Лист 118, 119

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

УТВЕРЖДАЮ
Проректор по УУР
_____ А.А.Панфилов
«12» 02 2015 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Хранение и защита компьютерной информации

(наименование дисциплины)

Направление подготовки 15.04.04 "Автоматизация технологических процессов и производств"

Уровень высшего образования: академ. магистратура

Форма обучения очная

Семестр	Трудоемкость зач. ед,час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
2	2/72	-	18	18	36	зачет
Итого	2/72	-	18	18	36	зачет

Владимир 2015

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Нормативно-правовое обеспечение УМК дисциплины

- Федеральный закон от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;

- Приказ Минобрнауки России от 19.12.2013 № 1367 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры»;

- Письмо Минобрнауки России № АК-1666/05 от 24.06.2014 «Об установлении соответствий при утверждении новых перечней профессий, специальностей и направлений подготовки указанным в предыдущих перечнях профессий, специальностей и направлений подготовки»;

- Письмо Минобрнауки России № АК-1807 от 27.08.2013 «О подготовке кадров высшей квалификации»;

Целями освоения дисциплины «Хранение и защита компьютерной информации» являются обеспечение подготовки магистров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 15.04.04 "Автоматизация технологических процессов и производств". Формирование у магистрантов знаний и навыков в предметной области. Предмет курса - понятийный аппарат, а также сущность, теоретические, концептуальные, методологические аспекты и структура ИБ и защиты компьютерной информации. Дисциплина дает представления об основных математических и алгоритмических подходах, применяемых для хранения, передачи, исправления информации, представленной в двоичных кодах.

Задачами дисциплины являются: изучение понятийного аппарата в области ИБ; раскрытие базовых содержательных положений в области ИБ; ознакомление с основами математической теории криптологии; приобретение навыков в практическом использовании, постановке и решении задач шифрования информации; - понимание сути информационных процессов в криптографических системах; - применение компьютеров для решения задач шифрования и дешифрования.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина изучается на первом курсе, для грамотного использования полученных знаний в профессиональной деятельности, требуется изучение курсов «Компьютерные технологии автоматизации и управления»; «Компьютерные технологии автоматизации и управления». Знания, полученные в результате курса, пригодятся при написании магистерской диссертации.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ

В результате освоения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ПК-9 - способностью обеспечивать надежность и безопасность на всех этапах жизненного цикла продукции, выбирать системы экологической безопасности производства

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) ***Знать:*** базовый понятийный аппарат в области ИБ; виды и состав угроз информационной безопасности; принципы и общие методы обеспечения информационной безопасности; виды носителей защищаемой информации; виды уязвимости защищаемой информации; источники, виды и способы дестабилизирующего воздействия на защищаемую информацию; классификацию видов, методов и средств защиты информации; основные положения криптологии, вытекающие из теории симметричных и ассиметричных криптографических подходов, а также информационные критерии оценок функционирования криптографических систем.

2) ***Уметь:*** - выявлять угрозы информационной безопасности применительно к компьютерной информации; определять направления и виды защиты информации с учетом характера информации и задач по ее защите; применять современные технологии криптографии в задачах обработки информации;

3) ***Владеть:*** научно-технической терминологией; современными программными средствами защиты компьютерной информации

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа.

№ 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	Семинары	Практические занятия	Лабораторные работы	Контрольные работы, коллоквиумы	СРС	КП / КР		
1	Введение. Базовый понятийный аппарат в области ИБ и защиты компьютерной информации; Виды и состав угроз информационной безопасности. Принципы и общие методы обеспечения информационной безопасности компьютерной информации;	2	1-6			6	6		12		6/50%	Рейтинг контроль №1
2	Виды носителей защищаемой компьютерной информации; уязвимости систем обработки компьютерной информации; источники, виды и способы дестабилизирующего воздействия на компьютерную информацию;	2	7-12			6	6		12		6/50%	Рейтинг контроль №2
3	Виды, методы и средства защиты компьютерной информации; Основные положения криптологии. Симметричные и ассиметричные криптографические подходы.	2	13-18			6	6		12		6/50%	Рейтинг контроль №3
Всего						18	18		36		18/50%	Зачет

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины предполагает не только запоминание и понимание, но и анализ, синтез, рефлексию, формирует универсальные умения и навыки, являющиеся основой становления магистра по направлению 15.04.04 "Автоматизация технологических процессов и производств".

