УП 2015

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
по образовательной деятельности
_____ А.А.Панфилов
«_29_» _12_____ 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Управление информационной безопасностью

Направление подготовки 10.04.01 Информационная безопасность

Программа подготовки _____

Уровень высшего образования магистратура

Форма обучения очная

Семестр	Трудоем-кость зач. ед./час.	Лек-ций, час.	Практич. занятий, час.	Лаборат. работ, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
3	3/108	18		18	36	Экзамен (36ч), КР
Итого	3/108	18		18	36	Экзамен (36ч), КР

ВЛАДИМИР 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Управление информационной безопасностью» являются обеспечение подготовки специалистов в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.04.01 «Информационная безопасность». Целью освоения дисциплины является формирование у студентов теоретических знаний и практических навыков по управлению информационной безопасностью автоматизированных систем. Кроме того, курс обеспечивает формирование у магистрантов обобщенного представления о методах анализа, оценки и управления рисками в условиях существования угроз, а также при разработке и принятии управленческих решений в условиях неопределенности и риска, характерных для функционирования современных предприятий. Задачами дисциплины «Управление информационной безопасностью» являются: - освоение принципов реализации и основных подходов к оптимальному управлению различными механизмами информационной безопасности в системах. Формирование представлений: - о риске, его видах и источниках возникновения; - о количественных и качественных методах анализа и оценки риска; - о методах управления рисками и снижения их последствий; - о функционировании риск-менеджмента на современном предприятии.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО МАГИСТРАТУРЫ

Данная дисциплина относится к базовым дисциплинам Блока Б1 (код М3.Б.3). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ.

Дисциплина изучается на 2 курсе, в 3 семестре, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по направлению 10.04.01 по курсам «Анализ и моделирование информационно-телекоммуникационных сетей», «Методы и средства защиты объектов информатизации», «Методология информационной безопасности», «Оценка и контроль обеспечения информационной безопасности», «Методы информационно-аналитической работы». Кроме того, требования к «входным» знаниям, умениям и готовностям обучающегося определяются требованиями к уровню подготовки выпускника бакалавриата при освоении курсов «Защита информации в корпоративных информационных системах» или аналогичных, в соответствии с программой подготовки бакалавров в следующих или смежных областях знаний: -информационная безопасность; -энергетика, энергетическое машиностроение и электротехника; -авиационная и ракетно-космическая техника; - фотоника, приборостроение, -оптические и биотехнические системы и технологии; - электронная техника, радиотехника и связь; -автоматика и управление; -информатика и вычислительная техника; -физико-технические науки и технологии; -управление в технических системах.

Курс тесно взаимосвязан с другими дисциплинами. Он может быть полезен для изучения таких дисциплин как «Организационно-правовые механизмы обеспечения информационной безопасности», «Защищённые информационные системы», «Экономика и управление», и т.д.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс изучения дисциплины направлен на формирование следующих профессиональных компетенций, которыми должен обладать выпускник:

ПК-12 – способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения;

ПК-13 – способностью организовать управление информационной безопасностью.

1) ***Знать:*** - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; - основные механизмы информационной безопасности и типовые процессы управления этими механизмами в информационной системе; - основные угрозы безопасности информации и модели нарушителя в

информационных системах; - принципы формирования политики информационной безопасности в информационных системах; - методы аттестации уровня защищенности информационных систем; - основные методы управления информационной безопасностью; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем (ПК-12; ПК-13);

2) ***Уметь:*** - строить системы обеспечения информационной безопасности в различных условиях функционирования защищаемых информационных систем;- разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; - разрабатывать частные политики информационной безопасности информационных систем; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; - оценивать информационные риски в информационных системах; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; - составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности (ПК-12; ПК-13);

3) ***Владеть:*** - методами и средствами выявления угроз безопасности информационным системам; - навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; - навыками участия в экспертизе состояния защищенности информации на объекте защиты; - методами управления информационной безопасностью информационных систем; - методами оценки информационных рисков; - методами организации и управления деятельностью служб защиты информации на предприятии; - навыками управления информационной безопасностью простых объектов (ПК-12; ПК-13).

