

Аннотация программы дисциплины:
«Авторское право в информационной безопасности»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Авторское право в информационной безопасности.

2. Место дисциплины в структуре ОП

Дисциплина «Авторское право в информационной безопасности» относится к числу учебных дисциплин дисциплины по выбору студента Б.1.2 блока Б.1 образовательной программы (Б.1.ДВ.4).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Авторское право в информационной безопасности» студенты должны:

знать:

- Технические и программные методы защиты авторских прав
- Основные права программного обеспечения
- Субъекты авторского права в информационной безопасности
- Объекты авторского права в информационной безопасности
- Законодательство по авторскому праву в информационной безопасности

уметь:

- Защищать свои и чужие авторские права в информационной безопасности
- Анализировать ситуации, возникшие в области авторского права в информационной безопасности

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	8
Практические занятия	
Лабораторные занятия	28
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Зачеты

Аннотация программы дисциплины:
«Администрирование серверов»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Администрирование серверов.

2. Место дисциплины в структуре ОП

Дисциплина «Администрирование серверов» относится к числу учебных дисциплин базовой части Б.1.1 блока Б.1 образовательной программы (Б.1.1.1).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Администрирование серверов» студенты должны:

знать:

- Современные подходы к администрированию серверов
- Базовые методологии и принципы в администрировании серверов
- Архитектуру серверов
- Существующее программное обеспечение для администрирования серверов

уметь:

- Организовывать оптимальную серверную архитектуру
- Настраивать производительность и устойчивость систем
- Решать технические проблемы
- Диагностировать и устранять инциденты в работе серверных ОС

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	
Практические занятия	
Лабораторные занятия	36
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Зачеты

Аннотация программы дисциплины:
«Архитектура безопасности облачных систем»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Архитектура безопасности облачных систем.

2. Место дисциплины в структуре ОП

Дисциплина «Архитектура безопасности облачных систем» относится к числу учебных дисциплин вариативной части Б.1.2 блока Б.1 образовательной программы (Б.1.2.9).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Архитектура безопасности облачных систем» студенты должны:

знать:

- Принципы построения и требования безопасности облачных систем
- Современные разновидности архитектур облачных систем
- Свойства архитектуры безопасности облачных систем
- Тенденции облачных систем на современном рынке
- Технические характеристики аппаратных и программных средств, используемых для построения облачных систем

уметь:

- Ориентироваться в современных аппаратных и программных средствах облачных систем
- Выявлять ключевые аспекты безопасности облачных систем
- Строить архитектуру безопасности облачных систем

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	22
В том числе	
Лекции	4
Практические занятия	
Лабораторные занятия	18
Самостоятельная работа	50
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Экзамены

Аннотация программы дисциплины:
«Аспекты веб-безопасности в социальных сетях»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Аспекты веб-безопасности в социальных сетях.

2. Место дисциплины в структуре ОП

Дисциплина «Аспекты веб-безопасности в социальных сетях» относится к числу учебных дисциплин дисциплины по выбору студента Б.1.2 блока Б.1 образовательной программы (Б.1.ДВ.3).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Аспекты веб-безопасности в социальных сетях» студенты должны:

знать:

- Современные социальные сети и принципы их построения
- Механизмы защиты в социальных сетях
- Методику обнаружения угроз в социальных сетях
- Функционал социальных сетей и как он работает

уметь:

- Вовремя реагировать на инциденты безопасности в социальных сетях
- Отличать реальную социальную сеть от подделки

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	8
Практические занятия	
Лабораторные занятия	28
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Зачеты

Аннотация программы дисциплины:
«Безопасность ПО»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Безопасность ПО.

2. Место дисциплины в структуре ОП

Дисциплина «Безопасность ПО» относится к числу учебных дисциплин вариативной части Б.1.2 блока Б.1 образовательной программы (Б.1.2.7).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Безопасность ПО» студенты должны:

знать:

- Основные понятия информационной безопасности и защиты информации
- Источники, риски, формы атак на информацию
- Политику и стандарты безопасности
- Методы обеспечения надежности программ
- Правовую и организационную поддержку процессов разработки и применения программного обеспечения.

уметь:

- Инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства защиты программного обеспечения
- Осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных средств защиты
- Устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	
Практические занятия	
Лабораторные занятия	36
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Зачеты

Аннотация программы дисциплины:
«Введение в безопасность персональных данных»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Введение в безопасность персональных данных.

