Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ
(наименование дисциплины)

Направление подготовки 10.03.01 «Информационная безопасность»
Профиль / программа подготовки Комплексная защита объектов информатизации
Уровень высшего образования бакалавриат
Форма обучения очная

Семестр	Трудоемкость зач. ед./ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
4	5/180	36		18	81	Экзамен (45ч)
5	5/180	36		36	72	Экзамен (36ч)
6	5/180	18		36	81	Экзамен (45ч), КР
Итого	16/576	90		90	234	Экзамен (126ч), КР

Владимир 2018

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Безопасность информационных систем» являются обеспечение подготовки студентов в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность», ознакомление студентов с технологиями безопасного с точки зрения возможности утечки информации интеллектуального анализа больших информационных массивов посредством и с помощью информационно-аналитических систем.

Задачами освоения дисциплины «Безопасность информационных систем» является:

- изучение основных положений, понятий и категорий, связанных с обеспечением безопасности информационно-аналитических систем;
- изучение основных подходов к выполнению безопасного интеллектуального анализа больших массивов данных посредством современных информационных технологий;
- формирование навыков противодействия несанкционированному проникновению в защищаемые информационные и аналитические системы с использованием современных информационно-вычислительных средств и систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО БАКАЛАВРИАТА

Данная дисциплина относится к базовой части Блока Б1 (код Б1.Б.03). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ.

Дисциплина изучается на 2 и 3 курсах, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по направлению 10.03.01 «Информационная безопасность» по курсам «Информатика», «Основы информационной безопасности», «Безопасность операционных систем», «Криптографические методы защиты информации», «Базы данных и экспертные системы», «Программно-аппаратные средства защиты информации». Курс тесно взаимосвязан с другими дисциплинами.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины специалист должен обладать следующими профессиональными компетенциями:

ПК- 3 - способностью осуществлять сбор, изучение, анализ и обобщение научно-технической информации, нормативных и методических материалов в области технологий информационно-аналитической деятельности и специальных ИАС, в том числе средств обеспечения их информационной безопасности;

ПК- 1 - способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) **Знать:** - активные и пассивные методы сбора информации; - информационные технологии в системе информационно-аналитического обеспечения безопасности; -- базовые криптографические протоколы и основные требования к ним; - механизмы реализации атак в компьютерных сетях; - защитные механизмы и средства обеспечения сетевой безопасности; - основные методы организационного обеспечения информационной безопасности специальных АИС; - области применения экспертных систем и этапы их проектирования; - методологические основы, методы и средства построения распределенных специальных АИС; - нормативную базу, регламентирующую создание и эксплуатацию специальных АИС; - принципы эксплуатации и сопровождения АИС (ПК-3; ПК-1).
2) **Уметь:** - составлять перечень сведений, содержащих коммерческую тайну; - использовать организационные, правовые и программно-аппаратные методы защиты информации; - решать задачи построения и эксплуатации распределенных автоматизированных систем обработки данных; - проектировать и сопровождать типовые специальные АИС, локальные сети; - устанавливать корреспондентские отношения с источниками информации, включая

взаимодействие с вычислительными системами и базами данных в телекоммуникационном режиме и работу в глобальных компьютерных сетях; - применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; - разрабатывать частные политики безопасности компьютерных систем, в том числе, политики управления доступом и информационными потоками (ПК-3; ПК-1).

3) Владеть: - навыками работы с имеющимися на рынке информационно-аналитическими системами; - навыками обработки информации в специальных АИС; - навыками выбора и обоснования критериев эффективности функционирования специальных АИС; - навыками конфигурирования локальных сетей, реализации сетевых протоколов с помощью программных средств; - методами и средствами выявления угроз безопасности компьютерным системам (ПК-3; ПК-1).

У обучаемых в процессе изучения дисциплины должны вырабатываться дополнительные компетенции, с учетом требований работодателей:

- способность применять навыки обеспечения защиты информации в информационных и аналитических системах.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 15 зачетных единиц, 540 часов.