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 бакалаврами, а также интенсификация и диверсификация учебного процесса.

Удельный вес **занятий, проводимых в интерактивных формах**, определяется главной целью ОПОП по направлению 15.04.04 "Автоматизация технологических процессов и производств", особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом, в учебном процессе, они должны составлять **не менее 20% 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 СРС

Текущий контроль успеваемости – по результатам рейтинг-контроля, который проводится по установленному графику.

Темы лабораторных работ:

1. Составление досье с использованием интернет- ресурсов для оценки воздействия икт-технологий на неприкосновенность частной жизни
2. Количественная оценка стойкости парольной защиты
3. Управление локальными параметрами безопасности ОС Windows

Темы практических работ:

1. Классическая модель доступа ОС на базе Linux
2. Расширенная модель доступа ОС на базе Linux
3. Установка и настройка программного межсетевого экрана

Темы и вопросы по СРС

1. Основные понятия информационной безопасности. Субъекты информационных отношений;
2. Какая информация является предметом защиты?
3. Понятие доступности, целостности и конфиденциальности.
4. Понятие угрозы, атаки, уязвимости. Примеры Угроз;
5. Понятие угрозы, атаки, уязвимости. Примеры уязвимостей;

6. Понятие угрозы, атаки, уязвимости. Примеры Атак;
7. Источник угроз ИБ. Понятие нарушителя. Модель нарушителя;
8. Модель безопасности по ГОСТ 13335-1-2006;
9. Угроза ИБ. Источники угроз ИБ. Модель угроз ИБ;
10. Угрозы ИБ. Классификация угроз ИБ. Классификация по расположению источника. Классификация по активности АИС.
11. Угрозы ИБ. Классификация угроз ИБ. Классификация по размеру ущерба. Классификация по отношению к защищаемой информации.
12. Угрозы ИБ. Классификация угроз ИБ. Классификация по аспекту ИБ. Классификация по компонентам АИС.
13. Методы, меры обеспечения ИБ и средства ЗИ. Классификация методов, мер и средств ЗИ.
14. Методы, меры обеспечения ИБ и средства ЗИ. Основные методы обеспечения ИБ. Привести примеры
15. Методы, меры обеспечения ИБ и средства ЗИ. Правовые (законодательные) меры и средства защиты информации. Привести примеры. Достоинства и недостатки законодательных мер и средств ЗИ;
16. Методы, меры обеспечения ИБ и средства ЗИ. Морально-этические меры и средства защиты информации. Привести примеры. Достоинства и недостатки морально-этических мер и средств ЗИ.
17. Методы, меры обеспечения ИБ и средства ЗИ. Организационные меры и средства защиты информации. Привести примеры. Достоинства и недостатки организационных мер и средств ЗИ.
18. Методы, меры обеспечения ИБ и средства ЗИ. Физические меры и средства защиты информации. Привести примеры. Достоинства и недостатки физических мер и средств ЗИ.
19. Методы, меры обеспечения ИБ и средства ЗИ. Программные меры и средства защиты информации. Привести примеры. Достоинства и недостатки программных средств ЗИ.
20. Методы, меры обеспечения ИБ и средства ЗИ. Аппаратные меры и средства защиты информации. Привести примеры. Достоинства и недостатки аппаратных средств ЗИ.
21. Механизмы ЗИ. Идентификация и аутентификация. Требования к идентификации. Биометрическая идентификация;
22. Механизмы ЗИ. Идентификация и аутентификация. Требования к идентификации. Пароль. Атаки на пароли. Администрирование парольной системы;
23. Механизмы ЗИ. Идентификация и аутентификация. Требования к идентификации. Криптографические ключи. Карты памяти (memory card). Смарт-карты (smart card);
24. Количественная оценка стойкости парольной защиты
25. Техники управление доступом. Матрица контроля доступа. Список контроля доступа (ACL). Таблица разрешений;
26. Техники управление доступом. Доступ на основе контента. Доступ на основе контекста. Ограниченный интерфейс. Доступ на основе правил;
27. Управление доступом. Мандатное управление доступом (MAC);
28. Управление доступом. Модель Белла-ЛаПадула;
29. Управление доступом. Избирательное управление доступом (DAC);
30. Управление доступом. Ролевое управление доступом (RBAC);
31. Управление доступом. Классическая модель доступа ОС на базе Linux
32. Механизмы ЗИ. Протоколирование и аудит;
33. Механизмы ЗИ. Шифрование. Цели и задачи. Алгоритмы шифрования;
34. Симметричное шифрование. Достоинства и недостатки.
35. Асимметричное шифрование. Достоинства и недостатки.
36. Механизмы ЗИ. Контроль целостности. Хэш-функция;
37. Механизмы ЗИ. Экранирование. Межсетевые экраты;
38. Механизмы ЗИ. Туннелирование. VPN;
39. Механизмы ЗИ. Резервное копирование и восстановление;
40. Механизмы ЗИ. Защита от компьютерных вирусов;

