2015

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего о 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

Технологии обеспечения информационной безопасности

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)
1	5/180	18	-	36	126	Зачет
2	2/72	-	-	36	-	Экзамен (36ч), КР
Итого	7/252	18	-	72	126	Зачет, экзамен (36ч), КР

ВЛАДИМИР 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Технологии обеспечения информационной безопасности» 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 теоретических знаний и практических навыков по обеспечению информационной безопасности в компьютерных системах.

Учебный курс позволяет получить знания по основным историческим аспектам, теоретическим положениям, технологиям, операциям, практическим методам и приемам проведения научных исследований на базе современных достижений отечественных и зарубежных ученых и овладеть навыками выбора темы научного исследования, научного поиска, анализа, экспериментирования, обработки данных, получения обоснованных эффективных решений с использованием информационных технологий. Изучение дисциплины обеспечивает прикладные научно-методические основы подготовки магистранта. Она способствует формированию у обучаемых научного подхода к исследованию процессов информационной безопасности. Знакомит с методами организации и проведения научных исследований. Задачами дисциплины «Технологии обеспечения информационной безопасности» являются: освоение принципов реализации и основных подходов к оптимальному управлению различными механизмами информационной безопасности в компьютерных системах. В процессе освоения дисциплины изучаются следующие вопросы: - основные руководящие документы и показатели эффективности системы защиты информации; -комплексный подход к обеспечению ИБ; -цели, стратегии и политика информационной безопасности; -организационные аспекты информационной безопасности; - функции управления информационной безопасностью; - процессный подход для управления информационной безопасностью; - система ответственности в области информационной безопасности; -организация и методика проведения аудита системы управления информационной безопасностью; -алгоритм проведения анализа информационных рисков в КИС предприятия; -аналитические технологии управления ИБ

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО МАГИСТРАТУРЫ

Данная дисциплина относиться к базовой части Блока Б1 (код Б1.Б.4). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ, ориентированных на освоение данной дисциплины магистрантами.

Профессиональное освоение данной учебной дисциплины предусматривает предварительное или параллельное глубокое основательное изучение и освоение таких общепризнанных, стандартных общих математических и естественнонаучных дисциплин, как высшая математика, информатика, концепции современного естествознания, основы стандартизации и компьютерное делопроизводство. Курс тесно взаимосвязан с другими дисциплинами данного цикла. Он изучается в комплексе с такими дисциплинами как «Анализ и моделирование информационно-телекоммуникационных сетей», «Методология информационной безопасности». Кроме того, курс полезен для изучения таких смежных дисциплин как «Управление информационной безопасностью», «Методы информационно-аналитической работы»; «Модели и методы планирования экспериментов, обработки экспериментальных данных».

Требования к «входным» знаниям, умениям и готовностям обучающегося определяются требованиями к уровню подготовки выпускника бакалавриата 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.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

ПК-1 – способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-2 – способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

ПК-3 – способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) ***Знать:*** - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; - методы концептуального проектирования технологий обеспечения информационной безопасности; - основные угрозы безопасности информации и модели нарушителя в компьютерных системах; принципы формирования политики информационной безопасности в компьютерных системах; - методы аттестации уровня защищенности компьютерных систем; - основные методы управления информационной безопасностью (ПК-1; ПК-2; ПК-3);

2) ***Уметь:*** - осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; - организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности;- разрабатывать модели угроз и нарушителей информационной безопасности компьютерных систем; - разрабатывать частные политики информационной безопасности компьютерных х систем; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности компьютерных систем; - оценивать информационные риски в компьютерных системах; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерных систем; - составлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем (ПК-1; ПК-2; ПК-3);

3) ***Владеть:*** - методами и средствами выявления угроз безопасности информационным системам; - навыками выбора и обоснования критериев эффективности функционирования защищенных компьютерных систем; - навыками участия в экспертизе состояния защищенности информации на объекте защиты; - методами управления информационной безопасностью компьютерных систем; - методами оценки информационных рисков; - методами организации и управления деятельностью служб защиты информации на предприятии; - навыками организации и обеспечения режима секретности; - навыками управления информационной безопасностью простых объектов (ПК-1; ПК-2; ПК-3).

