УП2012-15-16

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

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

(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	4/144	36		36	36	Экзамен
Итого	4/144	36		36	36	Экзамен

Владимир 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Программно-аппаратные средства защиты информации» являются обеспечение подготовки специалистов в соответствии с требованиями ФГОС ВО и учебного плана по специальности 10.05.04»Информационно-аналитические системы безопасности», формирования у студентов профессиональных навыков по эксплуатации и обслуживанию аппаратуры, оборудования и программного обеспечения, связанных с: -обеспечением безопасности данных; - шифрованием и защитой от несанкционированного доступа; -профессиональных навыков выявления и уничтожения компьютерных вирусов; - противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; -навыков работы со специальной технической литературой; -создание представления о принципах, методах и средствах выявления угроз безопасности информационных систем; -развитие способностей к логическому и алгоритмическому мышлению и осуществлению проверки защищенности объектов на соответствие требованиям нормативных документов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО СПЕЦИАЛИТЕТА

Данная дисциплина относится к обязательным дисциплинам Блока Б1 (код Б1.Б.23). 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 «Основы информационной безопасности», «Аппаратные средства вычислительной техники», «Криптографические методы защиты информации», «Техническая защита информации» по специальности 10.05.04 «Информационно-аналитические системы безопасности», квалификации - специалист.

Курс тесно взаимосвязан с другими дисциплинами. Он является полезным для изучения таких дисциплин как «Безопасность информационных и аналитических систем», «Служба информационной безопасности на предприятии», «Защита информации в корпоративных ИС», «Принципы построения, проектирования и эксплуатации автоматизированных информационных систем».

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ПК-10 – способностью осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС;

ПК-12 – способностью разрабатывать программное и иные виды обеспечения специальных ИАС.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) **Знать:** - основные средства и способы обеспечения информационной безопасности компьютерных систем; требования к защищенным АС; критерии оценки эффективности защищенности; типы и виды программных и программно-аппаратных систем защиты информации; методы идентификация пользователей КС-субъектов доступа к данным; средства и методы ограничения доступа к файлам; аппаратно-программные средства криптографической защиты информации; методы и средства ограничения доступа к компонентам ЭВМ; методы защиты программ от несанкционированного копирования, методы защиты программных средств от исследования (ПК-10; ПК-12);

2) **Уметь:** - квалифицированно оценивать область применения программно-аппаратного средства защиты с учетом специфика объекта защиты; применять средства ВТ, средства программирования для эффективной реализации аппаратно-программных

комплексов заданного качества и в заданные сроки; проводить испытания объектов профессиональной деятельности; производить установку, настройку и обслуживание программно-аппаратных средств защиты информации; ставить и решать задачи, возникающие в процессе проектирования, отладки, испытаний и эксплуатации системных программных средств (ПК-10; ПК-12);

3) **Владеть:** - навыками освоения, внедрения и сопровождения программно-аппаратных средств защиты информации на объектах различного типа; навыками сопровождения программно-аппаратных средств защиты информации; навыками консультирования персонала в процессе использования указанных средств (ПК-10; ПК-12).