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости *(по неделям семестра),* форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы,	СРС	КП / КР		
1.	Архитектура современных информационных и аналитических систем.	4	1-2	4		2		9		4/66%	
2.	Уязвимости и угрозы современных информационных и аналитических систем.	4	3-4	4		2		9		4/66%	
3.	Методы обеспечения ИБ информационных и аналитических систем	4	5-6	4		2		9		4/66%	Рейтинг-контроль №1
4.	Протоколы идентификации, аутентификации и учета	4	7-8	4		2		9		4/66%	
5.	Методы локальной аутентификации	4	9-10	4		2		9		4/66%	
6.	Протоколы идентификации и аутентификации современных информационных и аналитических системах.	4	11-12	4		2		9		4/66%	Рейтинг-контроль №2
7.	Протокол TACACS	4	13-14	4		2		9		4/66%	
8.	Протокол RADIUS.	4	15-16	4		2		9		4/66%	
9.	Управление доступом в хранилищах данных	4	17-18	4		2		9		4/66%	Рейтинг-контроль №3
Всего по 4 семестру:				36		18		81		36/66%	Экзамен (45ч)
10	Иерархия прав доступа. Виды привилегий.	5	1-2	4		4		8		4/50%	
11	Организация безопасного межсетевого взаимодействия	5	3-4	4		4		8		4/50%	
12	Защита удаленного доступа в АИС.	5	5-6	4		4		8		4/50%	Рейтинг-контроль №1
13	Организация защищенного удаленного доступа в информационных и аналитических системах.	5	7-8	4		4		8		4/50%	
14	Протоколы защищенного удаленного доступа.	5	9-10	4		4		8		4/50%	
15	Управление криптоключами в информационных и аналитических системах	5	11-12	4		4		8		4/50%	Рейтинг-контроль №2
16	Цифровая подпись. Сертификат цифровой подписи.	5	13-14	4		4		8		4/50%	
17	Инфраструктура управления открытыми ключами PKI	5	15-16	4		4		8		4/50%	

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости *(по неделям семестра),* форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы,	СРС	КП / КР		
18	Стандарты Public-Key Cryptography	5	17-18	4		4		8		4/50%	Рейтинг-контроль №3
Всего по 5 семестру:				36		36		72		36/50%	Экзамен (36ч)
19	Общие сведения по курсу; общие сведения по обычному и конфиденциальному делопроизводству; систематизации документов	6	1-2	2		4		9		2/33%	
20	Концепция безбумажной технологии управления	6	3-4	2		4		9		2/33%	
21	Проектирование и внедрение СЭД	6	5-6	2		4		9		2/33%	Рейтинг-контроль №1
22	Проектирование поведенческих моделей	6	7-8	2		4		9		2/33%	
23	Основные требования по защите информации (уровни конфиденциальности; основные виды угроз ИБ при использовании ЭД)	6	9-10	2		4		9		2/33%	
24	Требования по защите конфиденциальной информации при ЭД; межведомственный ЭД	6	11-12	2		4		9		2/33%	Рейтинг-контроль №2
25	Контроль и защита электронного документооборота	6	13-14	2		4		9		2/33%	
26	Криптопровайдеры; организация работ по защите конфиденциальной информации	6	15-16	2		4		9		2/33%	
27	Особенности защиты информации в СЭД; использование электронной подписи и признание ее действительности.	6	17-18	2		4		9		2/33%	Рейтинг-контроль №3
Всего по 6 семестру:				18		36		81	КР	18/33%	Экзамен (45ч)
ИТОГО:				90		90		240	КР	90/50%	Экзамен (45ч), Экзамен (36ч), Экзамен (45ч)

Содержание дисциплины «Безопасность информационных систем»

Раздел 1. Архитектура современных информационных и аналитических систем.

Раздел 2. Уязвимости и угрозы современных информационных и аналитических систем.

Раздел 3. Методы обеспечения ИБ информационных и аналитических систем

Раздел 4. Протоколы идентификации, аутентификации и учета в современных информационных и аналитических системах.