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

- способность разрабатывать, оформлять и реализовывать политики информационной безопасности для современных КИС предприятия.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 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.	Введение. Основные понятия	3	1-2	2		2		4		1/25%	
2.	Основные определения и критерии классификации угроз	3	3-4	2		2		4		2/50%	
3.	Общие положения управления рисками	3	5-6	2		2		4		1/25%	Рейтинг-контроль №1
4.	Подготовительные этапы управления рисками	3	7-8	2		2		4		2/50%	
5.	Анализ угроз и оценка рисков	3	9-10	2		2		4		2/50%	
6.	Выбор защитных мер и последующие этапы управления рисками	3	11-12	2		2		4		1/25%	Рейтинг-контроль №2
7.	Ключевые роли в процессе управления рисками	3	13-14	2		2		4		1/25%	
8.	Детальное рассмотрение процесса оценки рисков	3	15-16	2		2		4		2/50%	
9.	Результирующая документация	3	17-18	2		2		4	КР	2/50%	Рейтинг-контроль №3
Всего:				18		18		36		14/39%	Экзамен, КР

Содержание дисциплины «Управление информационной безопасностью»

Раздел 1. Введение. Основные понятия

Адекватная безопасность. Базовый уровень безопасности. Компрометация. Нарушение информационной безопасности. Уровень (степень) критичности ИС. Окружение (среда) . Воздействие (влияние). Анализ воздействия на производственную деятельность. Контрмеры. Риск. Риски, связанные с информационными технологиями. Остаточный риск. Совокупный (суммарный, полный) риск. Анализ рисков. Управление рисками. Нейтрализация (уменьшение, ослабление) рисков. Терпимость по отношению к риску. Санкционирование безопасной эксплуатации. Категория безопасности. Уровень защищенности. Требования безопасности. Наиболее распространенные угрозы

Раздел 2. Основные определения и критерии классификации угроз

Угроза. Атака. Злоумышленник. Источники угроз. Окно опасности. Наиболее распространенные угрозы, которым подвержены современные ИС. Наиболее распространенные угрозы доступности. Отказ пользователей. Внутренний отказ информационной системы. Отказ поддерживающей инфраструктуры. Основные источники внутренних отказов. Примеры угроз доступности. Вредоносное программное обеспечение: вредоносная функция; способ распространения; внешнее представление. Основные угрозы целостности. Угрозы статической и

динамической целостности. Основные угрозы конфиденциальности. Перехват данных. Злоупотребление полномочиями.

Раздел 3. Общие положения управления рисками

Цикл управления рисками: (пере)оценка (измерение) рисков; выбор эффективных и экономичных защитных средств (нейтрализация рисков). Основные этапы управления рисками. Интегрирование управления рисками в жизненный цикл ИС на этапах инициации, закупки (разработки), установки, эксплуатации и выведении системы из эксплуатации.

Раздел 4. Подготовительные этапы управления рисками

Выбор анализируемых объектов и уровня детализации их рассмотрения. Инфологическая модель. Карта информационной системы организации. Идентификация активов,

Раздел 5. Анализ угроз и оценка рисков

Перечень наиболее распространенных угроз. Модель угроз организации. Процедуры идентификации угроз. Выявление источников возникновения угроз. Типы злоумышленников. Модели оценки вероятности осуществления угрозы. Метрики, используемые для оценки вероятности осуществления угрозы. Размер потенциального ущерба.

Раздел 6. Выбор защитных мер и последующие этапы управления рисками

Оценка стоимости защитных мер. Проблема совместимости нового средства защитных мер со сложившейся организационной и аппаратно-программной структурой, с традициями организации. Планирование реализации и проверки новых регуляторов безопасности. План тестирования (автономного и комплексного) программно-технических механизмов защиты. Проверка того, что остаточные риски стали приемлемыми.

Раздел 7. Ключевые роли в процессе управления рисками

Управление рисками как деятельность административного уровня информационной безопасности. Роли в этой деятельности: руководителя организации, начальника управления (отдела) информатизации, владельцев систем и информации, руководителей производственных отделов и отдела закупок, начальника отдела (управления) информационной безопасности, администраторов безопасности, системных и сетевых администраторов, специалистов по обучению персонала.

