МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
Проф. Таюрский Д.А.
_____ "__" _____ 20___ г.

подписано электронно-цифровой подписью

Программа дисциплины

Организационное и правовое обеспечение информационной безопасности Б3.Б.5

Направление подготовки: 090900.62 - Информационная безопасность
Профиль подготовки: Математические и программные средства защиты информации
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):
Ишмухаметов Ш.Т.

Рецензент(ы):
Латыпов Р.Х.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Латыпов Р. Х.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 937216

Казань
2016

Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре основной образовательной программы
3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля
4. Структура и содержание дисциплины/ модуля
5. Образовательные технологии, включая интерактивные формы обучения
6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов
7. Литература
8. Интернет-ресурсы
9. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

Программу дисциплины разработал(а)(и) профессор, д.н. (доцент) Ишмухаметов Ш.Т. кафедра системного анализа и информационных технологий отделение фундаментальной информатики и информационных технологий , Shamil.Ishmukhametov@kpfu.ru

1. Цели освоения дисциплины

Цель курса - дать основы правового регулирования отношений в информационной сфере, конституционные гарантии прав граждан на получение информации

и механизм их реализации, понятия и виды защищаемой информации по законодательству РФ, систему защиты государственной тайны, основы правового

регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности, а также понятие и виды компьютерных преступлений.

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " Б3.Б.5 Профессиональный" основной образовательной программы 090900.62 Информационная безопасность и относится к базовой (общепрофессиональной) части. Осваивается на 2 курсе, 4 семестр.

Дисциплина входит в базовую часть профессионального цикла дисциплин и изучается студентами на 2 курсе в 4 семестре. Базируется на курсе

"Основы информационной безопасности", который дает понятие о целях, объектах и методах защиты компьютерной информации.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-1 (общекультурные компетенции)	способность осознавать необходимость соблюдения Конституции РФ, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма
ОК-2 (общекультурные компетенции)	способность осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм
ОК-6 (общекультурные компетенции)	способность находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность
ПК-24 (профессиональные компетенции)	способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности
ПК-25 (профессиональные компетенции)	способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью
ПК-27 (профессиональные компетенции)	способность принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных криптографических и технических средств защиты информации
ПК-28 (профессиональные компетенции)	способность изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-29 (профессиональные компетенции)	способность участвовать в работах по реализации политики информационной безопасности
ПК-5 (профессиональные компетенции)	способность организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации
ПК-6 (профессиональные компетенции)	способность организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов
ПК-7 (профессиональные компетенции)	способность использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий
ПК-8 (профессиональные компетенции)	способность определить виды и формы информации, подтвержденной угрозами, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятий

В результате освоения дисциплины студент:

1. должен знать:

Основные сведения по правовому обеспечению информационной безопасности;

- правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности;

- понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации;

- основы правового регулирования взаимоотношений администрации и персонала в области защиты информации;

- правила лицензирования и сертификации в области защиты информации;

- виды и признаки компьютерных преступлений.

2. должен уметь:

Ориентироваться в организационно-правовых аспектах информационной безопасности;

Применять необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с

помощью систем правовой информации;

- применять действующую законодательную базу в области информационной безопасности;

- разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других

организационно-распорядительных документов.

3. должен владеть:

- теоретическими знаниями о организации построения безопасных информационных систем;

- профессиональной терминологией и знаниями законов, обеспечивающих информационную безопасность

-навыками работы с нормативно-правовыми актами.

применять полученные знания в области организационно- правовогого обеспечения ИБ в своей профессиональной деятельности

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) 72 часа(ов).