Раздел 5. Методы локальной аутентификации

Раздел 6. Протоколы идентификации и аутентификации современных информационных и аналитических системах.
Раздел 7. Протокол TACACS.
Раздел 8. Протокол RADIUS.
Раздел 9. Управление доступом в хранилищах данных информационных и аналитических систем.
Раздел 10. Иерархия прав доступа. Виды привилегий.
Раздел 11. Организация безопасного межсетевого взаимодействия в распределенных информационных и аналитических системах. IPSec
Раздел 12. Защита удаленного доступа в АИС.
Раздел 13. Организация защищенного удаленного доступа в информационных и аналитических системах.
Раздел 14. Протоколы защищенного удаленного доступа
Раздел 15. Управление криптоключами в информационных и аналитических системах.
Раздел 16.Цифровая подпись. Сертификат цифровой подписи.
Раздел 17. Управление криптоключами в информационных и аналитических системах. Инфраструктура управления открытыми ключами PKI
Раздел 18. Управление криптоключами в информационных и аналитических системах. Стандарты Public-Key Cryptography
Раздел 19. Введение (общие сведения по курсу; общие сведения по обычному и конфиденциальному делопроизводству; систематизации документов).
Раздел 20. Концепция безбумажной технологии управления (текущее законодательство в сфере электронного документооборота и СЭД/ECM; рынок систем электронного документооборота).
Раздел 21. Проектирование и внедрение СЭД (методология проектирования и внедрения СЭД; разграничение доступа; электронный регламент управления организацией).
Раздел 22. Проектирование поведенческих моделей (схемы данных, программ, алгоритмов, взаимодействия программ, ресурсов системы, EPC, IDEF, ebXML, BPSS, ADF, BPMN, UML ARIS и др.).
Раздел 23. Основные требования по защите информации (уровни конфиденциальности; основные виды угроз ИБ при использовании ЭД).
Раздел 24. Требования по защите конфиденциальной информации при ЭД; межведомственный ЭД; ЖЦ разработки защищенной информационной системы.
Раздел 25. Контроль и защита электронного документооборота (виды электронных подписей и принципы их использования).
Раздел 26. Криптопровайдеры; организация работ по защите конфиденциальной информации.
Раздел 27. Особенности защиты информации в СЭД; использование электронной подписи и признание ее действительности.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины предполагает не только запоминание и понимание, но и анализ, синтез, рефлексию, формирует универсальные умения и навыки, являющиеся основой становления бакалавра по направлению 10.03.01 «Информационная безопасность».

Для реализации компетентностного подхода предлагается интегрировать в учебный процесс интерактивные образовательные технологии, включая информационные и коммуникационные технологии (ИКТ), при осуществлении различных видов учебной работы:

- учебную дискуссию;
- электронные средства обучения (слайд-лекции, электронные тренажеры, компьютерные тесты);
- дистанционные (сетевые) технологии.

Как традиционные, так и лекции инновационного характера могут сопровождаться компьютерными слайдами или слайд-лекциями. Основное требование к слайд-лекции – применение динамических эффектов (анимированных объектов), функциональным назначением которых является наглядно-образное представление информации, сложной для понимания и осмысления студентами, а также интенсификация и диверсификация учебного процесса.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью ОПОП направлению 10.03.01 «Информационная безопасность», особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом, в учебном процессе, они составляют не менее 30 процентов аудиторных занятий.

Занятия лекционного типа для соответствующих групп студентов согласно требованиям стандарта высшего образования не могут составлять более 55 процентов аудиторных занятий. Программа дисциплины соответствует данным требованиям.

Таким образом, применение интерактивных образовательных технологий придает инновационный характер практически всем видам учебных занятий, включая лекционные. При этом делается акцент на развитие самостоятельного, продуктивного мышления, основанного на диалогических дидактических приемах, субъектной позиции обучающегося в образовательном процессе. Тем самым создаются условия для реализации компетентностного подхода при изучении данной дисциплины.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Для текущего контроля успеваемости предлагается использование рейтинговой системы оценки, которая носит интегрированный характер и учитывает успешность студента в различных видах учебной деятельности, степень сформированности у студента общекультурных и профессиональных компетенций.