Раздел 8. Детальное рассмотрение процесса оценки рисков

Девять основных этапов процесса оценки рисков, их входная и выходная информация. Определение характеристик информационной системы. Информация об эксплуатационном окружении системы. Методы получения информации: вопросники, интервью, просмотр документации. Применение инструментов автоматического сканирования. Идентификация уязвимостей на стадии проектирования ИС, на этапе реализации, на этапе эксплуатации. Автоматические средства сканирования, средства тестирования и оценки, тестирование проникновением. Идентификация угроз. Анализ регуляторов безопасности. Определение вероятностей. Анализ воздействия. Определение рисков. Рекомендуемые контрмеры

Раздел 9. Результирующая документация

Определение приоритетов, оценка и реализация контрмер, уменьшающих риски и рекомендованных по результатам оценки рисков. Различные возможности в процессе управления рисками: принятие риска; уклонение от риска ; ограничение (нейтрализация) риска ; переадресация риска. Оценка экономической эффективности. Возможный формат отчета об оценке рисков. Возможный формат плана реализации контрмер. Возможные трактовки и способы вычисления рисков. Представление рисков в виде дерева уязвимостей, угроз и контрмер.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины «Управление информационной безопасностью» предполагает не только запоминание и понимание, но и анализ, синтез, рефлексию, формирует универсальные умения и навыки, являющиеся основой становления магистра в области информационной безопасности.

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

разбор конкретных ситуаций;

учебную дискуссию;

электронные средства обучения (слайд-лекции).

Лекционные занятия проводятся в аудитории, оборудованной проектором, что позволяет сочетать активные и интерактивные формы проведения занятий.

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 магистрантами, а также интенсификация и диверсификация учебного процесса.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью (миссией) программы, 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 по направлению подготовки 10.04.01 «Информационная безопасность» 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 САМОСТОЯТЕЛЬНОЙ РАБОТЫ МАГИСТРАНТОВ

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

Примерный перечень заданий для текущих контрольных мероприятий:

Вопросы рейтинг-контроля №1

1. Что понимается под адекватной безопасностью?
2. Что такое компрометация в информационной безопасности?
3. Что понимается под нарушением информационной безопасности?
4. Что понимается под уровнем (степенью) критичности ИС?
5. Определите окружение (среду) ИС .
6. Охарактеризуйте процесс воздействия на производственную деятельность.
7. Дайте определение понятию «риск».

8. В чем особенности рисков, связанных с информационными технологиями.
9. Что такое остаточный риск?
10. Что такое совокупный (суммарный, полный) риск.
11. Определите понятие «Анализ рисков».
12. В чем состоит управление рисками в информационной безопасности?
13. Что такое нейтрализация (уменьшение, ослабление) рисков?
14. Что такое терпимость по отношению к риску?
15. Определите основные категория безопасности.
16. Что понимают под уровнем защищенности.
17. Дайте определение угроз конфиденциальной информации.
18. Что такое атака?
19. Что такое окно опасности?
20. Какие события происходят во время существования окна опасности?
21. Что такое угрозы воздействия на источник информации?
22. Что такое угрозы утечки информации?
23. Какие угрозы называются преднамеренными?
24. Какие угрозы называются случайными?
25. Что такое канал несанкционированного доступа?
26. Что такое утечка информации?
27. Что такое перехват в теории информационной безопасности?
28. Что такое канал утечки информации?
29. Что такое технический канал утечки информации?
30. Охарактеризуйте случайный и организованный канал утечки информации.
31. Что такое источник угроз безопасности информации?
32. Назовите основные источники преднамеренных угроз.
33. Назовите основные источники случайных угроз.
34. Прокомментируйте наиболее распространенные угрозы доступности.
35. Охарактеризуйте непреднамеренные ошибки в качестве угрозы доступности.
36. Что такое отказ пользователей?
37. Прокомментируйте внутренний отказ ИС в качестве угрозы.
38. Прокомментируйте отказ поддерживающей инфраструктуры в качестве угрозы.
39. Каким образом происходит повреждение или даже разрушение оборудования?
40. Что такое вредоносное программное обеспечение?
41. Какие негативные последствия в функционировании ИС вызывает вредоносное ПО?
42. Охарактеризуйте основные угрозы целостности конфиденциальной информации.
43. Перечислите основные угрозы конфиденциальности информацию
44. Что понимают под перехватом данных и в чем заключается угроза конфиденциальности?
45. Охарактеризуйте этап выбора эффективных и экономичных защитных средств (нейтрализация рисков).
46. В чем заключается суть мероприятий по управлению рисками?
47. Какие возможны действия по отношению к выявленным рискам?
48. Какие этапы управления рисками относятся к вспомогательным и почему?
49. Почему карта информационной системы способствует управлению рисками?
50. Какие этапы управления рисками относятся к основным и почему?
51. Почему важен процесс интегрирования управления рисками в жизненный цикл ИС?