41. Механизмы ЗИ. Обнаружение вторжений. IDS/IPS;
42. Механизмы ЗИ. Анализ защищенности;
43. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Общие сведения о категорировании информации в РФ;
44. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Права и обязанности обладателя информации по N 149-ФЗ;
45. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Общедоступная информация;
46. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Коммерческая тайна;
47. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Служебная тайна;
48. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Государственная тайна;
49. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Профессиональная и банковская тайна;
50. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Персональные данные;
51. Стандарты в области ИБ. Классификации стандартов. Критерии оценки доверенных компьютерных систем.
52. Стандарты в области ИБ. Классификации стандартов. Руководящие документы (РД) ФСТЭК России.
53. Стандарты в области ИБ. Классификации стандартов. X.800 «Архитектура безопасности для взаимодействия открытых систем».
54. Система стандартов по ЗИ (ССЗИ) РФ. ГОСТ Р 52069.0-2013.
55. Система стандартов по ЗИ (ССЗИ) РФ. Группа стандартов Защита информации. Уязвимости информационных систем.
56. Система стандартов по ЗИ (ССЗИ) РФ. Группа стандартов Защита информации. Техника защиты информации.
57. Система стандартов по ЗИ (ССЗИ) РФ. Группа стандартов Информационная технология. Криптографическая защита информации.
58. ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
59. ГОСТ Р ИСО/МЭК 27000-27006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента ИБ (СМИБ).
60. ГОСТ Р ИСО/МЭК 27033 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей.

Рейтинг-контроль №1
1. Основные понятия информационной безопасности. Субъекты информационных отношений;
2. Какая информация является предметом защиты?
3. Понятие доступности, целостности и конфиденциальности.
4. Понятие угрозы, атаки, уязвимости. Примеры Угроз;
5. Понятие угрозы, атаки, уязвимости. Примеры уязвимостей;
6. Понятие угрозы, атаки, уязвимости. Примеры Атак;
7. Источник угроз ИБ. Понятие нарушителя. Модель нарушителя;
8. Модель безопасности по ГОСТ 13335-1-2006;

Рейтинг-контроль №2
1. Угроза ИБ. Источники угроз ИБ. Модель угроз ИБ;
2. Угрозы ИБ. Классификация угроз ИБ. Классификация по расположению источника. Классификация по активности АИС.

3. Угрозы ИБ. Классификация угроз ИБ. Классификация по размеру ущерба. Классификация по отношению к защищаемой информации.
4. Угрозы ИБ. Классификация угроз ИБ. Классификация по аспекту ИБ. Классификация по компонентам АИС.
5. Методы, меры обеспечения ИБ и средства ЗИ. Классификация методов, мер и средств ЗИ.
6. Методы, меры обеспечения ИБ и средства ЗИ. Основные методы обеспечения ИБ. Привести примеры
7. Методы, меры обеспечения ИБ и средства ЗИ. Правовые (законодательные) меры и средства защиты информации. Привести примеры. Достоинства и недостатки законодательных мер и средств ЗИ;
8. Методы, меры обеспечения ИБ и средства ЗИ. Морально-этические меры и средства защиты информации. Привести примеры. Достоинства и недостатки морально-этических мер и средств ЗИ.
9. Методы, меры обеспечения ИБ и средства ЗИ. Организационные меры и средства защиты информации. Привести примеры. Достоинства и недостатки организационных мер и средств ЗИ.
10. Методы, меры обеспечения ИБ и средства ЗИ. Физические меры и средства защиты информации. Привести примеры. Достоинства и недостатки физических мер и средств ЗИ.
11. Методы, меры обеспечения ИБ и средства ЗИ. Программные меры и средства защиты информации. Привести примеры. Достоинства и недостатки программных средств ЗИ.
12. Методы, меры обеспечения ИБ и средства ЗИ. Аппаратные меры и средства защиты информации. Привести примеры. Достоинства и недостатки аппаратных средств ЗИ.
13. Механизмы ЗИ. Идентификация и аутентификация. Требования к идентификации. Биометрическая идентификация;
14. Механизмы ЗИ. Идентификация и аутентификация. Требования к идентификации. Пароль. Атаки на пароли. Администрирование парольной системы;
15. Механизмы ЗИ. Идентификация и аутентификация. Требования к идентификации. Криптографические ключи. Карты памяти (memory card). Смарт-карты (smart card);
16. Количественная оценка стойкости парольной защиты

