ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

Методические рекомендации для самостоятельной работы обучающихся по дисциплине

Б1.В.08 Безопасность информации в банковских системах

Направление подготовки 10.03.01 Информационная безопасность

Профиль подготовки Безопасность автоматизированных систем

Квалификация выпускника бакалавр

Форма обучения очная

СОДЕРЖАНИЕ

1. ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1.1. Организационно-методические данные дисциплины

№ п.п.	Наименование темы	Общий объем часов по видам самостоятельной работы				
		подготовка курсового проекта (работы)	подготовка реферата/эссе	индивидуальные домашние задания (ИДЗ)	самостоятельное изучение вопросов (СИВ)	подготовка к занятиям (ПкЗ)
1	2	3	4	5	6	7
2	Основные положения концепции безопасности банка	-	-	-	8	20
3	Политика безопасности	-	-	-	8	20
4	Классификация угроз. Матрица угроз	-	-	-	8	20
5	Мошенничество. Виды мошенничества	-	-	-	8	20
6	Общие принципы обеспечения безопасности в автоматизированных банковских системах	-	-	-	6	6
7	Особенности обеспечения информационной безопасности в различных автоматизированных банковских системах	-	-	-	6	4
8	Организация и функционирование системы безопасности банка	-	-	-	6	6
9	Управление деятельностью службы безопасности банка	-	-	-	6	4

2. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО САМОСТОЯТЕЛЬНОМУ ИЗУЧЕНИЮ ВОПРОСОВ

2.1 Основные положения концепции безопасности банка (8 часов)

При изучении вопроса необходимо обратить внимание на следующие особенности.

Законодательные и правовые основы защиты компьютерной информации и информационных технологий

2.2 Политика безопасности (8 часов)

При изучении вопроса необходимо обратить внимание на следующие особенности.

Криптология, криптография и криптоанализ.

2.3 Классификация угроз. Матрица угроз (8 часов)

При изучении вопроса необходимо обратить внимание на следующие особенности.

В чем заключаются традиционные методы шифрования, являющиеся базовыми для современных производных шифров с секретным ключом. В чем заключается правило Кирхгоффа. Какой шифр считается стойким. В чем заключаются принципы блочного шифрования. В чем заключаются принципы поточного шифрования

.

2.4 Мошенничество. Виды мошенничества (8 часов)

При изучении вопроса необходимо обратить внимание на следующие особенности.

Основные преимущества и недостатки симметричных и асимметричных криптосистем.

2.5 Общие принципы обеспечения безопасности в автоматизированных банковских системах (6 часов)

При изучении вопроса необходимо обратить внимание на следующие особенности.

Базовый принцип доступа. Применяемая модуляция. Криптоалгоритмы.

2.6 Особенности обеспечения информационной безопасности в различных автоматизированных банковских системах (6 часов)

При изучении вопроса необходимо обратить внимание на следующие особенности.

Субъектно-объектный взгляд. Пространство состояний системы.

2.7 Организация и функционирование системы безопасности банка (6 часов)

При изучении вопроса необходимо обратить внимание на следующие особенности.

Наборы данных VSAM. Конструктор схемы компоновки данных.

2.8 Управление деятельностью службы безопасности банка (6 часов)

При изучении вопроса необходимо обратить внимание на следующие особенности.

Понятие компьютерной сети. Основные компоненты компьютерной сети. Классификация компьютерных сетей. Локальная сеть. Региональные сети

3. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ЗАНЯТИЯМ

3.1 Основные положения концепции безопасности банка

При подготовки к занятию необходимо обратить внимание на следующие моменты:

- Основные положения концепции безопасности банка.
- Федеральный закон «О Центральном банке Российской Федерации (Банке России)».

3.2 Политика безопасности

При подготовки к занятию необходимо обратить внимание на следующие моменты:
Криптология, криптография и криптоанализ.

3.3 Классификация угроз. Матрица угроз

При подготовки к занятию необходимо обратить внимание на следующие моменты:
В чем заключаются традиционные методы шифрования, являющиеся базовыми для современных производных шифров с секретным ключом. В чем заключается правило Кирхгоффа. Какой шифр считается стойким. В чем заключаются принципы блочного шифрования. В чем заключаются принципы поточного шифрования.

3.4 Мошенничество. Виды мошенничества

При подготовки к занятию необходимо обратить внимание на следующие моменты:
Основные преимущества и недостатки симметричных и асимметричных криптосистем.

3.5 Общие принципы обеспечения безопасности в автоматизированных банковских системах

При подготовки к занятию необходимо обратить внимание на следующие моменты:
Базовый принцип доступа. Применяемая модуляция. Криптоалгоритмы.

3.6 Особенности обеспечения информационной безопасности в различных автоматизированных банковских системах При подготовки к занятию необходимо обратить внимание на следующие моменты:
Субъектно-объектный взгляд. Пространство состояний системы.

3.7 Организация и функционирование системы безопасности банка

При подготовки к занятию необходимо обратить внимание на следующие моменты:
Наборы данных VSAM. Конструктор схемы компоновки данных.

3.8 Управление деятельностью службы безопасности банка

При подготовки к занятию необходимо обратить внимание на следующие моменты:

Понятие компьютерной сети. Основные компоненты компьютерной сети. Классификация компьютерных сетей. Локальная сеть. Региональные сети

4.Темы курсовых работ (проектов)

1. Угрозы безопасности: понятие, виды, классификация.
2. Требования, предъявляемые к системе защиты АБС, характеристики, обеспечивающие безопасность АБС.
3. Электронная цифровая подпись: понятие и назначение, компоненты.
4. Банковская информационная система.
5. Компьютерные сети: понятие, классификация, защита.
6. Угрозы безопасности: понятие, виды, классификация.
7. Принципы оперативной аналитической обработки данных OLAP.
8. Концептуальную модель хранилища данных.
9. Система электронных расчетов.
10. Виды межбанковских расчетов.
11. Важность и сложность проблемы информационной безопасности.
12. Правовая защита.
13. Организационная защита.
14. Инженерно техническая защита.
15. Физические средства защиты.
16. Аппаратные средства защиты.
17. Программные средства защиты.
18. Криптографические средства защиты
19. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации

20. Ответственность за нарушения в сфере информационной безопасности.

21. Правовые основы предоставления сведений конфиденциального характера.

22. Противодействие несанкционированному доступу к источникам конфиденциальной информации.

23. Методы и модели оценки уязвимости информации.

24. Рекомендации по использованию моделей оценки уязвимости информации.

25. Требования к безопасности информационных систем в России.

26. Требования к безопасности информационных систем в США («Оранжевая книга»)

27. Классы защищенности средств вычислительной техники от несанкционированного доступа.

28. Факторы, влияющие на требуемый уровень защиты информации.

29. Критерии оценки безопасности информационных технологий.