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

- способность осуществлять эксплуатационно-техническое обслуживание программно-аппаратных комплексов защиты информации согласно требованиям нормативно-распорядительных документов и документации производителей оборудования.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 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	Введение (предмет и задачи программно-аппаратной защиты информации; методы и средства защиты информации и предотвращения несанкционированного доступа).	7	1	2				2		1/50%	
2	Идентификация и аутентификация	7	2	2		4		2		2/33%	
3	Процедура идентификации и аутентификации. Однофакторная и двухфакторная идентификации.	7	3	2				2		1/50%	
4	Биометрические методы идентификации и аутентификации.	7	4	2		4		2		2/33%	
5	Протоколы идентификации/аутентификации	7	5	2				2		1/50%	
6	Протоколы идентификации с нулевой передачей знаний	7	6	2		4		2		2/33%	Рейтинг-контроль №1
7	Система разграничения доступа к информации	7	7	2				2		1/50%	
8	Методы и средства защиты программ от компьютерных вирусов (характеристика и классификация компьютерных вирусов	7	8	2		4		2		2/33%	
9	Характеристика средств нейтрализации компьютерных вирусов	7	9	2				2		1/50%	
10	Технологии обнаружения вирусов; антивирусные комплексы	7	10	2		4		2		2/33%	
11	Оценка антивирусов. Требования к средствам антивирусной защиты ФСТЭК России, классификация методов защиты от компьютерных вирусов.	7	11	2				2		1/50%	
12	Общая характеристика программно-аппаратных средств защиты информации	7	12	2		4		2		2/33%	Рейтинг-контроль №2
13	Общая характеристика электронных идентификаторов	7	13	2				2		1/50%	
14	Защите программ от программных закладок	7	14	2		4		2		2/33%	

15	Методы вскрытия недекларированных возможностей; подходы выявления дефектов в программном обеспечении, возможные методы защиты.	7	15	2				2		1/50%	
16	Методы и способы защиты программ от исследования.	7	16	2		4		2		2/33%	
17	Подходы к защите программ от несанкционированного копирования.	7	17	2				2		1/50%	
18	Архитектура ПАСЗИ	7	18	2		4		2		2/33%	Рейтинг-контроль №3
Всего				36		36		36		27/37%	Экзамен

Содержание дисциплины «Программно-аппаратные средства защиты информации»

Раздел 1. Введение (предмет и задачи программно-аппаратной защиты информации; методы и средства защиты информации и предотвращения несанкционированного доступа).

Раздел 2. Идентификация и аутентификация (идентификация пользователей (субъектов доступа к данным).

Раздел 3. Процедура идентификации и аутентификации. Однофакторная и двухфакторная идентификации.

Раздел 4. Биометрические методы идентификации и аутентификации. Технологии автоматической идентификации.

Раздел 5. Протоколы идентификации/аутентификации (обобщенный алгоритм, на основе алгоритма RSA, схемы Фейге-Фиата-Шамира, Эль-Гамаля, Шнорра).

Раздел 6. Протоколы идентификации с нулевой передачей знаний. Протоколы Kerberos, S/Key (RFC 1760), PAP и CHAP, OpenID, Windows Live ID, LDAP, OpenLDAP.

Раздел 7. Система разграничения доступа к информации (архитектура системы; концепция построения систем разграничения доступа; модели разграничения доступа; надежность систем разграничения доступа).

Раздел 8. Методы и средства защиты программ от компьютерных вирусов (характеристика и классификация компьютерных вирусов.

Раздел 9. Характеристика средств нейтрализации компьютерных вирусов.

Раздел 10. Технологии обнаружения вирусов; антивирусные комплексы.

Раздел 11. Оценка антивирусов. Требования к средствам антивирусной защиты ФСТЭК России, классификация методов защиты от компьютерных вирусов.

Раздел 12. Общая характеристика программно-аппаратных средств защиты информации (классификация средств защиты; государственный реестр сертифицированных средств защиты информации; краткая характеристика средства защиты СЗИ Secret Net, ПАК Криптон, Honeypot Manager, КИБ SearchInform, Secret Disk и т.д.).

Раздел 13. Общая характеристика электронных идентификаторов (идентификаторы eToken, JaCarta, Maxim (iButton), Sentinel, Guardant, Rutoken, CmDongle, WibuKey, SenseLock, LOCK и т.д.).

Раздел 14. Защите программ от программных закладок (способы внедрения закладок; классификация недекларированных возможностей программного обеспечения).

Раздел 15. Методы вскрытия недекларированных возможностей; подходы выявления дефектов в программном обеспечении, возможные методы защиты.

Раздел 16. Методы и способы защиты программ от исследования.