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

- способность разрабатывать, оформлять и реализовывать политики информационной безопасности для современных компьютерных систем.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 7 зачетных единиц, 252 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. Основные технические сервисы защиты информации в компьютерных системах.	1	1-2	2		4		14		3 (50%)	
2	"Слабые" протоколы аутентификации Парольная аутентификация	1	3-4	2		4		14		2 (33%)	
3	Двухфакторная аутентификация PIN-коды и одноразовые пароли.	1	5-6	2		4		14		2 (33%)	Рейтинг-контроль №1
4	"Сильные" протоколы аутентификации Протоколы типа "запрос-ответ".	1	7-8	2		4		14		2 (33%)	
5	Протоколы аутентификации с нулевым разглашением.	1	9-10	2		4		14		3 (50%)	
6	Модели контроля доступа в компьютерных системах. Общие сведения о задаче КД.	1	11-12	2		4		14		2 (33%)	Рейтинг-контроль №2
7	Дискреционное управление доступом.	1	13-14	2		4		14		3 (50%)	
8	Мандатное управление доступом.	1	15-16	2		4		14		2 (33%)	
9	Ролевое разграничение доступа. Модель администрирования РРД, дискреционная и мандатная модели	1	17-18	2		4		14		3 (50%)	Рейтинг-контроль №3

Всего				18		36		126		22 (41%)	Зачет
10	Построение проекта архитектуры сервиса хранения файлов в защищенном исполнении.	2	1-2	-		4				2 (50%)	
11	Разработка технического задания на сервис хранения файлов в защищенном исполнении.	2	3-4	-		4				2 (50%)	
12	Реализация каркаса приложений клиента и сервера для хранения файлов.	2	5-6	-		4				2 (50%)	Рейтинг-контроль №1
13	Разработка протокола обмена сообщениями между клиентом и сервером.	2	7-8	-		4				2 (50%)	
14	Реализация модуля шифрования содержимого базы данных.	2	9-10	-		4				2 (50%)	
15	Реализация модели контроля доступа.	2	11-12	-		4				2 (50%)	Рейтинг-контроль №2
16	Реализация модуля аутентификации	2	13-14	-		4				2 (50%)	
17	Реализация административных процедур для сервиса хранения файлов в защищенном исполнении	2	15-16	-		4				2 (50%)	
18	Тестирование сервиса хранения файлов в защищенном исполнении	2	17-18	-		4				2 (50%)	Рейтинг-контроль №3
Всего						36			КР	18 (50%)	Экзамен
Итого				18		72		126		40 (44%)	Зачет, экзамен, КР

««Технологии обеспечения информационной безопасности»»

Краткое содержание курса

1. Введение. Основные технические сервисы защиты информации в компьютерных системах. Принципы построения программных продуктов в защищенном исполнении. Идентификация, аутентификация и контроль доступа. Защита распределенных информационных систем и обеспечение безопасности взаимодействия компонентов этих систем.

2. "Слабые" протоколы аутентификации. Парольная аутентификация. Проблема хранения и передачи паролей. Хеширование паролей. Использование имитовставки для повышений стойкости к подбору паролей. Парольная политика.

3. Двухфакторная аутентификация. PIN-коды и одноразовые пароли. Вычисляемые ключи. Схема Лэмпорта. Атаки подбора паролей напрямую, по словарю, гибридная атака, атака повтора пароля, pass the hash.

4. "Сильные" протоколы аутентификации. Протоколы типа "запрос-ответ". Аутентификация на основе симметричного и асимметричного шифрования. Протоколы ISO 9798, схема Нидхэма-Шрёдера. Применение "сильных" схем аутентификации в аппаратных ключах.