Вопросы рейтинг-контроля №2

1. Каким образом производится выбор анализируемых объектов
2. Почему важен уровень детализации при рассмотрении анализируемых объектов?
3. Что такое инфологическая модель ИС?
4. Приведите основные объекты инфологической модели объекта
5. Как сформировать карту информационной системы организации?

6. Что такое идентификация активов в управлении рисками информационной безопасности?
7. Какие средства автоматизации идентификация активов ИС организации Вы знаете?
8. Приведите перечень наиболее распространенных угроз.
9. Что такое модель угроз организации?
10. Приведите основные компоненты модели угроз организации.
11. Охарактеризуйте процедуры идентификации угроз.
12. Приведите основные источники возникновения угроз.
13. Что включает в себя понятие «модель (облик) нарушителя»?
14. Приведите возможную классификацию нарушителей.
15. Прокомментируйте возможности конкурентов, клиентов, посетителей и хакеров в качестве потенциальных злоумышленников
16. Определите цели администраторов, программистов, операторов, руководителей, технического персонала, сотрудников, уволенных с работы в качестве потенциальных нарушителей ИБ
17. Что такое матрица нарушений ИБ? Приведите ее возможную структуру.
18. Зачем необходим сценарий нарушения ИБ?
19. Приведите модели оценки вероятности осуществления угрозы.
20. Охарактеризуйте основные метрики, используемые для оценки вероятности осуществления угрозы.
21. Дайте определение способа защиты информации.
22. Охарактеризуйте способ предупреждения возможных угроз.
23. Прокомментируйте основные действия способа выявления угроз
24. Охарактеризуйте способ обнаружения угроз.
25. Охарактеризуйте способ пресечения или локализации угроз.
26. Прокомментируйте основные действия способа ликвидации последствий.
27. Перечислите основные защитные действия при реализации способов ЗИ,
28. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации
29. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации
30. Назовите три группы мероприятий по технической защите информации.
31. Прокомментируйте основные организационные мероприятия по технической защите информации.
32. В каких ограничительных мерах выражаются организационные мероприятия по ЗИ.
33. Прокомментируйте основные организационно-технические мероприятия по ЗИ.
34. Прокомментируйте основные технические мероприятия по технической защите информации.
35. Как оценить стоимости защитных мер.
36. В чем заключается проблема совместимости нового средства защитных мер со сложившейся организационной и аппаратно-программной структурой, с традициями организации?
37. Планирование реализации и проверки новых регуляторов безопасности.
38. План тестирования (автономного и комплексного) программно-технических механизмов защиты.

Вопросы рейтинг-контроля №3

1. Почему управление рисками рассматривается на административном уровне ИБ?
2. Охарактеризуйте роль руководителя организации в процессе управления рисками информационной безопасности.
3. Охарактеризуйте роль начальника управления (отдела) информатизации в процессе управления рисками информационной безопасности.

