совокупная стоимость владения.
38. Экономическая эффективность обеспечения информационной безопасности организации.

Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических рекомендациях кафедры.

7 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций, формируемых в процессе освоения дисциплины

Перечень компетенций, формируемых в процессе освоения дисциплины содержится в разделе 2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.

7.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, владений

Примерный перечень заданий для проверки уровня сформированности компетенций в ходе зачета

1. Были ли в вашей практике случаи попыток несанкционированного получения информации, обрабатываемой в АС? Охарактеризуйте проявившийся в каждом конкретном случае канал несанкционированного доступа и оцените возможную уязвимость информации.
2. Какие вам известны подходы к классификации угроз безопасности информации? Сравните их между собой с точки зрения наибольшего соответствия практическим потребностям создания систем защиты информации.

3. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.
4. В чем, с вашей точки зрения, состоит опасность разработки и применения информационного оружия? Какие необходимо было бы применить меры международного характера в целях предотвращения информационных войн?
5. Каковы основные принципы защиты информации от несанкционированного доступа? В чем заключается суть каждого из них?
6. Представьте следующую ситуацию: министры внутренних дел и экономики имеют одинаковую (наивысшую) форму допуска и пытаются с помощью автоматизированной системы получить строго конфиденциальную информацию по вопросу расследования экономических преступлений. Каковы, на ваш взгляд, должны быть возможности их доступа к этой информации? Рассмотрите все возможные ситуации и последствия, к которым приведут принимаемые решения по доступу с точки зрения обеспечения безопасности информации.
7. Сравните различные известные вам модели защиты от несанкционированного доступа к информации.
8. Что можно сказать о взаимодействии уровней безопасности субъектов и объектов доступа для различных видов доступа, с которыми оперирует модель Белла – Ла Падула?
9. Дайте определения идентификации и аутентификации пользователей. В чем разница между этими понятиями?
10. Назовите основные способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным?
11. Приведите примеры известных вам систем аутентификации, построенных по принципу «пользователь имеет». Что вы можете

сказать о преимуществах и недостатках методов аутентификации пользователей пластиковых карт, широко используемых в банковской сфере?

12. Каковы основные характеристики устройств аутентификации? Сравните известные вам устройства по каждой из этих характеристик.
13. Какие основные методы контроля доступа используются в современных автоматизированных системах? Охарактеризуйте эти методы и рассмотрите их возможности для реализации автоматизированной системы ведения текущих счетов клиентов банка.
14. Охарактеризуйте процесс развития проблемы защиты информации в современных системах ее обработки.
15. Раскройте содержание разграничения доступа к информации с помощью монитора обращений.
16. Охарактеризуйте проблему определения предметной области информационной безопасности и дайте определения основным понятиям, используемым в этой сфере.
17. Раскройте содержание исторических этапов развития подходов к защите информации и обеспечению информационной безопасности.
18. Охарактеризуйте «вредительские» программы как один из видов угроз информационной безопасности.
19. Раскройте содержание модели разграничения доступа Лэмпсона – Грэхема – Деннинга.
20. Раскройте содержание принципов обоснованности доступа и персональной ответственности как основных принципов защиты от несанкционированного доступа.

21. В чем состоит суть принципов достаточной глубины контроля и разграничения потоков информации как основных принципов защиты информации от несанкционированного доступа?
22. Раскройте содержание принципов чистоты повторно используемых ресурсов и целостности средств защиты как основных принципов защиты информации от несанкционированного доступа.
23. Раскройте основные особенности известных вам методов аутентификации с использованием индивидуальных физиологических характеристик пользователей.
24. Рассмотрите основные методы повышения стойкости парольных систем аутентификации пользователей автоматизированных систем.
25. Что изучают криптография, криптоанализ и криптология? Дайте определения этим наукам.
26. Какие методы криптографического закрытия информации вы знаете? В чем разница между шифрованием и кодированием?
27. Объясните, что представляет собой стеганография?
28. Расскажите об особенностях симметричных и несимметричных шифров. Попробуйте привести примеры этих способов шифрования.
29. Объясните, почему основными требованиями, предъявляемыми к криптосистемам, являются наличие очень большого числа возможных ключей и равная вероятность их генерации.
30. От каких основных свойств криптографических алгоритмов зависит, на ваш взгляд, стойкость криптосистемы?
31. В чем принципиальное различие оценки стойкости криптосистемы с использованием теории информации и теории вычислительной сложности?
32. Какие основные способы шифрования вы знаете? Каковы их преимущества и недостатки?