Примерный перечень заданий для текущих контрольных мероприятий:

Вопросы рейтинг-контроля №1 семестр 4:

- Современные уязвимости программного обеспечения информационных и аналитических систем;
- Вредоносное программное обеспечение и программные средства сетевых атак
- Методы и средства защиты информационных и аналитических систем;
- Задачи, решаемые современными средствами идентификации и аутентификации в информационных и аналитических системах;
- Характеристики AAA.
- Конфигурирование локальной AAA аутентификации с CLI на устройствах Cisco
- Конфигурирование распределенной AAA аутентификации с CLI на устройствах Cisco

Вопросы рейтинг-контроля №2 семестр 4:

- Протокол TACACS+. Задачи и характеристики протокола

- Протокол RADIUS. Задачи и характеристики протокола
- Аутентификация средствами протокола TACACS+. Конфигурирование протокола на устройствах Cisco
- Аутентификация средствами протокола RADIUS. Конфигурирование протокола на устройствах Cisco
- Аутентификация с 802.1X
- Управление доступом в хранилищах данных информационных и аналитических систем.
- Иерархия прав доступа. Создание ролей.

Вопросы рейтинг-контроля №3 семестр 4:
- Виды привилегий. Операторы представления привилегий.
- Управление паролями в хранилищах данных информационных и аналитических систем. Операторы отмены привилегий
- Защита межсетевого взаимодействия в информационных и аналитических системах. Топологии виртуальных частных сетей.
- Управление доступом в хранилищах данных информационных и аналитических систем.
- Иерархия прав доступа. Создание ролей.
- Виды привилегий. Операторы представления привилегий.

Перечень вопросов к экзамену 4 семестр (промежуточной аттестации по итогам освоения дисциплины):

1. Современные угрозы информационной безопасности информационных и аналитических систем;
2. Современные уязвимости программного обеспечения информационных и аналитических систем;
3. Вредоносное программное обеспечение и программные средства сетевых атак
4. Методы и средства защиты информационных и аналитических систем;
5. Задачи, решаемые современными средствами идентификации и аутентификации в информационных и аналитических системах;
6. Характеристики AAA.
7. Конфигурирование локальной AAA аутентификации с CLI на устройствах Cisco
8. Конфигурирование распределенной AAA аутентификации с CLI на устройствах Cisco
9. Протокол TACACS+. Задачи и характеристики протокола
10. Протокол RADIUS. Задачи и характеристики протокола
11. Аутентификация средствами протокола TACACS+. Конфигурирование протокола на устройствах Cisco
12. Аутентификация средствами протокола RADIUS. Конфигурирование протокола на устройствах Cisco
13. Аутентификация с 802.1X
14. Управление доступом в хранилищах данных информационных и аналитических систем.
15. Иерархия прав доступа. Создание ролей.
16. Виды привилегий. Операторы представления привилегий.
17. Управление паролями в хранилищах данных информационных и аналитических систем. Операторы отмены привилегий
18. Защита межсетевого взаимодействия в информационных и аналитических системах. Топологии виртуальных частных сетей.
19. Защита межсетевого взаимодействия в информационных и аналитических системах. Топологии виртуальных частных сетей.

Вопросы рейтинг-контроля №1 семестр 5:
- Управление паролями в хранилищах данных информационных и аналитических систем. Операторы отмены привилегий
- Защита межсетевого взаимодействия в информационных и аналитических системах. Топологии виртуальных частных сетей.

- Защита межсетевого взаимодействия в информационных и аналитических системах. Топологии виртуальных частных сетей.
- Защита межсетевого взаимодействия в информационных и аналитических системах. Компоненты Remote-Access VPN
- Защита межсетевого взаимодействия в информационных и аналитических системах. Компоненты Site-to-Site VPN
- Защита межсетевого взаимодействия в информационных и аналитических системах. Протокол IPSec.