4. Охарактеризуйте роль владельцев систем и информации в процессе управления рисками информационной безопасности.
5. Охарактеризуйте роль руководителей производственных отделов и отдела закупок в процессе управления рисками информационной безопасности.
6. Охарактеризуйте роль начальника отдела (управления) информационной безопасности в процессе управления рисками информационной безопасности.
7. Охарактеризуйте роль администраторов безопасности в процессе управления рисками информационной безопасности.
8. Охарактеризуйте роль специалистов по обучению персонала в процессе управления рисками информационной безопасности.
9. Почему управление рисками рассматривается на административном уровне ИБ?
10. Охарактеризуйте роль руководителя организации в процессе управления рисками информационной безопасности.
11. Охарактеризуйте роль начальника управления (отдела) информатизации в процессе управления рисками информационной безопасности.
12. Охарактеризуйте роль владельцев систем и информации в процессе управления рисками информационной безопасности.
13. Охарактеризуйте роль руководителей производственных отделов и отдела закупок в процессе управления рисками информационной безопасности.
14. Охарактеризуйте роль начальника отдела (управления) информационной безопасности в процессе управления рисками информационной безопасности.
15. Охарактеризуйте роль администраторов безопасности в процессе управления рисками информационной безопасности.
16. Охарактеризуйте роль специалистов по обучению персонала в процессе управления рисками информационной безопасности.
17. Назовите и охарактеризуйте этапы процесса управления рисками.
18. Какие этапы управления рисками относятся к вспомогательным и почему?
19. Опишите этап выбора анализируемых объектов и уровня детализации их рассмотрения процесса управления рисками.
20. Какие этапы управления рисками относятся к основным и почему?
21. Охарактеризуйте основные шаги анализа угроз в процедуре управления рисками.
22. Охарактеризуйте этап оценки рисков в процедуре управления рисками.
23. Охарактеризуйте этап выбора защитных мер в процедуре управления рисками.
24. Охарактеризуйте этап реализации и проверки выбранных мер защиты в процедуре управления рисками.
25. Что такое оценка остаточного риска?
26. Определение приоритетов, оценка и реализация контрмер, уменьшающих риски и рекомендованных по результатам оценки рисков.
27. Назовите различные возможности в процессе принятия риска
28. Назовите различные возможности в процессе уклонения от риска
29. Назовите различные возможности в процессе ограничения (нейтрализации) риска
30. Назовите различные возможности в процессе переадресации риска.
31. В чем состоит оценка экономической эффективности.
32. Приведите возможный формат отчета об оценке рисков.
33. Приведите возможный формат плана реализации контрмер.
34. Приведите возможные трактовки и способы вычисления рисков.
35. Каким образом осуществляется представление рисков в виде дерева уязвимостей, угроз и контрмер.

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

1. Что понимается под нарушением информационной безопасности?
2. В чем особенности рисков, связанных с информационными технологиями.

3. Что такое остаточный риск?
4. Что такое совокупный (суммарный, полный) риск.
5. Определите понятие «Анализ рисков».
6. В чем состоит управление рисками в информационной безопасности?
7. Что понимают под уровнем защищенности.
8. Дайте определение угроз конфиденциальной информации.
9. Что такое угрозы воздействия на источник информации?
10. Какие угрозы называются преднамеренными?
11. Какие угрозы называются случайными?
12. Что такое канал несанкционированного доступа?
13. Что такое утечка информации?
14. Что такое перехват в теории информационной безопасности?
15. Что такое канал утечки информации?
16. Охарактеризуйте случайный и организованный канал утечки информации.
17. Прокомментируйте наиболее распространенные угрозы доступности.
18. Что такое вредоносное программное обеспечение?
19. Какие негативные последствия в функционировании ИС вызывает вредоносное ПО?
20. Охарактеризуйте основные угрозы целостности конфиденциальной информации.
21. Перечислите основные угрозы конфиденциальности информацию
22. В чем заключается суть мероприятий по управлению рисками?
23. Какие возможны действия по отношению к выявленным рискам?
24. Какие этапы управления рисками относятся к вспомогательным и почему?
25. Почему карта информационной системы способствует управлению рисками?
26. Какие этапы управления рисками относятся к основным и почему?
27. Почему важен процесс интегрирования управления рисками в жизненный цикл ИС?
28. Что такое инфологическая модель ИС?
29. Приведите основные объекты инфологической модели объекта
30. Как сформировать карту информационной системы организации?
31. Что такое идентификация активов в управлении рисками информационной безопасности?
32. Какие средства автоматизации идентификация активов ИС организации Вы знаете?
33. Что такое модель угроз организации?
34. Приведите основные компоненты модели угроз организации.
35. Что включает в себя понятие «модель (облик) нарушителя»?
36. Приведите возможную классификацию нарушителей.
37. Что такое матрица нарушений ИБ? Приведите ее возможную структуру.
38. Охарактеризуйте основные метрики, используемые для оценки вероятности осуществления угрозы.
39. Как оценить стоимости защитных мер.
40. В чем заключается проблема совместимости нового средства защитных мер со сложившейся организационной и аппаратно-программной структурой, с традициями организации?
41. Почему управление рисками рассматривается на административном уровне ИБ?
42. Назовите различные возможности в процессе принятия риска
43. Назовите различные возможности в процессе уклонения от риска
44. Назовите различные возможности в процессе ограничения (нейтрализации) риска
45. Назовите различные возможности в процессе переадресации риска.
46. В чем состоит оценка экономической эффективности.
47. Приведите возможный формат отчета об оценке рисков.
48. Приведите возможный формат плана реализации контрмер.
49. Приведите возможные трактовки и способы вычисления рисков.
50. Каким образом осуществляется представление рисков в виде дерева уязвимостей, угроз и контрмер.