5. Протоколы аутентификации с нулевым разглашением. Протокол Фиата-Шамира, Фейге-Фиата-Шамира. Схема GQ, протокол аутентификации Шнорра. Атаки на протоколы аутентификации: атака имперсонации, повторной отправки, атаки перемежения, отражения, вынужденной задержки и т.д.

6. Модели контроля доступа в компьютерных системах. Общие сведения о задаче контроля доступа. Классификация моделей управления доступом. Автоматная модель доступов в информационной системе. Понятия субъекта и объекта доступа. Каналы утечки по памяти и по времени.

7. Дискреционное управление доступом. Матрица доступа. Модель Харрисона-Руззо-Ульмана. Понятие утечки права. Модель типизированной матрицы доступов. Понятие передачи прав. Базовая и расширенная модель take-grant. Вопросы вычислительной сложности определения возможности утечки права.

8. Мандатное управление доступом. Понятие решетки уровней конфиденциальности. Модель Белла-Лападула. Политика high-watermark и low-watermark. Модель контроля целостности Биба. Вопросы вычислительной сложности верификации исходных условий в мандатном управлении доступом.

9. Ролевое разграничение доступа. Модель администрирования РРД, дискреционная и мандатная модели ролевого разграничения доступа. Контроль доступа в современных информационных системах.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины «Технологии защиты информации в компьютерных системах» 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 к рейтинг-контролю 1 семестр:

Вопросы к рейтинг-контролю №1 семестр 1

1. Основные технические сервисы защиты информации в компьютерных системах.
2. Принципы построения программных продуктов в защищенном исполнении.
3. Идентификация, аутентификация и контроль доступа.
4. Защита распределенных информационных систем и обеспечение безопасности взаимодействия компонентов этих систем.
5. "Слабые" протоколы аутентификации.

6. Парольная аутентификация.
7. Проблема хранения и передачи паролей.
8. Хеширование паролей.
9. Использование имитовставки для повышения стойкости к подбору паролей.
10. Парольная политика.

Вопросы к рейтинг-контролю №2 семестр 1

1. Двухфакторная аутентификация.
2. PIN-коды и одноразовые пароли.
3. Вычисляемые ключи.
4. Схема Лэмпорта.
5. Атаки подбора паролей напрямую.
6. Атаки подбора паролей по словарю.
7. Гибридная атака, атака повтора пароля, pass the hash.
8. "Сильные" протоколы аутентификации.
9. Протоколы типа "запрос-ответ".
10. Аутентификация на основе симметричного шифрования

Вопросы к рейтинг-контролю №3 семестр 1

1. Аутентификация на основе асимметричного шифрования.
2. Протоколы ISO 9798
3. Схема Нидхэма-Шрёдера.
4. Применение "сильных" схем аутентификации в аппаратных ключах.
5. Протоколы аутентификации с нулевым разглашением.
6. Протокол Фиата-Шамира.
7. Протокол Фейге-Фиата-Шамира.
8. Схема GQ
9. Протокол аутентификации Шнорра.
10. Атаки на протоколы аутентификации.

Вопросы к рейтинг-контролю 2семестр:

Вопросы к рейтинг-контролю №1 семестр 2

1. Атака имперсонации
2. Атака повторной отправки
3. Атаки перемежения.
4. Атаки отражения
5. Атака вынужденной задержки
6. Модели контроля доступа в компьютерных системах
7. Задача контроля доступа.
8. Классификация моделей управления доступом.
9. Автоматная модель доступов в информационной системе.
10. Понятия субъекта и объекта доступа.

Вопросы к рейтинг-контролю №2. семестр 2

1. Канал утечки по памяти
2. Канал утечки по времени
3. Дискреционное управление доступом.
4. Матрица доступа.
5. Модель Харрисона-Руззо-Ульмана.
6. Понятие утечки права.
7. Модель типизированной матрицы доступов.
8. Понятие передачи прав.
9. Базовая и расширенная модель take-grant.
10. Мандатное управление доступом.

Вопросы к рейтинг-контролю №3 семестр 2

1. Понятие решетки уровней конфиденциальности.