33. Опишите наиболее известный алгоритм шифрования DES. Какие из основных методов шифрования использованы в этом алгоритме?
34. Каковы основные особенности криптосистем с общедоступным ключом?
35. Раскройте основное содержание алгоритма электронной цифровой подписи.
36. Какие методы распределения ключей в криптографических системах с большим числом абонентов вы знаете? Охарактеризуйте основные особенности децентрализованных и централизованных систем.
37. Опишите последовательность установления связи и передачи сообщений в централизованных системах распределения ключей шифрования с центром трансляции ключей и с центром распределения ключей.
38. В каких случаях применяются криптографические методы защиты информации непосредственно в ЭВМ?
39. Дайте определение компьютерного вируса как саморепродуцирующейся программы. Приведите примеры известных вам случаев заражения компьютеров вирусами.
40. Попробуйте изобразить структуру компьютерного вируса в виде программы, написанной на псевдоязыке.
41. Охарактеризуйте основные фазы, в которых может существовать компьютерный вирус.
42. Охарактеризуйте известные вам основные классы антивирусных программ. В чем смысл комплексного применения нескольких программ?
43. Каковы, на ваш взгляд, должны быть основные правила работы с компьютером, предупреждающие возможное заражение его вирусами?

44. Охарактеризуйте перспективные методы защиты компьютеров от программ-вирусов.
45. Рассмотрите возможности вирусного подавления как одной из форм радиоэлектронной борьбы.
46. Каковы основные механизмы внедрения компьютерных вирусов в поражаемую систему?
47. Раскройте содержание комплексной стратегии защиты, ориентированной на противодействие возможному вирусному подавлению.
48. Дайте определение понятию «технический канал утечки информации». Назовите основные виды технических каналов.
49. Какой, по вашему мнению, технический канал утечки информации можно отнести к наиболее часто используемым техническими разведками для получения конфиденциальной информации? Раскройте особенности этого канала.
50. Дайте классификацию источников утечки информации по техническим каналам.
51. Что такое основные и вспомогательные технические средства автоматизированной системы? Приведите примеры и рассмотрите возможности их использования в качестве технических каналов утечки информации.
52. Назовите известные вам методы и средства контроля акустической информации.
53. Охарактеризуйте методы контроля информации техническими средствами в каналах телефонной связи.
54. Назовите методы контроля информации, обрабатываемой средствами вычислительной техники.
55. Охарактеризуйте основные способы предотвращения утечки информации по техническим каналам.

56. Приведите известные вам методы защиты от утечки информации по акустическому каналу. Попробуйте сравнить их, используя критерий «эффективность/стоимость».
57. Охарактеризуйте существующие на сегодняшний день способы защиты информации в каналах связи.
58. Назовите методы и средства защиты информации от утечки по побочному электромагнитному каналу.
59. С чем, по вашему мнению, связана необходимость организационно-правового обеспечения защиты информации? в чем заключается специфика этого обеспечения применительно к информации, обрабатываемой в автоматизированных системах?
60. Охарактеризуйте задачи, решаемые организационно-правовым обеспечением защиты информации в АС. Выделите особенности, связанные с «электронной» формой представления информации в АС.
61. Сформулируйте основные направления развития организационно-правового обеспечения защиты информации в зарубежных странах. Назовите известные вам законодательные акты зарубежных стран в области регулирования процессов информатизации и обеспечения безопасности информации.
62. Что вы знаете из истории развития организационно-правового обеспечения зашиты информации в СССР и Российской Федерации? Охарактеризуйте современное состояние отечественной законодательной базы в области информатизации и защиты информации.
63. Сформулируйте основные положения Закона Российской Федерации «Об информации, информационных технологиях и защите информации». Какие еще вы знаете российские законодательные акты в этой области?

64. Сформулируйте основные подходы к разработке организационно-правового обеспечения защиты информации. Раскройте содержание структуры этого обеспечения.
65. Сформулируйте основные требования, предъявляемые к системе стандартизации в области защиты информации. Назовите известные вам системы стандартов в этой области, принятые в России и за рубежом.
66. Опишите систему органов государственного управления Российской Федерации, осуществляющих управление и координацию деятельности в области защиты информации и обеспечения информационной безопасности.
67. Изложите кратко основное содержание деятельности ФСТЭК России в области обеспечения информационной безопасности.
68. Почему, на ваш взгляд, действительно эффективная защита информации может быть обеспечена только при комплексном системном подходе к решению этой проблемы? В чем заключается комплексность? Каким требованиям должна удовлетворять концепция комплексной защиты?
69. Сформулируйте основные концептуальные положения теории защиты информации.
70. Раскройте содержание функции защиты информации. Какие из функций образуют полное множество функций защиты?
71. Сформулируйте определение задачи защиты информации и попытайтесь назвать десять классов задач, образующих репрезентативное множество задач защиты.
72. Приведите наиболее распространенную на сегодняшний день классификацию средств защиты информации. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств защиты информации?