Темы лабораторных работ:

Лабораторная работа № 1.

ЛАБОРАТОРНАЯ РАБОТА 1. Сбор исходных данных для аудита информационной безопасности объекта (6 час);

ЛАБОРАТОРНАЯ РАБОТА 2. Выявление уязвимостей информационной системы (4 час);

ЛАБОРАТОРНАЯ РАБОТА 3. Идентификация защитных механизмов (4 час);

ЛАБОРАТОРНАЯ РАБОТА 4. Идентификация нарушителей (4 час).

Вопросы и задания к самостоятельной работе магистрантов:

Раздел 1.

1. Определите базовый уровень безопасности.
2. Определите окружение (среду) ИС .
3. Охарактеризуйте процесс воздействия на производственную деятельность.
4. В чем особенности рисков, связанных с информационными технологиями.
5. Что такое нейтрализация (уменьшение, ослабление) рисков?
6. Что такое терпимость по отношению к риску?
7. Определите основные категория безопасности.
8. Что понимают под уровнем защищенности.

Раздел 2.

1. Назовите типовые причины возникновения каналов несанкционированного доступа.
2. Какие действия пользователя информации и злоумышленника, создающие угрозы утечки информации, в случае попадания ее к злоумышленнику приводят к утечке?
3. Охарактеризуйте случайный и организованный канал утечки информации.
4. Приведите качественную зависимость вероятности возникновения угрозы воздействия от соотношения цены информации и затрат злоумышленника на ее добывание.
5. Назовите основные источники преднамеренных угроз.
6. Назовите основные источники случайных угроз.
7. Какие сигналы в теории информационной безопасности принято называть опасными?
8. Что такое опасный функциональный сигнал?
9. Назовите основные источники опасных функциональных сигналов.
10. Что такое вредоносное программное обеспечение?
11. Дайте определение «бомбы».
12. Дайте определение «червя».
13. Дайте определение «вируса».
14. Что в ИБ понимают под маскарадом?

Раздел 3.

1. В чем заключается суть мероприятий по управлению рисками?
2. Охарактеризуйте процесс интегрирования управления рисками на этапе закупки (разработки) жизненного цикла ИС.
3. Охарактеризуйте процесс интегрирования управления рисками на этапе установки жизненного цикла ИС.
4. Охарактеризуйте процесс интегрирования управления рисками на этапе эксплуатации жизненного цикла ИС.
5. Охарактеризуйте процесс интегрирования управления рисками на этапе выведении системы из эксплуатации жизненного цикла ИС.

Раздел 4.

1. Каким образом производится выбор анализируемых объектов
2. Приведите основные объекты инфологической модели объекта
3. Как сформировать карту информационной системы организации?

4. Какие средства автоматизации идентификация активов ИС организации Вы знаете?