2. Модель Белла-Лападула.
3. Политика high-watermark и low-watermark.
4. Модель контроля целостности Биба.
5. Вопросы вычислительной сложности верификации исходных условий в мандатном управлении доступом.
6. Ролевое разграничение доступа.
7. Модель администрирования РРД,
8. Дискреционная модель ролевого разграничения доступа.
9. Мандатная модель ролевого разграничения доступа
10. Контроль доступа в современных информационных системах.

Перечень вопросов к зачету 1 семестр: (промежуточной аттестации по итогам освоения дисциплины):

- Основные технические сервисы защиты информации в компьютерных системах.
- Принципы построения программных продуктов в защищенном исполнении.
- Идентификация, аутентификация и контроль доступа.
- Защита распределенных информационных систем и обеспечение безопасности взаимодействия компонентов этих систем.
- "Слабые" протоколы аутентификации.
- Парольная аутентификация.
- Проблема хранения и передачи паролей.
- Хеширование паролей.
- Использование имитовставки для повышения стойкости к подбору паролей.
- Парольная политика.
- Двухфакторная аутентификация.
- PIN-коды и одноразовые пароли.
- Вычисляемые ключи.
- Схема Лэмпорта.
- Атаки подбора паролей напрямую.
- Атаки подбора паролей по словарю.
- Гибридная атака, атака повтора пароля, pass the hash.
- "Сильные" протоколы аутентификации.
- Протоколы типа "запрос-ответ".
- Аутентификация на основе симметричного шифрования
- Аутентификация на основе асимметричного шифрования.
- Протоколы ISO 9798
- Схема Нидхэма-Шрёдера.
- Применение "сильных" схем аутентификации в аппаратных ключах.
- Протоколы аутентификации с нулевым разглашением.
- Протокол Фиата-Шамира.
- Протокол Фейге-Фиата-Шамира.
- Схема GQ
- Протокол аутентификации Шнорра.
- Атаки на протоколы аутентификации.

Перечень вопросов к экзамену 2 семестр: (промежуточной аттестации по итогам освоения дисциплины):

1. Идентификация, аутентификация и контроль доступа.
2. Модель нарушителя в компьютерных системах.
3. Основные сценарии атак в компьютерных системах.
4. Хэширование паролей

5. Хранение паролей.
6. Сложность подбора пароля.
7. Двухфакторная аутентификация.
8. Схема Лэмпорта
9. Одноразовые пароли с доставкой по выделенному каналу связи
10. Парольная политика.
11. Использование "соли" для предотвращения атаки подбора пароля
12. Атаки повтора пароля и pass the hash
13. Схемы аутентификации ISO 9798
14. Основные принципы "сильной" аутентификации
15. Протокол Диффи-Хеллмана
16. Схема Нидхэма-Шредера
17. Аутентификация в аппаратных токенах
18. Особенности доверенной третьей стороны в протоколах аутентификации
19. Принципы протоколов с нулевым разглашением
20. Протокол Фиата-Шамира
21. Протокол Фейге-Фиата-Шамира
22. Протокол GQ
23. Протокол Шнорра
24. Атаки на протоколы аутентификации
25. Задача контроля доступа
26. Основные принципы управления доступом в компьютерных системах
27. Понятие субъекта и объекта доступа
28. Каналы утечки по памяти и по времени
29. Классификация моделей управления доступом
30. Матрица доступа
31. Модель Харрисона-Руззо-Ульмана
32. Утечка права
33. Вычислительная сложность верификации по дискреционным моделям
34. Модель типизированной матрицы доступов
35. Модель take-grant
36. Решетка уровней конфиденциальности
37. Модель Белла-Лападула
38. Модель целостности Биба
39. Политика high-watermark и low-watermark
40. Дискреционное ролевое разграничение доступа
41. Мандатное ролевое разграничение доступа
42. Управление доступом в современных информационных системах

Темы лабораторных работ 1 семестр:

Лабораторная работа №1. Создание программного модуля парольной аутентификации. Пароль передается и хранится в виде значения односторонней функции от строки, введенной пользователем. Хранение пароля следует осуществлять в зашифрованном key-value хранилище.