2. Место дисциплины в структуре ОП

Дисциплина «Введение в безопасность персональных данных» относится к числу учебных дисциплин вариативной части Б.1.2 блока Б.1 образовательной программы (Б.1.2.5).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Введение в безопасность персональных данных» студенты должны:

Знать:

- Понятий аппарат безопасности информации
- Основы понятия о персональных данных
- Организационное обеспечение информационной безопасности и защиты персональных данных

Уметь:

- Оценивать угрозы защищаемой информации
- Проводить анализ каналов несанкционированного получения информации и причин нарушения целостности информации
- Организовывать защиту информации на объектах её обработки
- Организовывать работы по выявлению угроз безопасности информации на объектах информатизации
- Планировать, организовывать и контролировать выполнение мероприятий по технической защите конфиденциальной информации
- Разрабатывать необходимые документы по организации технической защиты конфиденциальной информации
- Оценивать эффективность защиты конфиденциальной информации

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36

В том числе	
Лекции	8
Практические занятия	
Лабораторные занятия	28
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Зачеты

Аннотация программы дисциплины:
«Веб-разработка»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Веб-разработка.

2. Место дисциплины в структуре ОП

Дисциплина «Веб-разработка» относится к числу учебных дисциплин базовой части Б.1.1 блока Б.1 образовательной программы (Б.1.1.3).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Веб-разработка» студенты должны:
знать:

- Этапы решения задачи на компьютере
- Типы данных
- Базовые конструкции изучаемых языков программирования
- Принципы структурного и модульного программирования
- Принципы объектно – ориентированного программирования.

уметь:

- Работать в среде программирования
- Реализовывать построенные алгоритмы в виде программ на конкретном языке программирования
- Создавать Web-страницы и узлы.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	
Практические занятия	
Лабораторные занятия	36
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Зачеты

Аннотация программы дисциплины:
«Выпускная квалификационная работа»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Выпускная квалификационная работа.

2. Место дисциплины в структуре ОП

Дисциплина «Выпускная квалификационная работа» относится к числу учебных дисциплин государственная итоговая аттестация Б.3.1 блока Б.3 образовательной программы (Б.3.1).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Выпускная квалификационная работа» студенты должны:

знать:

- Задачу и цель выпускной квалифицированной работы
- Средства, для написания выпускной квалификационной работы
- Алгоритм решения задачи
- Предметную область, актуальность и ценность выпускной квалификационной работы
- Сроки выполнения выпускной квалификационной работы

уметь:

- Вовремя завершить выполнение выпускной квалификационной работы
- Представить выпускную квалификационную работу
- Защитить выпускную квалификационную работу
- Использовать полученные знания в ходе выполнения выпускной квалификационной работы, на практике

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	(6 з.е.)
Аудиторные занятия (всего)	
В том числе	
Лекции	
Практические занятия	
Лабораторные занятия	
Самостоятельная работа	

Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	

Аннотация программы дисциплины:
«Законодательство в сфере защиты информации и обработки данных»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Законодательство в сфере защиты информации и обработки данных.

2. Место дисциплины в структуре ОП

Дисциплина «Законодательство в сфере защиты информации и обработки данных» относится к числу учебных дисциплин вариативной части Б.1.2 блока Б.1 образовательной программы (Б.1.2.10).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Законодательство в сфере защиты информации и обработки данных» студенты должны:

знать:

- Требования законодательной и нормативной правовой базы, регламентирующей защиту информации
- Классификацию угроз безопасности данных и каналы утечки информации
- Основные этапы организации обработки и защиты информации
- Основные методы, способы, программно-аппаратные и технические средства защиты информации.

уметь:

- Ориентироваться в системе законодательства и нормативных правовых актов, регламентирующих область ИС (в том числе сферу защиты информации в ИС)
- Использовать правовые нормы в сфере информационной безопасности
- Определять актуальные источники угроз безопасности для различных профессиональных областей.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	8
Практические занятия	
Лабораторные занятия	28
Самостоятельная работа	36

Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Экзамены

Аннотация программы дисциплины:
«Защита интеллектуальной собственности в информационной безопасности»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Защита интеллектуальной собственности в информационной безопасности.

2. Место дисциплины в структуре ОП

Дисциплина «Защита интеллектуальной собственности в информационной безопасности» относится к числу учебных дисциплин дисциплины по выбору студента Б.1.2 блока Б.1 образовательной программы (Б.1.ДВ.4).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Защита интеллектуальной собственности в информационной безопасности» студенты должны:

знать:

- Основные положения, понятия и категории законодательства Российской Федерации в области защиты интеллектуальной собственности
- Основные нормы международного права в области защиты интеллектуальной собственности
- Содержание институтов права интеллектуальной собственности
- Основные виды преступлений и правонарушений в информационной сфере • Относительно интеллектуальной собственности и авторских прав
- Основные подходы к принятию решений по выработке мер предупреждения право нарушений интеллектуальных прав в профессиональной деятельности.

уметь:

- Самостоятельно принимать решения по применению правовых норм и правил защиты права собственности, иных прав участников информационного обмена
- Применять организационно-правовые механизмы защиты интеллектуальной собственности
- Пользоваться информационно- правовыми системами для организации защиты результатов интеллектуальной деятельности
- Оформлять необходимую документацию для организации защиты результатов интеллектуальной деятельности.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	8
Практические занятия	
Лабораторные занятия	28
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Зачеты

Аннотация программы дисциплины:
«Защищенные информационные системы»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Защищенные информационные системы.

