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

УТВЕРЖДАЮ
Проректор УМР
_____ А.А.Панфилов
«___» _____ 2015 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(наименование дисциплины)

Направление подготовки 27.03.04 - Управление в технических системах

Профиль / программа подготовки Управление и информатика в технических системах

Уровень высшего образования бакалавриат

Форма обучения очная

Семестр	Трудоем-кость зач. ед,час.	Лек-ции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
5	3/108	18		18	72	зачет
Итого	3/108	18		18	72	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 Министерства образования и науки Российской Федерации от «28» октября 2009 г. № 496, утверждающий ФГОС ВПО по направлению подготовки 090900 «Информационная безопасность»;
- 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 «Информационная безопасность» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 27.03.04 - Управление в технических системах. Формирование у бакалавров знаний и навыков в предметной области. Предмет курса - понятийный аппарат, а также сущность, теоретические, концептуальные, методологические аспекты и структура ПБ.

Задачами дисциплины являются: изучение понятийного аппарата в области ИБ; раскрытие базовых содержательных положений в области ИБ; изучение современной доктрины информационной безопасности; установление факторов, влияющих на ИБ; изучение методов определения состава защищаемой информации, классификация ее по видам тайны, материальным носителям, собственникам и владельцам; установление структуры угроз защищаемой информации; изучение направлений, видов, методов и особенностей деятельности разведывательных органов по добыванию конфиденциальной информации; раскрытие сущности компонентов защиты информации; определение назначения, сущности и структуры комплексных систем защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина изучается на третьем курсе, для грамотного использования полученных знаний в профессиональной деятельности, требуется изучение курсов «Математика»; «Информатика», «Вычислительные машины, системы и сети». Знания, полученные в результате курса, пригодятся при выполнении ВКР.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ

В результате освоения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ОПК-9 - способность использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности

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; основные положения государственной политики обеспечения информационной безопасности; критерии, условия и принципы отнесения информации к защищаемой; виды носителей защищаемой информации; виды тайн конфиденциальной информации; виды уязвимости защищаемой информации; источники, виды и способы дестабилизирующего воздействия на защищаемую информацию; каналы и методы несанкционированного доступа к конфиденциальной информации; классификацию видов, методов и средств защиты информации);

2) ***Уметь:*** - выявлять угрозы информационной безопасности применительно к объектам защиты; определять состав конфиденциальной информации применительно к видам тайны; выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников воздействия; выявлять применительно к объекту защиты каналы и методы несанкционированного доступа к конфиденциальной информации; определять направления и виды защиты информации с учетом характера информации и задач по ее защите; организовывать системное обеспечение защиты информации;

3) ***Владеть:*** Основными системными подходами к определению целей, задач информационно-аналитической работы и источников специальной информации; информацией о современных и перспективных системах автоматизации информационно- аналитической работы.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3_зачетных единицы, 108 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. Знчение ИБ и ее место в системе национальной безопасности	5	1	2			2		8		2/50%	
2	Основные понятия и определения в области ИБ и ЗИ.	5	3	2			2		8		2/50%	
3	Основные компоненты ИБ. Взаимосвязь компонентов ИБ	5	5	2			2		8		2/50%	Рейтинг контроль №1
4	Категории защищаемой информации. Классификация информации по уровню доступа в РФ	5	7	2			2		8		2/50%	
5	Концептуальная модель системы ИБ. Методы, меры и средства ИБ	5	9	2			2		8		2/50%	
6	Угрозы ИБ. Классификация угроз ИБ.	5	11	2			2		8		2/50%	Рейтинг контроль №2
7	Управление доступом. Идентификация и аутентификация. Модели управления доступом	5	13	2			2		8		2/50%	
8	Программно-аппаратные средства ЗИ.	5	15	2			2		8		2/50%	
9	Уровни ИБ	5	17	2			2		8		2/50%	Рейтинг контроль №3
Всего				18			18		72		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 бакалавра по направлению 27.03.04 - Управление в технических системах.

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 ОПОИ бакалавриата по направлению 27.03.04 - Управление в технических системах, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом, в учебном процессе, они должны составлять **не менее 20% аудиторных занятий.** Занятия лекционного типа для соответствующих групп студентов не могут составлять более 45 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 СРС

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

Темы лабораторных работ:

1. Лабораторная работа: Составление досье с использованием интернет- ресурсов для оценки воздействия икт-технологий на неприкосновенность частной жизни
2. Лабораторная работа: количественная оценка стойкости парольной защиты
3. Лабораторная работа: Программирование задач шифрования методом подстановки
4. Лабораторная работа: Управление локальными параметрами безопасности ОС Windows
5. Лабораторная работа: Классическая модель доступа ОС на базе Linux
6. Лабораторная работа: Расширенная модель доступа ОС на базе Linux
7. Лабораторная работа: Установка и настройка программного межсетевого экрана
8. Лабораторная работа: Анализ программного обеспечения вычислительной системы
9. Лабораторная работа: Антивирусные программы

Темы и вопросы по СРС Раздел 1

1. Какие признаки объектов являются демаскирующими?
2. Приведите классификацию демаскирующих признаков объектов защиты.
3. Опишите опознавательные демаскирующие признаки объектов защиты.
4. Охарактеризуйте признаки деятельности как демаскирующие признаки объектов защиты.
5. Что такое информативность демаскирующего признака?
6. Что такое тезаурус?