Вопросы рейтинг-контроля №2 семестр 5:

- Протокол IPSec.Обеспечение конфиденциальности в информационных и аналитических системах.
- Протокол IPSec.Обеспечение целостности в информационных и аналитических системах.
- Защита межсетевого взаимодействия в информационных и аналитических системах. Протокол AH. Особенности применения
- Защита межсетевого взаимодействия в информационных и аналитических системах. Протокол ESP. Особенности применения
- Команды и алгоритм конфигурирования Site-to-Site VPN на устройствах Cisco
- Команды и алгоритм конфигурирования Remote-Access VPN на устройствах Cisco

Вопросы рейтинг-контроля №3 семестр 5:

- Политики ISAKMP. Конфигурирование Pre-Shared Key
- Протоколы защищенного удаленного доступа в информационных и аналитических системах.
- Конфигурирование протоколов защищенного удаленного доступа в информационных и аналитических системах.
- Инфраструктура PKI. Задачи PKI
- Особенности применения ЭП в информационных и аналитических системах.
- Криптографические стандарты PKI
- Топологии PKI

Перечень вопросов к экзамену 5 семестр (промежуточной аттестации по итогам освоения дисциплины):

1. Защита межсетевого взаимодействия в информационных и аналитических системах. Компоненты Remote-Access VPN
2. Защита межсетевого взаимодействия в информационных и аналитических системах. Компоненты Site-to-Site VPN
3. Защита межсетевого взаимодействия в информационных и аналитических системах. Протокол IPSec.
4. Протокол IPSec.Обеспечение конфиденциальности в информационных и аналитических системах.
5. Протокол IPSec.Обеспечение целостности в информационных и аналитических системах.
6. Защита межсетевого взаимодействия в информационных и аналитических системах. Протокол AH. Особенности применения
7. Защита межсетевого взаимодействия в информационных и аналитических системах. Протокол ESP. Особенности применения
8. Команды и алгоритм конфигурирования Site-to-Site VPN на устройствах Cisco
9. Команды и алгоритм конфигурирования Remote-Access VPN на устройствах Cisco
10. Политики ISAKMP. Конфигурирование Pre-Shared Key
11. Протоколы защищенного удаленного доступа в информационных и аналитических системах.
12. Конфигурирование протоколов защищенного удаленного доступа в информационных и аналитических системах.
13. Инфраструктура PKI. Задачи PKI
14. Особенности применения ЭП в информационных и аналитических системах.

15. Криптографические стандарты PKI
16. Топологии PKI

Вопросы рейтинг-контроля №1 семестр 6:
1) Реквизиты документов в соответствии с ГОСТ 6.30-2003 «Унифицированная система организационно-распорядительной документации».
2) Правила обработки поступающих (входящих) документов.
3) Правила обработки отправляемых (исходящих) документов.
4) Классификация конфиденциальной информации.
5) Организация конфиденциального документооборота.
6) Формирование и оформление дел.
7) Номенклатура дел.
8) Подготовка документов к передаче на архивное хранение.
9) Особенности систематизации конфиденциальных документов.
10) Основные термины и определения электронного документооборота (ГОСТ Р 7.0.8-2013 «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения»).

Вопросы рейтинг-контроля №2 семестр 6:
1) Проектирования поведенческих моделей (EPC, IDEF, ebXML, BPSS, ADF, BPMN, UML ARIS и др.)
2) Основные виды угроз информационной безопасности при использовании электронного документооборота.
3) Основные требования и меры по защите конфиденциальной информации при электронном документообороте.
4) Особенности и основные требования защиты персональных данных.

Вопросы рейтинг-контроля №3 (дополнительно к вопросам 1 и 2 рейтинг-контроля) семестр 6:
1) Защита конфиденциальной информации при ее автоматизированной обработке.
2) Виды электронных подписей и принципы их использования. Использование электронной подписи.
3) Принципы технологии docflow, workfow.
4) Криптопровайдеры. Основные технологии, используемые при развёртывании удостоверяющих центров.
5) Типовые решения, реализующие возможность применения электронной подписи.
6) Системы электронного документооборота, сертифицированные на территории России.