Раздел 17. Подходы к защите программ от несанкционированного копирования.

Раздел 18. Архитектура ПАСЗИ (конфигурации средств защиты; методы реализации; функционал и особенности использования).

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:

- Предмет и задачи программно-аппаратной защиты информации.
- Идентификация пользователей (субъектов доступа к данным).
- Протоколы идентификации/аутентификации (обобщенный алгоритм).
- Протоколы идентификации/аутентификации (на основе алгоритма RSA).
- Протоколы идентификации/аутентификации (схема Фейге-Фиата-Шамира).
- Протоколы идентификации/аутентификации (схема Эль-Гамаля).
- Протоколы идентификации/аутентификации (схема Шнорра).
- Протоколы идентификации с нулевой передачей знаний.

- Протокол Kerberos.
- Протоколы S/Key (RFC 1760), PAP и CHAP.
- Протоколы OpenID, Windows Live ID.
- Протоколы LDAP, OpenLDAP.
- Единая система идентификации и аутентификации РФ.
- Система разграничения доступа к информации.

Вопросы рейтинг-контроля №2:

- Методы и средства защиты программ от компьютерных вирусов (список уточняется ежегодно).
  - Обзор продуктов компании AVG Technologies.
  - Обзор продуктов компании AVAST Software (ALWIL).
  - Обзор продуктов Avira GmbH.
  - Обзор продуктов BitDefender.
  - Обзор продуктов Dr.Web.
  - Обзор продуктов G Data Software AG.
  - Обзор продуктов Microsoft.
  - Обзор продуктов ESET.
  - Обзор продуктов Symantec.
  - Обзор продуктов Panda Security.
  - Обзор продуктов ЗАО «Лаборатория Касперского».
  - Обзор продуктов Agnitum Ltd.
  - Обзор продуктов McAfee.
  - и т.д.
- Программные и аппаратные средства защиты (список уточняется ежегодно по реестру ФСТЭК):
  - ПАК Соболь / Росомаха / Криптон.
  - АПКШ "Континент".
  - СЗИ vGate.
  - Honeypot Manager.
  - Система комплексного управления безопасностью КУБ.
  - СЗИ от НСД "Страж NT".
  - Программные комплексы защиты информации от НСД Dallas Lock.
  - Контур информационной безопасности SearchInform.
  - Средства контроля защищенности от несанкционированного доступа «АИСТ».
  - Средство фиксации и контроля исходного состояния программного комплекса "ФИКС".
  - Система защиты конфиденциальной информации и персональных данных от НСД и копирования Secret Disk.
  - Средство создания модели системы разграничения доступа «Ревизор-1» («Ревизор-2»).
  - Программное средство защиты информации от несанкционированного доступа «Эгида+».
  - Программное средство защиты информации «Crypton Lock».
  - CSP VPN Client /Server / Gate.
  - Программный комплекс DeviceLock
  - Комплексная система защиты от несанкционированного доступа Diamond ACS.
  - Сервер безопасности DioNIS.
  - Программный комплекс "InfoWatch Traffic Monitor"
  - Система контроля защищенности и соответствия стандартам «MaxPatrol».
  - Устройство предотвращения сетевых атак Proventia Network Intrusion Prevention System.
  - Система управления скрытой маркировкой печатных копий документов «SafeCopy».
  - Программно-аппаратный комплекс SafeNet.
  - ПО ViPNet.
  - Аппаратно-программный комплекс обнаружения компьютерных атак "Аргус".
  - Система защиты информации от несанкционированного доступа «Аура».
  - Программно-аппаратная система защиты информации от НСД «Блокхост-сеть».