2. Место дисциплины в структуре ОП

Дисциплина «Защищенные информационные системы» относится к числу учебных дисциплин базовой части Б.1.1 блока Б.1 образовательной программы (Б.1.1.6).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Защищенные информационные системы» студенты должны:

знать:

- Современную классификацию средств защиты информации в корпоративных вычислительных сетях и системах
- Современные технологии построения безопасных информационных систем
- Этапы и технологию проектирования и создания безопасных информационных систем
- Современные программные и аппаратные средства защиты информации; -
- Основные угрозы информации в информационных системах и сетях
- Инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей.

уметь:

- Проектировать комплексную защищенную инфраструктуру для типовых современных применений, отвечающую предъявляемым требованиям к уровню защищенности
- Применять современные программные средства защиты информации
- Применять современные аппаратные средства защиты информационных процессов в компьютерных системах
- Применять программные библиотеки и пакеты для создания безопасных информационных систем.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	22
В том числе	
Лекции	
Практические занятия	
Лабораторные занятия	22
Самостоятельная работа	50
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Экзамены

Аннотация программы дисциплины:
«Интернет-протоколы и веб-технологии»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Интернет-протоколы и веб-технологии.

2. Место дисциплины в структуре ОП

Дисциплина **«Интернет-протоколы и веб-технологии»** относится к числу учебных дисциплин базовой части Б.1.1 блока Б.1 образовательной программы (Б.1.1.4).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Интернет-протоколы и веб-технологии» студенты должны:

знать:

- Основные принципы и технологии организации глобальной компьютерной сети Интернет
- Основы построения и функционирования прикладных сервисов Интернет
- Основные технологии прикладного программирования для сети Интернет
- Язык разметки гипертекста
- Механизм использования языка создания сценариев JavaScript для построения интерактивных Web-страниц
- Правила формирования и встраивания каскадных таблиц стилей CSS
- Механизм создания и встраивания анимации в Web-страницы
- Синтаксис языка серверных сценариев PHP
- Методику разработки динамических Web-страниц

уметь:

- Работать с языком разметки гипертекста для построения HTML-документов
- Использовать объектно-ориентированные технологии в построении интерактивных WEB-документов
- Встраивать правила каскадных таблиц стилей CSS
- Определять участок сети с максимальной задержкой передачи IP-пакетов;
- Формировать HTTP-запросы и анализировать поля HTTP-ответов;
- Разрабатывать гипертекстовые документы.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	
Практические занятия	
Лабораторные занятия	36
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Зачеты

Аннотация программы дисциплины:
«Инфокогнитивные технологии»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Инфокогнитивные технологии.

2. Место дисциплины в структуре ОП

Дисциплина «Инфокогнитивные технологии» относится к числу учебных дисциплин базовой части Б.1.1 блока Б.1 образовательной программы (Б.1.1.2).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Инфокогнитивные технологии» студенты должны:

знать:

- Историю развития инфокогнитивных технологий
- Современные области применения инфокогнитивных технологий

уметь:

- Использовать инфокогнитивные технологии

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	8
Практические занятия	
Лабораторные занятия	28
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Экзамены

Аннотация программы дисциплины:
**«Информационная безопасность в технологическом предпринимательстве,
углубленный курс»**

Направление подготовки

10.04.01 «Информационная безопасность»

Образовательная программа (профиль)

**«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)**

очная форма обучения

Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Информационная безопасность в технологическом предпринимательстве, углубленный курс.

2. Место дисциплины в структуре ОП

Дисциплина **«Информационная безопасность в технологическом предпринимательстве, углубленный курс»** относится к числу учебных дисциплин дисциплины по выбору студента Б.1.2 блока Б.1 образовательной программы (Б.1.ДВ.5).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Информационная безопасность в технологическом предпринимательстве, углубленный курс» студенты должны:

знать:

- Особенности и способы управления информационными потоками в производственных предприятиях
- Современные решения информационных и коммуникационных проблем производственных компаний с помощью специализированных программных продуктов
- Современные технологии связи и автоматизации управления процессами в производственных компаниях
- Особенности современных программных продуктов для автоматизации производственных компаний
- Базовые принципы внедрения и развертывания информационных систем, ориентированных на решение задач управления производственными компаниями
- Функциональные и архитектурные возможности информационных систем управления производственными компаниями

уметь:

- Решать задачи выбора необходимого программного обеспечения для автоматизации производственных компаний
- Ориентироваться на рынке современных программно-технологических решений для производственных компаний

- Применять полученные знания в практической работе с программами и информационными системами
- Правильно оценить достаточность и эффективность используемой на предприятии информационной системы
- Правильно сформулировать цели и критерии успешности внедрения информационной системы

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	22
В том числе	
Лекции	4
Практические занятия	
Лабораторные занятия	18
Самостоятельная работа	50
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Экзамены

Аннотация программы дисциплины:
«Информационная безопасность в технологическом предпринимательстве»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Информационная безопасность в технологическом предпринимательстве.