Рейтинг-контроль №3

1. Техники управление доступом. Матрица контроля доступа. Список контроля доступа (ACL). Таблица разрешений;
2. Техники управление доступом. Доступ на основе контента. Доступ на основе контекста. Ограниченный интерфейс. Доступ на основе правил;
3. Управление доступом. Мандатное управление доступом (MAC);
4. Управление доступом. Модель Белла-ЛаПадула;
5. Управление доступом. Избирательное управление доступом (DAC);
6. Управление доступом. Ролевое управление доступом (RBAC);
7. Управление доступом. Классическая модель доступа ОС на базе Linux
8. Механизмы ЗИ. Протоколирование и аудит;
9. Механизмы ЗИ. Шифрование. Цели и задачи. Алгоритмы шифрования;
10. Симметричное шифрование. Достоинства и недостатки.
11. Асимметричное шифрование. Достоинства и недостатки.
12. Механизмы ЗИ. Контроль целостности. Хэш-функция:
13. Механизмы ЗИ. Экранирование. Межсетевые экраты;
14. Механизмы ЗИ. Туннелирование. VPN;
15. Механизмы ЗИ. Резервное копирование и восстановление:
16. Механизмы ЗИ. Защита от компьютерных вирусов;
17. Механизмы ЗИ. Обнаружение вторжений. IDS/IPS;
18. Механизмы ЗИ. Анализ защищенности;
19. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Общие сведения о категорировании информации в РФ;

20. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Права и обязанности обладателя информации по N 149-ФЗ;
21. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Общедоступная информация;
22. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Коммерческая тайна;
23. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Служебная тайна;
24. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Государственная тайна;
25. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Профессиональная и банковская тайна;
26. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Персональные данные;
27. Стандарты в области ИБ. Классификации стандартов. Критерии оценки доверенных компьютерных систем.
28. Стандарты в области ИБ. Классификации стандартов. Руководящие документы (РД) ФСТЭК России.
29. Стандарты в области ИБ. Классификации стандартов. X.800 «Архитектура безопасности для взаимодействия открытых систем».
30. Система стандартов по ЗИ (ССЗИ) РФ. ГОСТ Р 52069.0-2013.
31. Система стандартов по ЗИ (ССЗИ) РФ. Группа стандартов Защита информации. Уязвимости информационных систем.
32. Система стандартов по ЗИ (ССЗИ) РФ. Группа стандартов Защита информации. Техника защиты информации.
33. Система стандартов по ЗИ (ССЗИ) РФ. Группа стандартов Информационная технология. Криптографическая защита информации.
34. ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
35. ГОСТ Р ИСО/МЭК 27000-27006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента ИБ (СМИБ).
36. ГОСТ Р ИСО/МЭК 27033 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей.

Вопросы к зачету:
1. Основные понятия информационной безопасности. Субъекты информационных отношений;
2. Классификация ИР ИС;
3. Понятие доступности, целостности и конфиденциальности.
4. Понятие угрозы, атаки, уязвимости. Примеры Угроз;
5. Понятие угрозы, атаки, уязвимости. Примеры уязвимостей;
6. Понятие угрозы, атаки, уязвимости. Примеры Атак;
7. Источник угроз ИБ. Понятие нарушителя. Модель нарушителя;
8. Модель безопасности по ГОСТ 13335-1-2006;
9. Угроза ИБ. Источники угроз ИБ. Модель угроз ИБ;
10. Угрозы ИБ. Классификация угроз ИБ. Классификация по расположению источника. Классификация по активности АИС.
11. Угрозы ИБ. Классификация угроз ИБ. Классификация по размеру ущерба. Классификация по отношению к защищаемой информации.
12. Угрозы ИБ. Классификация угроз ИБ. Классификация по аспекту ИБ. Классификация по компонентам АИС.
13. Методы, меры обеспечения ИБ и средства ЗИ. Классификация методов, мер и средств ЗИ.