- Программный комплекс «Электронный замок «Витязь».
- Пакет программ «ЗАСТАВА»
- Межсетевой экран с расширенной функциональностью, коммуникационный центр "ИВК Кольчуга".
- ПК «Анализатор программного кода «Квазар».
- Программное средство защиты информации «КРИПТОН-ЩИТ».
- Аппаратно-программный комплекс доверенной загрузки «Лабиринт-ДЗ».
- Аппаратно-программный комплекс «Панцирь».
- Программа поиска и гарантированного уничтожения на дисках «TERRIER».
- Программа фиксации и контроля исходного состояния программных комплексов «Трафарет».
- Анализатор исходных текстов программ «Тритон».
- Система обнаружения компьютерных атак «Форпост».
- Персональное средство криптографической защиты информации "Шипка".
- и т.д.

- Электронные идентификаторы:
- Компании "Аладдин Р.Д." (eToken).
- Компании "Аладдин Р.Д." (JaCarta).
- Компании "Аладдин Р.Д."/ Maxim (iButton).
- SafeNet (Sentinel).
- ЗАО «Актив-софт» (Guardant).
- ЗАО «Актив-софт» (Rutoken).
- WIBU-SYSTEMS AG (CmDongle).
- WIBU-SYSTEMS AG (WibuKey).
- ЗАО "Секьюлэб" (SenseLock).
- ООО "Астрома" (LOCK).

Вопросы рейтинг-контроля №3 (дополнительно к вопросам 1 и 2 рейтинг-контроля):

- Способы внедрения закладок.
- Классификация недекларированных возможностей программного обеспечения.
- Методы вскрытия недекларированных возможностей программного обеспечения.
- Подходы выявления дефектов в программном обеспечении.
- Методы и способы защиты программ от исследования.
- Подходы к защите программ от несанкционированного копирования.

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

Экзаменационный билет состоит из 4-х вопросов.

Вопросы 1 и 2:

1. Предмет и задачи программно-аппаратной защиты информации. Предмет и объект защиты. Методы и средства защиты информации и предотвращения доступа к ней.
2. Идентификация пользователей (субъектов доступа к данным). Идентификация, аутентификация и авторизация. Одно и двухфакторная идентификация. Типовой алгоритм аутентификации пользователей.
3. Идентификация пользователей (субъектов доступа к данным). Биометрические при-знаки, которые могут быть использованы при идентификации.
4. Технологий автоматической идентификации. Штриховые коды (символики). Радио-частотная идентификация.
5. Система разграничения доступа к информации. Функциональные блоки. Концепция построения.
6. Механизмы управления доступом (модели разграничения доступа). Дискреционное управление доступом.
7. Механизмы управления доступом (модели разграничения доступа). Мандатное управление доступом.