2. Место дисциплины в структуре ОП

Дисциплина **«Информационная безопасность в технологическом предпринимательстве»** относится к числу учебных дисциплин дисциплины по выбору студента Б.1.2 блока Б.1 образовательной программы (Б.1.ДВ.5).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Информационная безопасность в технологическом предпринимательстве» студенты должны:

знать:

- Особенности и способы управления информационными потоками в производственных предприятиях
- Современные решения информационных и коммуникационных проблем производственных компаний с помощью специализированных программных продуктов
- Современные технологии связи и автоматизации управления процессами в производственных компаниях
- Особенности современных программных продуктов для автоматизации производственных компаний
- Базовые принципы внедрения и развертывания информационных систем, ориентированных на решение задач управления производственными компаниями
- Функциональные и архитектурные возможности информационных систем управления производственными компаниями

уметь:

- Решать задачи выбора необходимого программного обеспечения для автоматизации производственных компаний
- Ориентироваться на рынке современных программно-технологических решений для производственных компаний

- Применять полученные знания в практической работе с программами и информационными системами
- Правильно оценить достаточность и эффективность используемой на предприятии информационной системы
- Правильно сформулировать цели и критерии успешности внедрения информационной системы

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	22
В том числе	
Лекции	4
Практические занятия	
Лабораторные занятия	18
Самостоятельная работа	50
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Экзамены

Аннотация программы дисциплины:
«Конечные автоматы и формальные грамматики»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Конечные автоматы и формальные грамматики.

2. Место дисциплины в структуре ОП

Дисциплина «**Конечные автоматы и формальные грамматики**» относится к числу учебных дисциплин вариативной части Б.1.2 блока Б.1 образовательной программы (Б.1.2.3).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «**Конечные автоматы и формальные грамматики**» студенты должны:

знать:

- Основные понятия теории регулярных языков, регулярных грамматик и конечных автоматов, взаимосвязь способов определения регулярных языков
- Основные понятия теории контекстно-свободных языков, грамматик и автоматов с магазинной памятью, взаимосвязь способов определения контекстно-свободных языков
- Теоретические основы построения алгоритмов синтаксического анализа контекстно-свободных языков

уметь:

- Строить конечный автомат по регулярной правосторонней грамматике и обратно
- Применять алгоритмы эквивалентных преобразований контекстно-свободных грамматик в нормальные формы
- Строить автомат с магазинной памятью по контекстно-свободной грамматике и обратно

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	
Практические занятия	36

Лабораторные занятия	
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Экзамены

Аннотация программы дисциплины:
«Криптография»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Криптография.

2. Место дисциплины в структуре ОП

Дисциплина «Криптография» относится к числу учебных дисциплин вариативной части Б.1.2 блока Б.1 образовательной программы (Б.1.2.4).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Криптография» студенты должны:

знать:

- Историю развития криптографических методов защиты информации
- Современные методы криптографической защиты информации
- Требования нормативных документов к средствам криптографической защиты информации

уметь:

- Использовать современные средства и методы криптографической защиты информации

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	22
В том числе	
Лекции	4
Практические занятия	
Лабораторные занятия	18
Самостоятельная работа	50
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Зачеты

Аннотация программы дисциплины:
«Методы коммуникации в области информационной безопасности, углубленный курс»

Направление подготовки

10.04.01 «Информационная безопасность»

Образовательная программа (профиль)

**«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)**

очная форма обучения

Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Методы коммуникации в области информационной безопасности, углубленный курс.

2. Место дисциплины в структуре ОП

Дисциплина **«Методы коммуникации в области информационной безопасности, углубленный курс»** относится к числу учебных дисциплин дисциплины по выбору студента Б.1.2 блока Б.1 образовательной программы (Б.1.ДВ.6).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Методы коммуникации в области информационной безопасности, углубленный курс» студенты должны:

знать:

- Современные методы научных исследований и информационно-коммуникационных технологий в области организации информационной безопасности социально-экономических информационных систем (СЭИС)

уметь:

- Проводить сравнительную оценку эффективности различных методов научных исследований и информационно-коммуникационных технологий в области организации информационной безопасности СЭИС

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	8
Практические занятия	
Лабораторные занятия	28
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Зачеты

Аннотация программы дисциплины:
«Методы коммуникации в области информационной безопасности»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Методы коммуникации в области информационной безопасности.

2. Место дисциплины в структуре ОП

Дисциплина «Методы коммуникации в области информационной безопасности» относится к числу учебных дисциплин дисциплины по выбору студента Б.1.2 блока Б.1 образовательной программы (Б.1.ДВ.6).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Методы коммуникации в области информационной безопасности» студенты должны:

знать:

- Современные методы научных исследований и информационно-коммуникационных технологий в области организации информационной безопасности социально-экономических информационных систем (СЭИС)

уметь:

- Проводить сравнительную оценку эффективности различных методов научных исследований и информационно-коммуникационных технологий в области организации информационной безопасности СЭИС

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	8
Практические занятия	
Лабораторные занятия	28
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Зачеты

Аннотация программы дисциплины:
«Методы статистического оценивания распределенных данных»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Методы статистического оценивания распределенных данных.