7. Перечислите основные носители признаковой информации.
8. Перечислите основные источники конфиденциальной информации.
9. В чем отличие прямых источников семантической информации от косвенных?
10. Охарактеризуйте производственные и промышленные отходы как источник конфиденциальной информации

Раздел 2

1. В чем специфика деятельности Межведомственной комиссии по защите государственной тайны?
2. Перечислите основные задачи в области обеспечения информационной безопасности для ФСТЭК России.
3. В чем специфика деятельности Федеральной службы безопасности?
4. Прокомментируйте основные права ФСБ в части задач информационной безопасности.
5. В чем специфика деятельности службы внешней разведки РФ в отношении ИБ?
6. В чем специфика деятельности Минобороны России в отношении проблем ИБ?
7. В чем специфика деятельности органов государственного управления (министерств, ведомств) в обеспечении ИБ?
8. Какие ключевые проблемы необходимо решить безотлагательно, чтобы обеспечить достаточный уровень ИБ в России?
9. Раскройте содержание политических факторов, влияющих на состояние информационной безопасности РФ.
10. Раскройте содержание экономических факторов, влияющих на состояние информационной безопасности РФ.
11. Раскройте содержание организационно-технических факторов, влияющих на состояние информационной безопасности РФ.

Раздел 3

1. Как в Доктрине информационной безопасности Российской Федерации определяется термин «информационная безопасность»?
2. Как в Законе РФ "Об участии в международном информационном обмене" определяется термин «информационная безопасность»?
3. Дайте определение информационной безопасности, прокомментируйте его составляющие.
4. Что такое защита информации?
5. Приведите убедительные доводы того, что информационная безопасность - одна из важнейших проблем современной жизни.

Раздел 4

1. Какую информацию нельзя засекречивать как имеющую статус государст-'венной тайны?
2. Что характеризует политический ущерб, наносимый при утечке сведений, составляющих государственную тайну?
3. Что характеризует экономический ущерб, наносимый при утечке сведений, составляющих государственную тайну?
4. Что характеризует моральный ущерб, наносимый при утечке сведений, составляющих государственную тайну?
5. Перечислите основные виды конфиденциальной информации, нуждающейся в защите.
6. Какая информация не может быть отнесена к коммерческой тайне?
7. Перечислите основные объекты банковской тайны.
8. Приведите перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения (согласно законодательству).
9. Какие сведения могут быть отнесены к персональным данным? Кто является держателем персональных данных?
10. Перечислите основные объекты интеллектуальной собственности.

Раздел 5

1. Что такое объекты угроз ИБ и в чем они выражаются?
2. Каковы основные источники угроз защищаемой информации?
3. Каковы цели угроз информации со стороны злоумышленников?
4. Перечислите основные источники конфиденциальной информации.

5. Назовите основные способы неправомерного овладения конфиденциальной информацией (способы доступа).
6. Перечислите базовые способы защиты информации.
7. Изобразите графически схему концептуальной модели системы ИБ.

Раздел 6

1. Перечислите основные способы несанкционированного доступа к конфиденциальной информации.
2. Охарактеризуйте обобщенную модель взаимодействия способов несанкционированного доступа и источников конфиденциальной информации.
3. Определите понятие «разглашение» конфиденциальной информации, в чем оно выражается?
4. Как осуществляется утечка конфиденциальной информации?

Раздел 7

1. Каким образом непреднамеренное разглашение информации может привести к ее утечке?
2. Что такое наблюдение в теории информационной безопасности?
3. Что такое подслушивание в теории информационной безопасности?
4. Что такое перехват в теории информационной безопасности?
5. Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.
6. Какие организации формируют структуру разведывательного сообщества США?
7. Охарактеризуйте непреднамеренные ошибки в качестве угрозы доступности.
8. Охарактеризуйте программные атаки на доступность.
9. Приведите примеры «бомбы», «червя», «вируса».
10. Прокомментируйте понятия «кража» и «подлог» в качестве угрозы целостности.
11. Что в ИБ понимают под маскарадом?

Раздел 8

1. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации
2. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации
3. Назовите три группы мероприятий по технической защите информации.
4. Прокомментируйте основные организационные мероприятия по технической защите информации. В каких ограничительных мерах они выражаются?
5. Прокомментируйте основные организационно-технические мероприятия по ЗИ.
6. Прокомментируйте основные технические мероприятия по технической защите информации.

Раздел 9

Назовите основные меры и архитектурные принципы обеспечения обслуживаемости ИС. В чем заключается специфика управления, как сервиса безопасности?

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. Х.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:

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/

Основные положения информационной безопасности: Учебное пособие/В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 е.: ISBN 978-5-00091-079-5, Режим доступа: http://znanium.com/

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. -

б) Дополнительная литература:

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

Информационная безопасность: защита и нападение / Бирюков А. А. - М.: ДМК Пресс, 2012. - http://www.studentlibrary.ru/book/ISBN9785940746478.html 474 с.

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/

в) Периодические издания

1. Отраслевой lifestyle-журнал по теме безопасности «Рубеж». Режим доступа: http://ru- bezh.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/

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)

Лекционная аудитория 408-2. Перечень оборудования: переносной проектор, маркерная доска, переносной ноутбук. Компьютерный класс 117-3 на 8 персональных рабочих мест с доступом в Интернет, переносной проектор, маркерная, переносной ноутбук.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению 27.03.04 - Управление в технических системах

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 № 4 от 18.11.15 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 27.03.04 - Управление в технических системах

Протокол № 8 от 18.11.15 года

Председатель комиссии Градусов А.Б.
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ

РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на 2018/19 учебный год

Протокол заседания кафедры № 1 от 14.09.18 года

Заведующий кафедрой _____