Перечень вопросов к экзамену семестр 6 (промежуточной аттестации по итогам освоения дисциплины):
1. В чем заключается необходимость перехода к безбумажной технологии управления?
2. Каковы основные концепции перехода к безбумажной технологии управления?
3. Что такое экономическая система?
4. Какие подсистемы можно выделить в экономической системе?
5. Каков набор основных функций управления?
6. Что такое бизнес-процесс?
7. Какие классы бизнес-процессов характерны для экономических систем?
8. Что такое документ и его роль в процессах, протекающих в ЭС?
9. Что такое система документации и каковы основные признаки классификации документов?
10. Что такое документопоток и какие показатели оценки потоков информации используют при проектировании информационных систем?
11. Что такое документооборот, его связь с функциями управления и бизнес-процессами, типы документооборот.
12. Что такое служба СДОУ, ее роль в организации документооборота в экономической системе?

13. Какие функции выполняет СДОУ?
14. Что такое делопроизводство?
15. Какие типы документооборота курирует СДОУ?
16. Какие классы форм организации СДОУ вы знаете?
17. Что такое ОРД и какие классы ОРД по содержанию и структуре выделяют?
18. Каково структура типоых ОРД?
19. В чем особенности структуры неформализованных ОРД?
20. Каков состав операций процедуры составления типовых и неформализованных документов?
21. Каков состав операций процедуры приема-передачи для разных классов потоков информации?
22. Каково назначение процедуры контроля исполнения документов?
23. Каков состав операций процедуры контроля исполнения документов?
24. Какое назначение контрольно-регистрационной карточки?
25. Какова структура процедуры формирования дел и сдачи их в архив?
26. Что такое "Дело"?
27. Что такое "Номенклатура дел" и ее назначение?
28. Каков состав операций процедуры "Формирование дел и сдача их в архив"?
29. Каково назначение экономических информационных систем?
30. Какие типы подсистем можно выделить в ЭИС?
31. Каков состав функциональных подсистем характерен для ЭИС?
32. Что такое информационное обеспечение ЭИС и его состав?
33. Что такое программное обеспечение ЭИС и его состав?
34. Что такое техническое обеспечение ЭИС и его состав?
35. Что такое технологическое обеспечение ЭИС и его состав?
36. Что такое АРМ и какова его структура?
37. Какие классы ЭИС Вы знаете?
38. Что такое корпоративная ЭИС и каковы ее свойства?
39. Каково назначение ЭСУД и ее место в ЭИС?
40. Какие принципы построения ЭСУД Вы знаете?
41. Какие функциональные подсистемы можно выделить в ЭСУД?

Какими методами можно создавать и внедрять ЭСУД в ЭС?

Вопросы и задания для самостоятельной работы студентов на 4,5 и 6 семестра:

ТЕМЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ НА 4, 5 И 6 СЕМЕСТР

1. Общая структура информационных и аналитических систем.
2. Базовые информационные процессы в информационных и аналитических системах.
3. Аналитические системы безопасности: понятия и задачи
4. Современные методы защиты информации в информационных и аналитических системах;
5. Методики выявления основных угрозы безопасности информации, в информационных и аналитических системах;
6. Построение модели нарушителя в информационных и аналитических системах;
7. Защитные механизмы информационной безопасности информационных и аналитических системах;
8. Практика использования информационно-аналитические систем безопасности в профессиональной деятельности;
9. Направления и тенденции совершенствования в вопросах безопасности современных информационно-аналитических систем
10. Регламенты работы с информационно-аналитическими системами
11. Комплект положений, инструкций и других организационно-распорядительных документов для информационно-аналитических системам
12. организационные проблемы информационной безопасности информационно-аналитических систем
13. Технические проблемы информационной безопасности информационно-аналитических систем

14. Требования к организации и функционированию информационно-аналитических систем
15. Модельное представление информационно-аналитических систем
16. Защищенные каналы передачи информации. ESP в туннельном режиме. SSL
17. Защищенные каналы передачи информации. Протокол рукопожатия (SSL HP).
18. Честный обмен цифровыми подписями и его приложения. Схема Asokan - Slioup - Waidner

ВОПРОСЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ НА 4, 5 И 6 СЕМЕСТР

1. Общая структура информационных и аналитических систем.
2. Базовые информационные процессы в информационных и аналитических системах.
3. Аналитические системы безопасности: понятия и задачи
4. Современные методы защиты информации в информационных и аналитических системах;
5. Методики выявления основных угрозы безопасности информации, в информационных и аналитических системах;
6. Построение модели нарушителя в информационных и аналитических системах;
7. Защитные механизмы информационной безопасности информационных и аналитических системах;
8. Практика использования информационно-аналитические систем безопасности в профессиональной деятельности;
9. Направления и тенденции совершенствования в вопросах безопасности современных информационно-аналитических систем
10. Регламенты работы с информационно-аналитическими системами
11. Комплект положений, инструкций и других организационно-распорядительных документов для информационно-аналитических системам
12. организационные проблемы информационной безопасности информационно-аналитических систем
13. Технические проблемы информационной безопасности информационно-аналитических систем
14. Требования к организации и функционированию информационно-аналитических систем
15. Модельное представление информационно-аналитических систем
16. Защищенные каналы передачи информации. ESP в туннельном режиме. SSL
17. Защищенные каналы передачи информации. Протокол рукопожатия (SSL HP).
18. Честный обмен цифровыми подписями и его приложения. Схема Asokan - Slioup - Waidner
19. Решения в области ECM систем (Alfresco software, Box, EMC, Everteam, iBM, iManage, lexmark international, M-Files, Microsoft, open text, and springCM).
20. Методика IDEF0/SADT. Функциональная модель
21. Методики IDEF1 и IDEF1X. Информационная модель и модель данных
22. Методика IDEF2. Имитационная модель.
23. Методика IDEF3. Модель процессов
24. Универсальный язык UML моделирования сложных систем.
25. Описание бизнес-процессов с использованием обозначений BPMN.
26. Методология ARIS
27. Электронный регламент управления организацией.
28. Юридическая сила электронного документа.
29. Защита от вредоносных программ в СЭД.
30. Организация и защита электронного почтового взаимодействия.
31. Жизненный цикл разработки защищенной информационной системы.
32. Электронные архивы российских предприятий.
33. Разработка требований по организационной защите электронного документооборота внутри организации и при взаимодействии со сторонними организациями.
34. Проектирование системы электронного документооборота.

Перечень тем лабораторных работ 4 семестр:

Лабораторная работа №1. Управление правами доступа и разрешениями к создаваемым объектам БД подсистем управления данными информационных и аналитических систем;

Лабораторная работа №2. Установка и конфигурирование сервера RADIUS;
Лабораторная работа №3. Обеспечение защищенного административного доступа с применением AAA и RADIUS;

Перечень тем лабораторных работ 5 семестр:
Лабораторная работа №1. Практика конфигурирования AAA на маршрутизаторах Cisco;
Лабораторная работа №2. Практика конфигурирования site-to-site VPN;
Лабораторная работа №3. Практика конфигурирования защищенного доступа к удаленной сети.

Перечень тем лабораторных работ 6 семестр:
Лабораторная работа №1. Обеспечение безопасности информации в системах электронного документооборота встроенными средствами;
Лабораторная работа №2. Системы электронного документооборота и проблемы обеспечения безопасности информации в них;
Лабораторная работа №3. Криптографическая защита ЭДО;
Лабораторная работа №4. Организация защищенной электронной почты;

Перечень тем и заданий к курсовой работе 6 семестр:

Курсовая работа разделяется на две части: разработку приложения для обмена текстовыми сообщениями по сетям TCP/IP в защищенном исполнении и анализ защищенности этого приложения индивидуально по вариантам. В ходе разработки студент имеет право выбирать язык разработки и средства защиты из перечня предварительно им изученных (например, в ходе изучения дисциплины "Программирование").

