УП 2015-2016

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

Политики информационной безопасности в корпоративных информационных системах

(наименование дисциплины)

Специальность 10.05.04 "Информационно-аналитические системы безопасности"

Специализация "Автоматизация информационно-аналитической деятельности"

Уровень высшего образования специалитет

Форма обучения очная

Семестр	Трудоемкость зач. ед,/ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
7	2/72	18		36	18	Зачет
Итого	2/72	18		36	18	Зачет

Владимир 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Политики информационной безопасности в корпоративных информационных системах» являются обеспечение профессиональной подготовки специалистов в соответствии с требованиями ФГОС ВО и учебного плана специальности 10.05.04 «Информационно-аналитические системы безопасности»; формирование у студентов обобщенного представления по следующим вопросам: - назначение политик информационной безопасности на предприятии; -требования к политике информационной безопасности; -стандарты информационной безопасности; - содержание политик информационной безопасности. Базисы. Руководства. Процедуры; - аудит проведения информационной безопасности на предприятии; административные политики (Governing Policy) информационной безопасности на предприятии; технические политики (Technical Policy) информационной безопасности на предприятии; политики информационной безопасности на предприятии конечного пользователя (End User Policy)

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО СПЕЦИАЛИТЕТА

Данная дисциплина относится к дисциплинам по выбору вариативной части Блока Б1 (код Б1.В.ДВ.3). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ. Дисциплина изучается на четвертом курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по курсам «Профессиональная работа на ПК», «Структуры данных» и «Основы информационной безопасности» «Информационные технологии» профессионального цикла по специальности 10.05.04 «Информационно-аналитические системы безопасности», квалификации - специалист.

Курс тесно взаимосвязан с другими дисциплинами данного цикла. Он является полезным для изучения таких дисциплин как «Безопасность информационных и аналитических систем», «Безопасность операционных систем», «Система защиты информации на предприятии» и др.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины студент должен обладать следующими профессиональными компетенциями:

ПК-9 – способностью выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах;

ПК-16 – способностью разрабатывать проекты нормативных, методических, организационно-распорядительных документов, регламентирующих функционирование специальных ИАС и средств обеспечения их информационной безопасности.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) ***Знать:*** понятия: «информационная технология», «информационная система», корпоративная информационная система, смысл и функции управления в КИС; особенности предприятия как сложного экономического объекта управления; задачи, решаемые с использованием политик безопасности КИС на различных уровнях управления; компоненты корпоративной информационной системы; современные технологии построения КИС; современные средства проектирования и создания КИС; пути достижения максимальной эффективности от внедрения КИС (ПК –9, ПК-16);

2) ***Уметь:*** анализировать процессы управления на различных уровнях корпоративных систем; анализировать специфику задач обеспечения безопасности в КИС и составления политик безопасности в КИС (ПК –9, ПК-16);

3) ***Владеть:*** навыками постановки задач управления на различных уровнях корпоративных систем; навыками моделирования бизнес-процессов в корпоративных системах; навыками выбора современных средств информационной безопасности КИС,

наиболее подходящих для решения задач управления конкретным предприятием; навыки составления политик безопасности различного уровня в КИС; навыки по планированию процесса внедрения КИС (ПК –9, ПК-16).

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

- способность осуществлять эксплуатационно-техническое обслуживание аппаратных средств и сопровождение программных продуктов современных систем мобильной передачи 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	Практические занятия	Лабораторные работы	Контрольные работы,	СРС	КП / КР		
1	Определение политики информационной безопасности. Назначение политик информационной безопасности предприятия	7	1-2	2		4		2		3 (50%)	-
2	Принципы политики ИБ. Требования к политике информационной безопасности.	7	3-4	2		4		2		2 (33%)	
3	Стандарты информационной безопасности	7	5-6	2		4		2		3 (50%)	Рейтинг-контроль №1
4	Этапы выработки политик информационной безопасности	7	7-8	2		4		2		2 (33%)	
5	Содержание политик информационной безопасности. Базисы. Руководства. Процедуры	7	9-10	2		4		2		2 (33%)	
6	Реализация политик информационной безопасности на предприятии. Аудит проведения информационной безопасности на предприятии	7	11-12	2		4		2		3 (50%)	Рейтинг-контроль №2
7	Административные политики (Governing Policy) ИБ на предприятии	7	13-14	2		4		2		3 (50%)	
8	Технические политики (Technical Policy) информационной безопасности на предприятии	7	15-16	2		4		2		2 (33%)	
9	Политики информационной безопасности на предприятии конечного пользователя (End User Policy)	7	17-18	2		4		2		3 (50%)	Рейтинг-контроль №3
Всего				18		36		18		23 (42%)	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 специалиста по специальности 10.05.04 «Информационно-аналитические системы 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:

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

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

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью ОПОП специальности 10.05.04 «Информационно-аналитические системы безопасности», особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом, в учебном процессе, они составляют не менее 30 процентов аудиторных занятий.

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

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

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

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

Примерный перечень заданий для текущих контрольных мероприятий:

Вопросы рейтинг-контроля №1

- Определение политики информационной безопасности.
- Назначение политик информационной безопасности предприятия
- Область применения политик информационной безопасности предприятия
- Принципы политики информационной безопасности.
- Ответственность за соблюдение политики информационной безопасности предприятия
- Требования к политике информационной безопасности.