2. Место дисциплины в структуре ОП

Дисциплина «Методы статистического оценивания распределенных данных» относится к числу учебных дисциплин вариативной части Б.1.2 блока Б.1 образовательной программы (Б.1.2.2).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Методы статистического оценивания распределенных данных» студенты должны:

знать:

- Методы получения "хороших оценок"
- Статистические методы проверки параметрических и непараметрических гипотез
- Методы регрессионного и дискриминантного анализа
- Методы идентифицирования модели, оценки качества и параметров модели

уметь:

- Проводить точечное и интервальное оценивание экспериментальных данных
- Проанализировать исходные данные, выдвигать и проверять гипотезы (параметрические и непараметрические)

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	8
Практические занятия	
Лабораторные занятия	28
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Экзамены

Аннотация программы дисциплины:
«Модели безопасности в ВТ»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Модели безопасности в ВТ.

2. Место дисциплины в структуре ОП

Дисциплина «Модели безопасности в ВТ» относится к числу учебных дисциплин дисциплины по выбору студента Б.1.2 блока Б.1 образовательной программы (Б.1.ДВ.2).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Модели безопасности в ВТ» студенты должны:

знать:

- Виды, источники и носители защищаемой информации
- Источники опасных сигналов
- Структуру, классификацию и основные характеристики технических каналов утечки информации
- Классификацию технических разведок и противодействия им
- Методы и средства технической защиты информации
- Методы скрытия информации
- Программно-аппаратные средства защиты информации
- Структуру подсистемы безопасности операционных систем и выполняемые ею функции
- Средства защиты в вычислительных сетях
- Средства обеспечения защиты информации в системах управления базами данных
- Критерии защищенности компьютерных систем
- Методики проверки защищенности объектов информатизации на соответствие
- Требованиям нормативных документов.

уметь:

- Работать с техническими средствами защиты информации
- Работать с защищенными автоматизированными системами
- Передавать информацию по защищенным каналам связи
- Фиксировать отказы в работе средств вычислительной техники

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	8
Практические занятия	
Лабораторные занятия	28
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Экзамены

Аннотация программы дисциплины:
«Моделирование угроз и анализ рисков информационной безопасности»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Моделирование угроз и анализ рисков информационной безопасности.

2. Место дисциплины в структуре ОП

Дисциплина «Моделирование угроз и анализ рисков информационной безопасности» относится к числу учебных дисциплин вариативной части Б.1.2 блока Б.1 образовательной программы (Б.1.2.12).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Моделирование угроз и анализ рисков информационной безопасности» студенты должны:

знать:

- Основные положения, понятия и категории, теоретические основы моделирования угроз и прогнозирования рисков информационной безопасности
- Предпосылки для управления информационными рисками
- Основные требования по управлению рисками информационной безопасности
- Состав системы управления информационными рисками
- Порядок оценки рисков информационной безопасности
- Порядок обработки рисков информационной безопасности

уметь:

- Использовать стандарты в области управления рисками информационной безопасности
- Осуществлять оценку рисков информационной безопасности
- Осуществлять обработку результатов оценки рисков информационной безопасности
- Применять программное обеспечение для оценки рисков информационной безопасности

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	108 (3 з.е.)
Аудиторные занятия (всего)	72
В том числе	

Лекции	
Практические занятия	
Лабораторные занятия	72
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Экзамены

Аннотация программы дисциплины:
«Надежность и отказоустойчивость ВТ в ИС»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Надежность и отказоустойчивость ВТ в ИС.

2. Место дисциплины в структуре ОП

Дисциплина «Надежность и отказоустойчивость ВТ в ИС» относится к числу учебных дисциплин дисциплины по выбору студента Б.1.2 блока Б.1 образовательной программы (Б.1.ДВ.2).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Надежность и отказоустойчивость ВТ в ИС» студенты должны:

знать:

- Способы оценки и расчет надежности отказоустойчивости ВТ и ИС
- Основные методы диагностирования ВТ

уметь:

- Применять методы расчета надежности ВТ в ИС

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	8
Практические занятия	
Лабораторные занятия	28
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Экзамены

Аннотация программы дисциплины:
«Нейрокриптография»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Нейрокриптография.

2. Место дисциплины в структуре ОП

Дисциплина «Нейрокриптография» относится к числу учебных дисциплин дисциплины по выбору студента Б.1.2 блока Б.1 образовательной программы (Б.1.ДВ.7).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Нейрокриптография» студенты должны:

знать:

- историю развития нейрокриптографических методов защиты информации
- Знание современных методов нейрокриптографической защиты информации
- Знание требований нормативных документов к средствам нейрокриптографической защиты информации

уметь:

- Использовать современные средства и методы нейрокриптографической защиты информации

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	22
В том числе	
Лекции	4
Практические занятия	
Лабораторные занятия	18
Самостоятельная работа	50
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Зачеты

Аннотация программы дисциплины:
«Организационно-правовая защита персональных данных»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Организационно-правовая защита персональных данных.