73. Дайте определение системы защиты информации и сформулируйте основные концептуальные требования, предъявляемые к ней.
74. Раскройте содержание концепции управления системой защиты информации. Каковы ее особенности по сравнению с общей концепцией управления системами организационно-технологического типа?

7.3 Соответствующие приказы, распоряжения ректората о контроле уровня освоения дисциплин и сформированности компетенций студентов.

Приказ от 23.03.2017 №0557/о «Об утверждении Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по программам бакалавриата и магистратуры в Финансовом университете».

8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Нормативные акты

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»
2. Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне»
3. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»
4. СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»
5. СТО БР ИББС-1.2 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций

банковской системы Российской Федерации требованиям СТО БР ИББС-1.0»

6. Рекомендации в области стандартизации Банка России РС БР ИББС-2.0 «Обеспечение информационной безопасности организаций БС РФ. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0»
7. СТО БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности»
8. РС БР ИББС-2.7-2015 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Ресурсное обеспечение информационной безопасности

а) основная литература:

9. Хорев П.Б. Программно-аппаратная защита информации [Электронный ресурс]: учебное пособие / П.Б. Хорев. - Москва: Форум: НИЦ ИНФРА-М, 2015. - 352 с. – Режим доступа: http://znanium.com.
10. Гришина Н.В. Информационная безопасность предприятия [Электронный ресурс]: учебное пособие / Н.В.Гришина. - Москва: Форум: НИЦ ИНФРА-М, 2017. - 239 с. – Режим доступа: http://znanium.com.

б) дополнительная литература:

11. Баранова Е. К. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие / Е. К.Баранова, А. В. Бабаш. - Москва: ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 336 с. - Режим доступа: http://znanium.com.

12. Ищейнов В.Я. Основные положения информационной безопасности [Электронный ресурс]: учебное пособие / В.Я.Ищейнов, М.В.Мецатунян. - Москва: Форум, НИЦ ИНФРА-М, 2018. - 208 с. - Режим доступа: http://znanium.com.
13. Жук А.П. Защита информации [Электронный ресурс]: учебное пособие / А.П. Жук [и др.]. - Москва: РИОР: ИНФРА-М, 2018. - 392 с. - Режим доступа: http://znanium.com.
14. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс]: учебное пособие / В.Ф. Шаньгин. - Москва: ИД ФОРУМ: НИЦ ИНФРА-М, 2018. - 416 с. - Режим доступа: http://znanium.com.

9 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Сайт Федеральной службы по техническому и экспортному контролю www.fstec.ru
2. Справочная правовая система КонсультантПлюс. http://www.consultant.ru/
3. Аналитический ресурс по информационной безопасности AntiMalware: https://www.anti-malware.ru
4. Научная электронная библиотека Киберленинка: https://cyberleninka.ru
5. Электронная библиотека Финансового университета (ЭБ) http://elib.fa.ru/
6. Электронно-библиотечная система BOOK.RU http://www.book.ru
7. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» http://biblioclub.ru/
8. Электронно-библиотечная система Znanium http://www.znanium.com

9. Электронно-библиотечная система издательства «ЮРАЙТ» https://www.biblio-online.ru/
10. Электронно-библиотечная система издательства «Лань» https://e.lanbook.com/
11. Деловая онлайн-библиотека Alpina Digital http://lib.alpinadigital.ru/
12. Научная электронная библиотека eLibrary.ru http://elibrary.ru
13. Национальная электронная библиотека http://нэб.рф/
14. Электронная библиотека диссертаций Российской государственной библиотеки https://dvs.rsl.ru/

10 Методические указания для обучающихся по освоению дисциплины

Рекомендации по освоению дисциплины приведены в «Методических рекомендациях для студентов бакалавриата по освоению дисциплин образовательных программ высшего образования», утвержденных распоряжением Финуниверситета от 14 мая 2014 г. № 256.

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

Комплект лицензионного программного обеспечения:

- Windows, Microsoft Office
- антивирус ESET Endpoint Security

Современные профессиональные базы данных и информационные справочные системы:

- Консультант Плюс
- Гарант

Сертифицированные программные и аппаратные средства защиты информации.

Не используются.

12 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Занятия по дисциплине проводятся в аудиториях, оборудованных мультимедийными комплексами, компьютерами с выходом в Интернет.