Вопросы рейтинг-контроля №2

- Стандарты информационной безопасности
- Этапы выработки политик информационной безопасности
- Содержание политик информационной безопасности. Базисы.
- Содержание политик информационной безопасности. Руководства.
- Содержание политик информационной безопасности. Процедуры
- Реализация политик информационной безопасности на предприятии.

Вопросы рейтинг-контроля №3

- Аудит проведения информационной безопасности на предприятии
- Административные политики (Governing Policy) информационной безопасности на предприятии
- Технические политики (Technical Policy) информационной безопасности на предприятии
- Политики информационной безопасности на предприятии конечного пользователя (End User Policy)
- Реагирование на инциденты информационной безопасности на предприятии
- Правила внесения изменений в политику информационной безопасности предприятиия

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

1. Определение политики информационной безопасности.
2. Назначение политик информационной безопасности предприятия
3. Область применения политик информационной безопасности предприятия
4. Принципы политики информационной безопасности.
5. Ответственность за соблюдение политики информационной безопасности предприятия
6. Требования к политике информационной безопасности.
7. Стандарты информационной безопасности
8. Этапы выработки политик информационной безопасности
9. Содержание политик информационной безопасности. Базисы.
10. Содержание политик информационной безопасности. Руководства.
11. Содержание политик информационной безопасности. Процедуры
12. Реализация политик информационной безопасности на предприятии.
13. Аудит проведения информационной безопасности на предприятии
14. Административные политики (Governing Policy) информационной безопасности на предприятии
15. Технические политики (Technical Policy) информационной безопасности на предприятии
16. Политики информационной безопасности на предприятии конечного пользователя (End User Policy)
17. Реагирование на инциденты информационной безопасности на предприятии
18. Правила внесения изменений в политику информационной безопасности предприятиия

Темы лабораторных работ:

- Разработка политики использования ресурсов интернета.
- Разработка политики использования паролей.
- Разработка политики шифрования.
- Разработка политики антивирусной защиты.
- Разработка политики аудита информационной безопасности на предприятии
- Разработка политики для пограничных маршрутизаторов
- Разработка политики удаленного доступа
- Разработка политики построения виртуальных частных сетей
- Разработка политики внутренней сети
- Разработка политики демилитаризованной зоны
- Разработка политики для конфиденциальной информации

- Разработка политики защиты веб-сервера компании
- Разработка политики электронной почты компании
- Разработка политики межсетевого экранирования. ACL
- Разработка политики межсетевого экранирования. ZoneBased
- Разработка политики подключения новых устройств в корпоративную сеть
- Разработка политики использования ИМ
- Разработка политики использования съемных носителей

Вопросы и задания для самостоятельной работы студентов:

- Особенности разработки и содержание политики использования ресурсов интернета.
- Особенности разработки и содержание политики использования паролей.
- Особенности разработки и содержание политики шифрования.
- Особенности разработки и содержание политики антивирусной защиты.
- Особенности разработки и содержание политики аудита информационной безопасности на предприятии
- Особенности разработки и содержание политики для пограничных маршрутизаторов
- Особенности разработки и содержание политики удаленного доступа
- Особенности разработки и содержание политики построения виртуальных частных сетей
- Особенности разработки и содержание политики внутренней сети
- Особенности разработки и содержание политики демилитаризованной зоны
- Особенности разработки и содержание политики для конфиденциальной информации
- Особенности разработки и содержание политики защиты веб-сервера компании
- Особенности разработки и содержание политики электронной почты компании
- Особенности разработки и содержание политики межсетевого экранирования. ACL
- Особенности разработки и содержание политики межсетевого экранирования. ZoneBased
- Особенности разработки и содержание политики подключения новых устройств в корпоративную сеть
- Особенности разработки и содержание политики использования ИМ
- Особенности разработки и содержание политики использования съемных носителей
- Базовый комплект документов по информационной безопасности
- Безопасность персонала
- Документы, разрабатываемые при создании автоматизированной системы
- Документы, разрабатываемые при создании выделенного помещения
- План защиты информационных ресурсов от несанкционированного доступа
- Классификация защищаемой информации на предприятии
- Политика обеспечения физической защиты

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с. ISBN 978-5-8199-0411-4 Режим доступа: http://znanium.com/catalog.php?bookinfo=402686
2. Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности : 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
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. 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. Золотарев, В. В. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков: учеб. пособие/ В. В. Золотарев, Е. А. Данилова. - Красноярск :Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=463037
2. Моделирование процессов управления и принятия решений в условиях чрезвычайных ситуаций / Ямалов И.У. - М. : БИНОМ, 2015. - http://www.studentlibrary.ru/book/ISBN9785996325627.html. 291 с.
3. 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 сетевых решений/LAN» -Режим доступа: http://www.osp.ru/lan/current:
2. Электронный журнал «Корпоративные сети передачи данных» -Режим доступа: http://www.delpress.ru/

г) Программное обеспечение и Интернет-ресурсы:

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

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

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

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

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.04 "Информационно-аналитические системы безопасности", специализация «автоматизация информационно-аналитической деятельности»

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 28.12.2016 года
Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии по специальности 10.05.04 "Информационно-аналитические системы безопасности", специализация «автоматизация информационно-аналитической деятельности»

Протокол № 4 от 28.12.2016 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/
(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: _____