Работу можно разбить на ряд этапов: - проектирование клиент-серверной архитектуры приложения; - разработка потоков, реализующих доступ к базе данных, пользовательский ввод-вывод, доступ к сокетам и сетевым интерфейсам; - реализация обмена информацией между потоками на базе синхронизированных структур данных; - реализация статической защиты, динамической защиты и контроля целостности; - тестирование и отладка; - статический анализ кода; - динамический анализ и отладка с целью обхода защиты; - тестирование на возможность обхода механизмов контроля целостности.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с. ISBN 978-5-8199-0411-4 Режим доступа: http://znanium.com/catalog.php?bookinfo=402686
2. Интеллектуальные системы защиты информации: учеб. пособие/ Васильев В.И. - 2-е изд., испр. и доп. - М.: Машиностроение, 2013. - http://www.studentlibrary.ru/book/ISBN9785942756673.html 172 с.
3. Информационная безопасность: защита и нападение / Бирюков А.А. - М. : ДМК Пресс, 2012. - http://www.studentlibrary.ru/book/ISBN9785940746478.html. 474 с.
4. Мишин Д.В. Анализ защищенности распределенных информационных систем. Идентификация ресурсов корпоративной сети передачи данных : практикум для вузов по направлению "Информационная безопасность" / Д. В. Мишин, Ю. М. Монахов ; Владимирский государственный университет (ВлГУ) .— Владимир : 2012 .— 94 с. ISBN 978-5-9984-0295-1.
5. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.: ISBN 978-5-8199-0331-5, Режим доступа: http://znanium.com/catalog.php?bookinfo=423927

б) Дополнительная литература:

1. Бизнес-безопасность / Кузнецов И.Н. - М. : Дашков и К, 2012. - http://www.studentlibrary.ru/book/ISBN9785394014383.html. 416 с.
2. Офисный шпионаж / Мелтон К., Пилиджан К., Сверчински Д. - М. : Альпина Паблишер, 2013. - http://www.studentlibrary.ru/book/ISBN9785916712070.html. 182 с.
3. Воронин А.А. Вычислительные сети : учебное пособие / А. А. Воронин ; Владимирский государственный университет (ВлГУ) .— Владимир : 2011 .— 87 с.
4. Основы информационных и телекоммуникационных технологий. Сетевые информационные технологии : учеб. пособие / В.Б. Попов. - М. : Финансы и статистика, 2015. - http://www.studentlibrary.ru/book/ISBN5279030139.html 224 с.
5. Введение в сетевые технологии: Элементы применения и администрирования сетей: учеб. пособие / С.В. Никифоров.- 2-е изд. - М. : Финансы и статистика, 2007. - http://www.studentlibrary.ru/book/ISBN9785279032808.html 224 с.

в) Периодические издания:

1. Журнал «Вопросы защиты информации». Режим доступа: http://i-vimi.ru/editions/detail.php?SECTION_ID=155/;
2. Журнал "Information Security/Информационная безопасность". Режим доступа: http://www.itsec.ru/insec-about.php.
3. Ежемесячный теоретический и прикладной научно-технический журнал «Информационные технологии». Режим доступа http://novtex.ru/IT/.
4. «Журнал сетевых решений/LAN» -Режим доступа: http://www.osp.ru/lan/current;
5. Электронный журнал «Корпоративные сети передачи данных» -Режим доступа: http://www.delpress.ru/

г) Программное обеспечение и Интернет-ресурсы:

1. Образовательный сервер кафедры ИЗИ.– Режим доступа: http://edu.izi.vlsu.ru
2. Информационная образовательная сеть.- Режим доступа: http://ien.izi.vlsu.ru
3. Внутривузовские издания ВлГУ.– Режим доступа: http://e.lib.vlsu.ru/
4. ИНТУИТ. Национальный открытый университет.– Режим доступа: http://www.intuit.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м2, оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м2, оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4, симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м2, оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор ST-031P «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, виброакустический генератор шума «Соната АВ 1М», имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокруст 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и виброакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3»,учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Xaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению 10.03.01 "Информационная безопасность ", направленность «Комплексная защита объектов информатизации»

Рабочую программу составил доц. кафедры ИЗИ к.т.н., Мишин Д.В.

(ФИО, подпись)

Рецензент
(представитель работодателя) к.т.н. Вертилевский Н.В. РАЦ ООО «ИнфоЦентр»
Заместитель руководителя.
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 1 от 30.08.18 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/

(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии по направлению 10.03.01 "Информационная безопасность ", направленность «Комплексная защита объектов информатизации»

Протокол № 1 от 30.08.18 года

Председатель комиссии д.т.н., профессор /М.Ю. Монахов/

(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/

(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/

(ФИО, подпись)