14. Методы, меры обеспечения ИБ и средства ЗИ. Основные методы обеспечения ИБ. Привести примеры
15. Методы, меры обеспечения ИБ и средства ЗИ. Правовые (законодательные) меры и средства защиты информации. Привести примеры. Достоинства и недостатки законодательных мер и средств ЗИ;
16. Методы, меры обеспечения ИБ и средства ЗИ. Морально-этические меры и средства защиты информации. Привести примеры. Достоинства и недостатки морально-этических мер и средств ЗИ.
17. Методы, меры обеспечения ИБ и средства ЗИ. Организационные меры и средства защиты информации. Привести примеры. Достоинства и недостатки организационных мер и средств ЗИ.
18. Методы, меры обеспечения ИБ и средства ЗИ. Физические меры и средства защиты информации. Привести примеры. Достоинства и недостатки физических мер и средств ЗИ.
19. Методы, меры обеспечения ИБ и средства ЗИ. Программные меры и средства защиты информации. Привести примеры. Достоинства и недостатки программных средств ЗИ.
20. Методы, меры обеспечения ИБ и средства ЗИ. Аппаратные меры и средства защиты информации. Привести примеры. Достоинства и недостатки аппаратных средств ЗИ.
21. Механизмы ЗИ. Идентификация и аутентификация. Требования к идентификации. Биометрическая идентификация;
22. Механизмы ЗИ. Идентификация и аутентификация. Требования к идентификации. Пароль. Атаки на пароли. Администрирование парольной системы;
23. Механизмы ЗИ. Идентификация и аутентификация. Требования к идентификации. Криптографические ключи. Карты памяти (memory card). Смарт-карты (smart card);
24. Количественная оценка стойкости парольной защиты
25. Техники управление доступом. Матрица контроля доступа. Список контроля доступа (ACL). Таблица разрешений;
26. Техники управление доступом. Доступ на основе контента. Доступ на основе контекста. Ограниченный интерфейс. Доступ на основе правил;
27. Управление доступом. Мандатное управление доступом (MAC);
28. Управление доступом. Модель Белла-ЛаПадула;
29. Управление доступом. Избирательное управление доступом (DAC);
30. Управление доступом. Ролевое управление доступом (RBAC);
31. Управление доступом. Классическая модель доступа ОС на базе Linux
32. Механизмы ЗИ. Протоколирование и аудит;
33. Механизмы ЗИ. Шифрование. Цели и задачи. Алгоритмы шифрования;
34. Симметричное шифрование. Достоинства и недостатки.
35. Асимметричное шифрование. Достоинства и недостатки.
36. Механизмы ЗИ. Контроль целостности. Хэш-функция;
37. Механизмы ЗИ. Экранирование. Межсетевые экраты;
38. Механизмы ЗИ. Туннелирование. VPN;
39. Механизмы ЗИ. Резервное копирование и восстановление;
40. Механизмы ЗИ. Защита от компьютерных вирусов;
41. Механизмы ЗИ. Обнаружение вторжений. IDS/IPS;
42. Механизмы ЗИ. Анализ защищенности;
43. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Общие сведения о категорировании информации в РФ;
44. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Права и обязанности обладателя информации по N 149-ФЗ;
45. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Общедоступная информация;
46. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Коммерческая тайна;
47. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Служебная тайна;

48. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Государственная тайна;
49. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Профессиональная и банковская тайна;
50. Правовые средства ЗИ. Классификация информации по уровню доступа в РФ. Персональные данные;
51. Стандарты в области ИБ. Классификации стандартов. Критерии оценки доверенных компьютерных систем.
52. Стандарты в области ИБ. Классификации стандартов. Руководящие документы (РД) ФСТЭК России.
53. Стандарты в области ИБ. Классификации стандартов. Х.800 «Архитектура безопасности для взаимодействия открытых систем».
54. Система стандартов по ЗИ (ССЗИ) РФ. ГОСТ Р 52069.0-2013.
55. Система стандартов по ЗИ (ССЗИ) РФ. Группа стандартов Защита информации. Уязвимости информационных систем.
56. Система стандартов по ЗИ (ССЗИ) РФ. Группа стандартов Защита информации. Техника защиты информации.
57. Система стандартов по ЗИ (ССЗИ) РФ. Группа стандартов Информационная технология. Криптографическая защита информации.
58. ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
59. ГОСТ Р ИСО/МЭК 27000-27006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента ИБ (СМИБ).
60. ГОСТ Р ИСО/МЭК 27033 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Башлы, П. Н. Информационная безопасность и защита информации: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2 Режим доступа: http://znanium.com/
2. Основные положения информационной безопасности: Учебное пособие/В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 с.: ISBN 978-5-00091-079-5, Режим доступа: http://znanium.com/
3. 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.
4. Кнауб, Л. В. Теоретико-численные методы в криптографии: Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2012. - 160 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=441493