8. Механизмы управления доступом (модели разграничения доступа). Управление доступом на основе ролей.
9. Надежность систем разграничения доступа. Интенсивность отказов. Среднее время восстановления системы защиты после отказа.
10. Методы предотвращения утечек из КС. Классификация внутренних ИТ-угроз.
11. Методы предотвращения утечек из КС. Законный перехват данных.
12. Методы предотвращения утечек из КС. Обобщенный процесс выбора систем DLP.
13. Методы и средства защиты программ от компьютерных вирусов. Общая характеристика и классификация.
14. Методы и средства защиты программ от компьютерных вирусов. Общая характеристика средств нейтрализации компьютерных вирусов. Методы защиты от компьютерных вирусов.
15. Методы защиты программ от исследования. Сфера применения. Компоненты системы защиты и их функции.
16. Способы защиты программ от исследования. 4-е класса способов защиты.
Вопрос 3:
В приведенном далее списке укажите программно-аппаратные средства (минимум 3), которые могут использоваться:
1. для контроля утечек и каналов распространения защищаемой информации.
2. для разграничения доступа.
3. для организации доверенной загрузки вычислительной системы.
4. как электронный замок.
5. как межсетевые экраны.
6. для организация VPN.
7. для анализа исходных кодов программ с целью выявления закладок.
8. как средство фиксации состояния ПО.
и приведете описание их основных функций, сведения о наличии сертификатов ФСТЭК (класс защищенности АС, класс ИСПДн, уровень защищенности ИСПДн, уровень НДВ, класс МЭ, ОУД), ФСБ (наличие), Минобороны РФ (наличие).
ПАСЗИ (перечень уточняется по реестру ФСТЭК): CSP VPN Gate; CSP VPN Server; Honeypot Manager; ViPNet BOX; ViPNet CUSTOM; АПКШ Континент; ИВК Кольчуга; Комплекс DeviceLock; Комплекс Diamond VPN/FW; Комплекс Ideco ICS 3; Комплекс InfoWatch Traffic Monitor; Контур ИБ SearchInform; ПАК SafeNet; ПАК Аргус; ПАК Лабиринт-ДЗ; ПАК Панцирь; ПАК Соболь; ПАК Росомаха; ПАК Криптон; ПАК ФПСУ-IP; Па-кет программ "ЗАСТАВА"; ПКЗИ Dallas Lock; ПО TERRIER; ПО Ревизор-1 (Ревизор-2); ПО Трафа-рет; ПО Тритон; ПО ФИКС; Сервер DioNIS; СЗИ Crypton Lock; СЗИ Diamond ACS; СЗИ Secret Disk; СЗИ Secret Net; СЗИ TrustAccess; СЗИ vGate; СЗИ Аура; СЗИ Блокпост-2000/XP; СЗИ Блокхост-сеть; СЗИ Шипка; СЗИ Эгида+; Система КУБ; Система Форпост; СКЗ MaxPatrol; Устройство Proventia Network IPS.
Вопрос 4: Тест по программно-аппаратным средствам защиты информации.

Темы лабораторных работ:
1. Корпоративные межсетевые экраны на базе специализированных дистрибутивов;
2. межсетевые экраны на базе Linux;
3. Основы конфигурирования Netfilter/Iptables;
4. Средства межсетевого экранирования устройств Cisco. ACL;
5. Конфигурирование виртуальной частной сети (VPN);
6. Система обнаружения вторжений.

Самостоятельная работа студента предполагает индивидуальную работу с литературой при подготовке к лекциям и лабораторным занятиям. Контроль самостоятельной работы проводится в процессе сдачи лабораторных работ.

Вопросы и задания для самостоятельной работы студентов:

1) Системы биометрической идентификации.
2) Механизмы управления доступом (реализация в современных операционных системах).
3) Разработчики антивирусных средств защиты, ПО.
4) Программно-аппаратные средства защиты (средства криптографической защиты).
5) Программно-аппаратные средства защиты (средства защиты от несанкционированного доступа).
6) Программно-аппаратные средства защиты (средства защиты информации сетевого действия).
7) Системы централизованного управления учетными записями и правами доступа.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Башлы, П. Н. Информационная безопасность и защита информации: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=405000
2. Интеллектуальные системы защиты информации: учеб. пособие/ Васильев В.И. - 2-е изд., испр. и доп. - М: Машиностроение , 2013. - http://www.studentlibrary.ru/book/ISBN9785942756673.html 172 с.
3. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с., Режим доступа: http://znanium.com/catalog.php?bookinfo=489084

б) Дополнительная литература:

1. Система защиты информации от несанкционированного доступа на основе программно-аппаратного комплекса "Secret Net 5.0" / Помешкин А.А., Коротких И.В. - Новосиб.:НГТУ, 2012. - 47 с.: ISBN 978-5-7782-1990-8 Режим доступа: http://znanium.com/catalog.php?bookinfo=556699
2. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с., Режим доступа: http://znanium.com/catalog.php?bookinfo=405313
3. 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

в) Периодические издания:

1. Журнал «Защита информации. Инсайд» ISSN 2413-3582, Режим доступа: http://inside-zi.ru/pages/about.html;
2. 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/
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. Воронин А.А.
(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 28.12.16 года
Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

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

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/
(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: _____