Раздел 5.

1. Приведите перечень наиболее распространенных угроз.
2. Приведите основные компоненты модели угроз организации.
3. Приведите основные источники возникновения угроз.
4. Приведите возможную классификацию нарушителей.
5. Прокомментируйте возможности конкурентов, клиентов, посетителей и хакеров в качестве потенциальных злоумышленников
6. Определите цели администраторов, программистов, операторов, руководителей, технического персонала, сотрудников, уволенных с работы в качестве потенциальных нарушителей ИБ
7. Приведите модели оценки вероятности осуществления угрозы.
8. Охарактеризуйте основные метрики, используемые для оценки вероятности осуществления угрозы.

Раздел 6.

1. Дайте определение способа защиты информации.
2. Охарактеризуйте способ предупреждения возможных угроз.
3. Прокомментируйте основные действия способа выявления угроз
4. Охарактеризуйте способ обнаружения угроз.
5. Охарактеризуйте способ пресечения или локализации угроз.
6. Прокомментируйте основные действия способа ликвидации последствий.
7. Перечислите основные защитные действия при реализации способов ЗИ,
8. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации
9. Назовите три группы мероприятий по технической защите информации.
10. Прокомментируйте основные организационные мероприятия по технической защите информации.
11. В каких ограничительных мерах выражаются организационные мероприятия по ЗИ.

Раздел 7.

1. Охарактеризуйте роль руководителя организации в процессе управления рисками информационной безопасности.
2. Охарактеризуйте роль начальника управления (отдела) информатизации в процессе управления рисками информационной безопасности.
3. Охарактеризуйте роль владельцев систем и информации в процессе управления рисками информационной безопасности.
4. Охарактеризуйте роль руководителей производственных отделов и отдела закупок в процессе управления рисками информационной безопасности.
5. Охарактеризуйте роль начальника отдела (управления) информационной безопасности в процессе управления рисками информационной безопасности.
6. Охарактеризуйте роль администраторов безопасности в процессе управления рисками информационной безопасности.
7. Охарактеризуйте роль специалистов по обучению персонала в процессе управления рисками информационной безопасности.
8. Почему управление рисками рассматривается на административном уровне ИБ?

Раздел 8.

1. Назовите и охарактеризуйте этапы процесса управления рисками.
2. Опишите этап выбора анализируемых объектов и уровня детализации их рассмотрения процесса управления рисками.
3. Охарактеризуйте основные шаги анализа угроз в процедуре управления рисками.
4. Охарактеризуйте этап оценки рисков в процедуре управления рисками.
5. Охарактеризуйте этап выбора защитных мер в процедуре управления рисками.
6. Охарактеризуйте этап реализации и проверки выбранных мер защиты в процедуре управления рисками.

Раздел 9.

1. Назовите различные возможности в процессе ограничения (нейтрализации) риска
2. Назовите различные возможности в процессе переадресации риска.
3. В чем состоит оценка экономической эффективности.
4. Приведите возможный формат отчета об оценке рисков.
5. Приведите возможный формат плана реализации контрмер.
6. Приведите возможные трактовки и способы вычисления рисков.
7. Каким образом осуществляется представление рисков в виде дерева уязвимостей, угроз и контрмер.

Варианты задания к курсовой работе:

Тема работы: «Формирование проектной документации для технических систем защиты от НСД объекта» по вариантам. Всего в методических рекомендациях по выполнению курсовой работы имеется 18 вариантов заданий.

Вопросы для выполнения в курсовой работе:

- Составить акт обследования инженерно-технического укрепления объекта с перечнем всех недостатков в укреплении элементов строительных конструкций объекта и рекомендациями по устранению выявленных недостатков;

- Проектирование охранно-тревожной сигнализации объектов на основе оборудования интегрированной системы безопасности (ИСБ) «Орион» НВП «Болид» (по выданным вариантам планировок разработка структурной схемы, поэтажных планов сетей ОТС, пояснительной записки, расчет цепей питания, создание спецификации оборудования);

- Формирование технического задания на проектирование объекта охранно-тревожной сигнализацией;