б) Дополнительная литература:

1. А.Ю. Щербаков. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. - М.: Книжный мир, 2009. - 352 с. http://www.studentlibrary.ru/book/ISBN9785804103782.html
2. Информационная безопасность: защита и нападение / Бирюков А.А. - М. : ДМК Пресс, 2012. - http://www.studentlibrary.ru/book/ISBN9785940746478.html 474 с.
3. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с. ISBN 978-5-00091-007-8. Режим доступа: http://znanium.com/
4. Практическая криптография: алгоритмы и их программирование / Аграновский А.В., Хади Р.А. - М. : СОЛОН-ПРЕСС, 2009. - http://www.studentlibrary.ru/book/ISBN5980030026.html 256 с. ISBN 5-98003-002-6.
5. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев - М. : СОЛОН-ПРЕСС, 2009. http://www.studentlibrary.ru/book/ISBN5980030115.html 272 с.
6. Башлы, П. Н. Информационная безопасность и защита информации : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2 Режим доступа: http://znanium.com/catalog.php?bookinfo=405000

в) Периодические издания

1. Отраслевой lifestyle-журнал по теме безопасности «Рубеж». Режим доступа: http://rubezh.ru/;
2. Журнал «Защита информации. Инсайд» ISSN 2413-3582, Режим доступа: http://inside-zi.ru/pages/about.html;
3. Журнал "Алгоритм безопасности» – Режим доступа: http://www.algoritm.org/index.php;
4. Электронный научный журнал «Проблемы безопасности» – Режим доступа: http://www.pb.littera-n.ru/
5. Журнал «Вопросы защиты информации». Режим доступа: http://i-vimi.ru/editions/detail.php?SECTION_ID=155/;
6. Журнал "Information Security/Информационная безопасность". Режим доступа: http://www.itsec.ru/insec-about.php.

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://icn.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)

Лекционная аудитория 111-2. Перечень оборудования: переносной проектор, маркерная доска, переносной ноутбук. Компьютерный класс 234-2 на 10 персональных рабочих мест с доступом в Интернет, переносной проектор, маркерная, переносной ноутбук.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению 15.04.04 "Автоматизация технологических процессов и производств"

Рабочую программу составил доцент кафедры ИЗИ к.т.н. Мишин Д.В.
(ФИО, подпись)

Рецензент
(представитель работодателя) к.т.н. Абрамов Константин Германович ведущий специалист управления поддержки инфраструктуры ООО «ОМК - Информационные технологии».
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ
Протокол № 7 от 10.02.2015 года
Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 15.04.04 "Автоматизация технологических процессов и производств"
Протокол № 3 от 12.02.2015 года
Председатель комиссии В.Ф. Корастелев
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на 2017/18 учебный год
Протокол заседания кафедры № 2 от 21.02.17 года
Заведующий кафедрой В.Ф. Корастелев
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на 2018/19 учебный год
Протокол заседания кафедры № 1 от 03.09.18 года
Заведующий кафедрой В.Ф. Корастелев
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 2019/20 учебный год

Протокол заседания кафедры № 2 от 03.09.19 года

Заведующий кафедрой _____ В.Ф. Коростелев

Рабочая программа одобрена на 2020/21 учебный год

Протокол заседания кафедры № 1 от 01.09.20 года

Заведующий кафедрой _____ В.Ф. Коростелев

Рабочая программа одобрена на 2021/22 учебный год

Протокол заседания кафедры № 2 от 14.09.21 года

Заведующий кафедрой _____ В.Ф. Коростелев

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой _____ В.Ф. Коростелев

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой _____ В.Ф. Коростелев

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой _____ В.Ф. Коростелев