Лабораторная работа №2. Создание программного модуля двухфакторной аутентификации по схеме Лэмпорта с генерацией одноразовых паролей. Пароль передается и хранится в виде значения односторонней функции от строки, введенной пользователем. Хранение пароля следует осуществлять в зашифрованном key-value хранилище.

Лабораторная работа №3. Создание программного модуля генерации пары ключей для асимметричных криптосистем. Пара ключей должна быть снабжена сертификатом формата X.509. Размер ключа принять равным или более 128 бит.

Лабораторная работа №4. Создание программного модуля, поддерживающего протоколы аутентификации стандарта 9798-2 и 9798-3. Транзакции следует осуществлять поверх протокола безопасности транспортного уровня TLS. Для реализации криптографических примитивов рекомендуется воспользоваться библиотекой OpenSSL.

Лабораторная работа №5. Создание программного модуля, поддерживающего один из протоколов аутентификации с нулевым разглашением (на выбор). Протестировать его в отношении технологической устойчивости к основным атакам на схемы аутентификации.

Темы лабораторных работ 2 семестр:

Лабораторная работа №1. Построение проекта архитектуры сервиса хранения файлов в защищенном исполнении. Сервис должен поддерживать шифрование файлов, аутентификацию с нулевым разглашением и мандатную модель контроля доступа.

Лабораторная работа №2. Разработка технического задания на сервис хранения файлов в защищенном исполнении. Сервис должен иметь возможность параллельной работы более 10 клиентов и предусматривать возможность передачи файлов между пользователями.

Лабораторная работа №3. Реализация каркаса приложений клиента и сервера для хранения файлов. Проектирование пользовательского интерфейса для клиента и сервера.

Лабораторная работа №4. Разработка протокола обмена сообщениями между клиентом и сервером. Разработка и реализация структуры базы данных для хранения файлов и пользовательских данных.

Лабораторная работа №5. Реализация модуля шифрования содержимого базы данных. Оценка утечки данных в случае компрометации клиента, сервера, пользовательских аутентификаторов, канала связи.

Лабораторная работа №6. Реализация модели контроля доступа. Написание методов для основных процедур передачи прав, назначения мандатов субъектов и объектов, сброса мандатов в соответствии с политикой low-watermark

Лабораторная работа №7. Реализация модуля аутентификации. Написание процедур, осуществляющих создание и хранение аутентификаторов пользователей. Реализация защищенного обмена аутентификаторами.

Лабораторная работа №8. Реализация административных процедур для сервиса хранения файлов в защищенном исполнении - создания, удаления пользователей, выделения им дисковой квоты и т. д.

Лабораторная работа №9. Тестирование сервиса хранения файлов в защищенном исполнении, в том числе и в отношении технологической устойчивости к основным атакам на схемы аутентификации.

Задание к курсовой работе 2 семестр:

Курсовая работа заключается в создании программного комплекса, реализующего защищенное хранение файлов. Программный комплекс должен быть реализован с использованием архитектуры "клиент-сервер" и содержать механизмы аутентификации, шифрования и управления доступом.

Протокол аутентификации с нулевым разглашением, используемая криптосистема и модель контроля доступа выбирается по желанию студента из рассмотренных в курсе лекций.

Работу можно разбить на ряд этапов:

- построение проекта архитектуры сервиса хранения файлов;
- разработку технического задания на сервис хранения файлов;
- реализацию каркаса приложений клиента и сервера для хранения файлов;
- проектирование пользовательского интерфейса для клиента и сервера;
- реализацию модуля шифрования содержимого базы данных;
- написание методов для основных процедур передачи прав, назначения мандатов субъектов и объектов, сброса мандатов в соответствии с политикой low-watermark;

- реализацию модуля аутентификации;
- реализацию административных процедур для сервиса;
- тестирование и отладку.