- Формирование технического задания на проектирование объекта системой контроля и управления доступом (СКУД);

- Формирование технического задания на проектирование объекта системой охранного телевидения (СОТ);

- Проектирование систем СКУД объектов (составить поэтажные план-схемы объекта с указанием помещений и аппаратуры СКУД; составить структурную схему СКУД; составить краткое описание принципа работы СКУД и техописание (краткое) контроллера СКУД и используемого ПО; составить спецификацию оборудования для оборудования объекта СКУД (в т.ч. кабельная продукция, источники питания и прочее); по источникам питания просчитать их токовую нагрузку, нарисовать структурную схему питания элементов СКУД).

- Проектирование систем охранного телевидения объектов (составить поэтажные план-схемы объекта с указанием помещений и аппаратуры СВН; выбрать самостоятельно расстояние от каждой камеры до объекта наблюдения; рассчитать углы обзора и фокусное расстояние каждой камеры; выбрать марки камер, кожухов, объективов, мультиплексоров и др. оборудования; рассчитать время записи на видеорегистраторе; составить структурную схему СВН; составить краткое техописание оборудования и используемого ПО; - составить спецификацию оборудования для СВН (в т.ч. кабельная продукция, источники питания и прочее); - по источникам питания просчитать их токовую нагрузку, нарисовать структурную схему питания элементов СВН).

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Жукова, М. Н. Управление информационной безопасностью. Ч. 2.: учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=463061
2. Интеллектуальные системы защиты информации: учеб. пособие/ В. И. Васильев. 2-е изд., испр. и доп. - М.: Машиностроение, 2013.- 172 с. - ISBN 978-5-94275-667-3. Режим доступа: http://www.studentlibrary.ru/book/ISBN9785942756673.html
3. Информационная безопасность: защита и нападение / Бирюков А.А. - М. : ДМК Пресс, 2012. - http://www.studentlibrary.ru/book/ISBN9785940746478.html. 474 с.

б) Дополнительная 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. Бизнес-безопасность / Кузнецов И.Н. - М. : Дашков и К, 2012. - http://www.studentlibrary.ru/book/ISBN9785394014383.html. 416 с.
3. Офисный шпионаж / Мелтон К., Пилиджан К., Сверчински Д. - М. : Альпина Паблишер, 2013. - http://www.studentlibrary.ru/book/ISBN9785916712070.html. 182 с.
4. Искусство управления информационными рисками / Астахов А.М. - М. : ДМК Пресс, 2010. - http://www.studentlibrary.ru/book/ISBN9785940745747.html. 312 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. Журнал «Защита информации. Инсайд» ISSN 2413-3582, Режим доступа: http://inside-zi.ru/pages/about.html;
4. Журнал «Спецтехника и Связь» , Режим доступа: http://www.st-s.su/

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/

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.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению 10.04.01 «Информационная безопасность»

Рабочую программу составил доцент кафедры ИЗИ к.т.н. Полянский Д.А.

(ФИО, подпись)

Рецензент
(представитель работодателя) к.т.н. Курысев Константин Николаевич ВРИО заместителя начальника Владимирского юридического института ФСИН России по учебной работе

(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 7 от 28.12.16 года

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

(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 10.04.01 «Информационная безопасность»

Протокол № 4 от 28.12.16 года

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

(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на 2017/18 учебный год

Протокол заседания кафедры № 1 от 28.08.17 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/ з

(ФИО, подпись)

Приложение

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

Институт _____

Кафедра _____

Актуализированная
рабочая программа
рассмотрена и одобрена
на заседании кафедры
протокол № ____ от ____ 20__г.

Заведующий кафедрой

_____
(подпись, ФИО)

Актуализация рабочей программы дисциплины

_____
(наименование дисциплины)

Направление подготовки

Профиль/программа подготовки

Уровень высшего образования

Форма обучения

Владимир 20__

Рабочая программа учебной дисциплины актуализирована в части рекомендуемой литературы.

Актуализация выполнена: _____
(подпись, должность, ФИО)

а) основная литература:_____

б) дополнительная литература: _____

в) периодические издания: _____

в) интернет-ресурсы: _____