2. Место дисциплины в структуре ОП

Дисциплина «Организационно-правовая защита персональных данных» относится к числу учебных дисциплин дисциплины по выбору студента Б.1.2 блока Б.1 образовательной программы (Б.1.ДВ.1).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Организационно-правовая защита персональных данных» студенты должны:

знать:

- Определение и категории персональных данных
- Права субъектов и операторов персональных данных
- Типовые модели угроз безопасности персональных данных
- Принципы и условия обработки и хранения персональных данных
- Организационные и технические меры безопасности при хранении персональных данных на носителях
- Мероприятия по защите персональных данных при их обработке в информационных системах
- Структуру государственной системы контроля и надзора за обеспечением безопасности персональных данных
- Основные руководящие, методические и нормативные документы в области безопасности персональных данных.

уметь:

- Классифицировать информационные системы безопасности персональных данных
- Формировать перечень актуальных угроз безопасности персональных данных оптимизировать систему защиты персональных данных.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	8
Практические занятия	
Лабораторные занятия	28
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Зачеты

Аннотация программы дисциплины:
«Персональные и открытые данные»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Персональные и открытые данные.

2. Место дисциплины в структуре ОП

Дисциплина «Персональные и открытые данные» относится к числу учебных дисциплин дисциплины по выбору студента Б.1.2 блока Б.1 образовательной программы (Б.1.ДВ.1).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Персональные и открытые данные» студенты должны:

знать:

- Что представляют из себя персональные и открытые данные
- Основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области
- Технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации

уметь:

- Анализировать и оценивать угрозы информационной безопасности объекта
- Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем
- Пользоваться нормативными документами по защите информации

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	8
Практические занятия	
Лабораторные занятия	28

Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Зачеты

Аннотация программы дисциплины:
«Практическая защита персональных данных»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Практическая защита персональных данных.

2. Место дисциплины в структуре ОП

Дисциплина «Практическая защита персональных данных» относится к числу учебных дисциплин вариативной части Б.1.2 блока Б.1 образовательной программы (Б.1.2.6).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Практическая защита персональных данных» студенты должны:

знать:

- Основные особенности современного состояния организационно-правового обеспечения защиты персональных данных в информационных системах персональных данных;
- Проблемы охраны конфиденциальности персональных данных лиц в Российской Федерации;
- Подходы к правовой защите персональных данных, организации контроля за возможными каналами их утечки;
- Методы и способы выявления угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- Порядок организации работ по обеспечению безопасности информации в информационных системах персональных данных;
- Требования и рекомендации по обеспечению безопасности информации в информационных системах персональных данных;
- Основные технические, программные, криптографические, программно-аппаратные средства, применяемые для защиты персональных данных;
- Методы контроля и оценки состояния обеспечения безопасности информации в информационных системах персональных данных;
- Об угрозах безопасности персональных данных и их источниках
- О способах и средствах технической защиты информации ограниченного доступа

уметь:

- Составлять перечень сведений, отнесенных к персональным данным и проводить их классификацию

- Проводить классификацию информационных систем персональных данных с составлением соответствующего акта
- Выявлять актуальные угрозы безопасности информации в информационных системах персональных данных
- Разрабатывать частные модели угроз безопасности персональных данных в конкретных информационных системах персональных данных с учетом их назначения, условий и особенностей функционирования;
- Разрабатывать техническое обоснование для создания системы защиты информационных систем персональных данных
- Оформлять техническое (частное техническое) задание на разработку системы (подсистемы) защиты персональных данных
- Разрабатывать необходимую организационно-распорядительную и нормативно-техническую документацию в интересах организации защиты персональных данных
- Планировать, организовывать и контролировать выполнение работ и мероприятий по защите персональных данных
- Оценивать эффективность защиты информационных систем персональных данных

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	22
В том числе	
Лекции	
Практические занятия	
Лабораторные занятия	22
Самостоятельная работа	50
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Экзамены

Аннотация программы дисциплины:
«Преддипломная практика»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Преддипломная практика.

2. Место дисциплины в структуре ОП

Дисциплина «Преддипломная практика» относится к числу учебных дисциплин практики, в том числе научно-исследовательская работа (НИР) Б.2.2 блока Б.2 образовательной программы (Б.2.2).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Преддипломная практика» студенты должны:

знать:

- Задачи и цели преддипломной практики
- Место и сроки проведения преддипломной практики
- Представление о конечном результате

уметь:

- Вовремя реализовывать поставленные задачи и цели в течение преддипломной практики

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	(6 з.е.)
Аудиторные занятия (всего)	
В том числе	
Лекции	
Практические занятия	
Лабораторные занятия	
Самостоятельная работа	
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	

Аннотация программы дисциплины:
«Производственная практика, в том числе научно-исследовательская работа (НИР)»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Производственная практика, в том числе научно-исследовательская работа (НИР).