Вопросы и задания к самостоятельной работе магистрантов 1 семестр:

- Принципы и технологии построения DLP-систем.
- Аппаратные и программные межсетевые экраны
- Системы протоколирования событий в информационных системых
- Ролевое разграничение доступа в СУБД Oracle
- Ролевое разграничение доступа в СУБД MS SQL Server
- Экранирование и фильтрация запросов на уровне приложений
- Алгоритм шифрования AES
- Протоколы безопасности транспортного уровня
- Протокол аутентификации LDAP
- Протокол аутентификации Kerberos
- Система аутентификации Radius
- Single Sign-on в Windows-сетях
- Способы организации сессий в Web-сервисах
- Аутентификация в Web-сервисах
- Протокол Oauth2
- Способы хранения аутентификаторов в Windows
- Способы хранения аутентификаторов в GNU/Linux
- Контексты безопасности SELinux
- Модель изолированной программной среды
- Модель системы военных сообщений
- Модель Кларка-Уилсона
- Атаки типа "человек посередине"
- Аппаратные ключи eToken
- Виды программных закладок и бэкдоров.
- Протокол Диффи-Хеллмана
- Схема Нидхэма-Шредера
- Аутентификация в аппаратных токенах
- Особенности доверенной третьей стороны в протоколах аутентификации
- Принципы протоколов с нулевым разглашением
- Протокол Фиата-Шамира
- Протокол Фейге-Фиата-Шамира
- Протокол GQ
- Протокол Шнорра
- Атаки на протоколы аутентификации
- Задача контроля доступа
- Основные принципы управления доступом в компьютерных системах
- Понятие субъекта и объекта доступа
- аналы утечки по памяти и по времени
- Классификация моделей управления доступом
- Матрица доступа
- Модель Харрисона-Руззо-Ульмана
- Утечка права
- Вычислительная сложность верификации по дискреционным моделям
- Модель типизированной матрицы доступов
- Модель take-grant

- Решетка уровней конфиденциальности
- Модель Белла-Лападула
- Модель целостности Биба
- Политика high-watermark и low-watermark
- Дискреционное ролевое разграничение доступа
- Мандатное ролевое разграничение доступа
- Управление доступом в современных информационных системах

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Башлы, П. Н. Информационная безопасность и защита информации: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2 Режим доступа: http://znanium.com/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. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с. ISBN 978-5-8199-0331-5, Режим доступа: http://znanium.com/catalog.php?bookinfo=423927

4. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. ISBN 978-5-369-01378-6, Режим доступа: http://znanium.com/catalog.php?bookinfo=474838

б) Дополнительная литература:

1. Корпоративные информационные системы управления: Учебник / Под науч. ред. Н.М. Абдикеева, О.В. Китовой. - М.: НИЦ ИНФРА-М, 2014. - 464 с. ISBN 978-5-16-003860-5, Режим доступа: http://znanium.com/

2. 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

3. Информационная система предприятия: Учебное пособие/Вдовенко Л. А. - 2 изд., перераб. и доп. - М.: Вузовский учебник, НИЦ ИНФРА-М, 2015. - 304 с. ISBN 978-5-9558-0329-6, Режим доступа http://znanium.com/catalog.php?bookinfo=501089

4. Проектирование информационных систем: Учебное пособие / Н.Н. Заботина. - М.: НИЦ Инфра-М, 2013. - 331 с.: Режим доступа: http://znanium.com/catalog.php?bookinfo=371912

в) Периодические издания:

1. Информационно-методический журнал «Защита информации. Конфидент» http://sec4all.net/konfj-5_03.html

2. Научный журнал «Проблемы машиностроения и автоматизации» Режим доступа: http://ores.su/ru/journals/problemyi-mashinostroeniya-i-avtomatizatsii/

3. Каталог журналов в области охраны и безопасности. http://secandsafe.ru/jurnaly/

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. Тельный А.В.

(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 № 4 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 10.043.01 «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/

(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: _____