2. Место дисциплины в структуре ОП

Дисциплина ««Производственная практика, в том числе научно-исследовательская работа (НИР)»» относится к числу учебных дисциплин практики, в том числе научно-исследовательская работа (НИР) Б.2.1 блока Б.2 образовательной программы (Б.2.1).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Производственная практика, в том числе научно-исследовательская работа (НИР)» студенты должны:

знать:

- Задачи и цели производственной практики
- Место и сроки проведения производственной практики
- Представление о конечном результате

уметь:

- Вовремя реализовывать поставленные задачи и цели в течение производственной практики

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	(48 з.е.)
Аудиторные занятия (всего)	
В том числе	
Лекции	
Практические занятия	
Лабораторные занятия	
Самостоятельная работа	
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	

Аннотация программы дисциплины:
«Разработка веб-приложений»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Разработка веб-приложений.

2. Место дисциплины в структуре ОП

Дисциплина «Разработка веб-приложений» относится к числу учебных дисциплин вариативной части Б.1.2 блока Б.1 образовательной программы (Б.1.2.1).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Разработка веб-приложений» студенты должны:

знать:

- этапы решения задачи на компьютере
- типы данных
- базовые конструкции изучаемых языков программирования
- принципы структурного и модульного программирования
- принципы объектно – ориентированного программирования

уметь:

- работать в среде программирования
- реализовывать построенные алгоритмы в виде программ на конкретном языке программирования
- создавать Web-страницы и узлы.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	
Практические занятия	
Лабораторные занятия	36
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Экзамены

Аннотация программы дисциплины:
«Распределенные и облачные системы»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Распределенные и облачные системы.

2. Место дисциплины в структуре ОП

Дисциплина «Распределенные и облачные системы» относится к числу учебных дисциплин вариативной части Б.1.2 блока Б.1 образовательной программы (Б.1.2.8).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Распределенные и облачные системы» студенты должны:

знать:

- Основные понятия, методы, алгоритмы и средства распределенных вычислений, виды облачных вычислений, платформы облачных вычислений, основные преимущества и риски, связанные с облачными вычислениями
- Виды технологических процессов обработки информации в распределенных системах, особенности их применения

уметь:

- Осуществлять разработку типовых технологических процессов автоматизированной обработки информации
- Использовать технологии построения и эксплуатации распределенных информационных систем
- Выявлять автоматизированные и бизнес-процессы, которые эффективнее перенести в «облака», оценивать возможные риски использования облачных технологий, выбирать оптимальную стратегию перехода на облачные технологии

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	108 (3 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	
Практические занятия	
Лабораторные занятия	36
Самостоятельная работа	72
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Экзамены

Аннотация программы дисциплины:
«Случайные процессы»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Случайные процессы.

2. Место дисциплины в структуре ОП

Дисциплина «Случайные процессы» относится к числу учебных дисциплин базовой части Б.1.1 блока Б.1 образовательной программы (Б.1.1.5).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Случайные процессы» студенты должны:

знать:

- Важнейшие понятия и термины теории случайных процессов, их виды и методы исследования

уметь:

- Правильно классифицировать случайные процессы, пользоваться основными методами их анализа, применять полученные знания к практическим задачам.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	8
Практические занятия	
Лабораторные занятия	28
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Экзамены

Аннотация программы дисциплины:
«Современные угрозы в интернет, облачной и распределенной сфере»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Современные угрозы в интернет, облачной и распределенной сфере.

2. Место дисциплины в структуре ОП

Дисциплина «Современные угрозы в интернет, облачной и распределенной сфере» относится к числу учебных дисциплин вариативной части Б.1.2 блока Б.1 образовательной программы (Б.1.2.11).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Современные угрозы в интернет, облачной и распределенной сфере» студенты должны:

знать:

- Основные проблемы безопасности облачной инфраструктуры
- Источники современных угроз в интернет, облачной и распределенной сфере
- Общие принципы построения защищенных систем.
- Иерархический метод разработки защищенных систем.

уметь:

- Обеспечить безопасность на административном и процедурном уровнях
- Разработать инструментарий для построения распределенной вычислительной системы на основе персональных компьютеров, подключенных к сети Интернет

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	144 (4 з.е.)
Аудиторные занятия (всего)	72
В том числе	
Лекции	
Практические занятия	
Лабораторные занятия	72
Самостоятельная работа	72
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Экзамены

Аннотация программы дисциплины:
«Социально-психологические аспекты веб-безопасности»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Социально-психологические аспекты веб-безопасности.

2. Место дисциплины в структуре ОП

Дисциплина «Социально-психологические аспекты веб-безопасности» относится к числу учебных дисциплин дисциплины по выбору студента Б.1.2 блока Б.1 образовательной программы (Б.1.ДВ.3).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Социально-психологические аспекты веб-безопасности» студенты должны:

знать:

- Влияние человеческого фактора на информационную безопасность
- Принципы анализа информационной культуры
- Правовые аспекты информатизации
- Законодательные акты РФ в области информатизации, информационной безопасности
- Правовые проблемы в области информатизации
- Принципы соблюдения компьютерной этики

уметь:

- Использовать уровни рассмотрения информационной культуры с целью ее анализа и оценки
- Учитывать требования законодательства в области информационной политики и информационной безопасности в повседневной жизни и профессиональной деятельности

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	8
Практические занятия	
Лабораторные занятия	28
Самостоятельная работа	36
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Зачеты

Аннотация программы дисциплины:
«Стеганография»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Стеганография.

2. Место дисциплины в структуре ОП

Дисциплина «Стеганография» относится к числу учебных дисциплин дисциплины по выбору студента Б.1.2 блока Б.1 образовательной программы (Б.1.ДВ.7).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Стеганография» студенты должны:

знать:

- Основные алгоритмы защиты информации
- Методы применяемые для анализа надежности стеганосистемы
- Принципы построения моделей стеганосистем
- Методику сокрытия информации при передаче её по открытому каналу
- Методы и средства обнаружения скрытой информации.
- Терминологию принятую в области защиты информации и стеганографии

уметь:

- Реализовывать основные типы стеганосистем
- Осуществлять управление стеганосистемой
- Обеспечивать высокую надежность стеганосистеме и ее каналам передачи информации
- Распознавать модифицированные стеганосистемы
- Реализовать представленные методы и алгоритмы на любом языке программирования
- Использовать существующий инструментарий для обнаружения скрытой информации

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	22
В том числе	
Лекции	4
Практические занятия	

Лабораторные занятия	18
Самостоятельная работа	50
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Зачеты

Аннотация программы дисциплины:
«Технологии обеспечения информационной безопасности»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Технологии обеспечения информационной безопасности.

2. Место дисциплины в структуре ОП

Дисциплина «Технологии обеспечения информационной безопасности» относится к числу учебных дисциплин базовой части Б.1.1 блока Б.1 образовательной программы (Б.1.1.8).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Технологии обеспечения информационной безопасности» студенты должны:

знать:

- Основные положения, понятия и категории, относящиеся к базовым и расширенным технологиям обеспечения информационной безопасности
- Отечественные и международные стандарты и спецификаций информационной безопасности, их классификация и выявление взаимосвязей
- Множество требований, предъявляемых к процессам защиты информации в современных информационных системах
- Модели и методы анализа рисков и выделения опасных факторов ИБ, применяемые в международных стандартах
- Множество типовых подходов и методов противодействия наиболее распространенным угрозам информационной безопасности
- Множество принципов организации, комплексного подхода к выбору средств и технологий обеспечения информационной безопасности объектов защиты

уметь:

- Осуществлять успешную классификацию угроз и объектов защиты
- Применять концептуальные основы технической защиты информации
- Обеспечивать выполнение требований и рекомендации по защите информации, обрабатываемой средствами вычислительной техники
- Осуществлять создание средств безопасности, отвечающих требованиям к архитектуре, указанным в соответствующих стандартах

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	144 (4 з.е.)
Аудиторные занятия (всего)	72
В том числе	
Лекции	
Практические занятия	
Лабораторные занятия	72
Самостоятельная работа	72
Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Экзамены

Аннотация программы дисциплины:
«Управление информационной безопасностью»
Направление подготовки
10.04.01 «Информационная безопасность»
Образовательная программа (профиль)
«Информационная безопасность в веб-разработке и облачных технологиях»
(магистратура)
очная форма обучения
Год приема – 2017/2018

1. Цели и задачи дисциплины

Целью является усвоение понятий и методов дисциплины Управление информационной безопасностью.

2. Место дисциплины в структуре ОП

Дисциплина «Управление информационной безопасностью» относится к числу учебных дисциплин базовой части Б.1.1 блока Б.1 образовательной программы (Б.1.1.7).

Дисциплина взаимосвязана логически и содержательно-методически со дисциплинами и практиками направления «Информационная безопасность».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Управление информационной безопасностью» студенты должны:

знать:

- Современные подходы к управлению ИБ и направлениях их развития
- Основные стандарты, регламентирующие управление ИБ
- Принципы построения СУИБ
- Принципы разработки процессов управления ИБ
- Взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ

уметь:

- Анализировать текущее состояние ИБ с целью разработки требований к разрабатываемым процессам управления ИБ
- Определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ применять процессный подход к управлению ИБ в различных сферах деятельности
- Практически решать задачи формализации разрабатываемых процессов управления ИБ разрабатывать и внедрять СУИБ и оценивать ее эффективность.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Общая трудоемкость	72 (2 з.е.)
Аудиторные занятия (всего)	36
В том числе	
Лекции	
Практические занятия	
Лабораторные занятия	36
Самостоятельная работа	36

Курсовая работа	
Курсовой проект	
Вид промежуточной аттестации	Экзамены