Форма промежуточного контроля дисциплины зачет в 4 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Законодательный уровень защиты информации.	4		6	6	0	домашнее задание
2.	Тема 2. Основные положения Конституции РФ и Федерального Закона "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года.	4		4	4	0	домашнее задание
3.	Тема 3. Основные положения ФЗ "Об электронной подписи" в редакции от 5 апреля 2013 г.	4		2	2	0	домашнее задание

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
4.	Тема 4. Основные положения ФЗ "О лицензировании отдельных видов деятельности" от 20.07.2001 и ФЗ "О персональных данных" от 27.07.2006.	4		2	2	0	домашнее задание
5.	Тема 5. Основные положения Уголовный кодекс РФ, Кодекс Российской Федерации об административных правонарушениях, Трудовой кодекс Российской Федерации, Гражданский кодекс Российской Федерации об ответсвенности в области информационной безопасности.	4		2	2	0	домашнее задание
6.	Тема 6. Изучение алгоритмов построени цифровой подписи.	4		2	2	0	контрольная работа
.	Тема . Итоговая форма контроля	4		0	0	0	зачет
	Итого			18	18	0	

4.2 Содержание дисциплины

Тема 1. Законодательный уровень защиты информации.

лекционное занятие (6 часа(ов)):

Значение и место законодательного уровеня защиты информации в системе комплексной защиты информации. Основные законы и акты в области информационной безопасности.

практическое занятие (6 часа(ов)):

Изучение основных положений Конституции РФ в области вопросов создания и распространения информации. Руководящие органы РФ в области информационной безопасности.

Тема 2. Основные положения Конституции РФ и Федерального Закона "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года.

лекционное занятие (4 часа(ов)):

Изучение основных положений и понятий Федерального Закона"Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года, определение понятий информации и документированной информации (документа), информационных процессов, информационной системы, информационных ресурсов.

практическое занятие (4 часа(ов)):

Изучение понятий информации и документированной информации (документа), информационных процессов, информационной системы, информационных ресурсов из ФЗ РФ "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года.

Тема 3. Основные положения ФЗ "Об электронной подписи" в редакции от 5 апреля 2013 г.

лекционное занятие (2 часа(ов)):

Изучение основных положений Федерального Закона ""Об электронной подписи" в редакции от 5 апреля 2013 г. Технические средства генерации цифровой подписи.

практическое занятие (2 часа(ов)):

Разбор алгоритма создания электронной подписи, понятий открытого и закрытого ключей. Юридическая сила электронной подписи (по ФЗ ""Об электронной подписи").

Тема 4. Основные положения ФЗ "О лицензировании отдельных видов деятельности" от 20.07.2001 и ФЗ "О персональных данных" от 27.07.2006.

лекционное занятие (2 часа(ов)):

Изучение основных положений ФЗ "О лицензировании отдельных видов деятельности" от 20.07.2001 и ФЗ "О персональных данных" от 27.07.2006

практическое занятие (2 часа(ов)):

Изучение порядка работы с персональными данными. Особенности распространения и обработки песональных данных в государственных органах.

Тема 5. Основные положения Уголовный кодекс РФ, Кодекс Российской Федерации об административных правонарушениях, Трудовой кодекс Российской Федерации, Гражданский кодекс Российской Федерации об ответсвенности в области информационной безопасности.

лекционное занятие (2 часа(ов)):

Изучение положений УК Российской Федерации и других законодательных актов в области ответственности за правонарушения в области информационной безопасности.

практическое занятие (2 часа(ов)):

Разбор Трудового и Гражданского Кодекса РФ в части, связанной с информационной безопасностью.

Тема 6. Изучение алгоритмов построени цифровой подписи.

лекционное занятие (2 часа(ов)):

Изучение схем цифровой подписи Эль-Гамаля, ГОСТ Р 34.10-2012 от 01.01.2013 г.

практическое занятие (2 часа(ов)):

Программная реализация схемы цифровой подписи Эль-Гамаля. Оценка сложности реализации подписи и ее криптостойкость.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Законодательный уровень защиты информации.	4		подготовка домашнего задания	8	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
2.	Тема 2. Основные положения Конституции РФ и Федерального Закона "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года.	4		подготовка домашнего задания	8	домашнее задание
3.	Тема 3. Основные положения ФЗ "Об электронной подписи" в редакции от 5 апреля 2013 г.	4		подготовка домашнего задания	8	домашнее задание
4.	Тема 4. Основные положения ФЗ "О лицензировании отдельных видов деятельности" от 20.07.2001 и ФЗ "О персональных данных" от 27.07.2006.	4		подготовка домашнего задания	8	домашнее задание
5.	Тема 5. Основные положения Уголовный кодекс РФ, Кодекс Российской Федерации об административных правонарушениях, Трудовой кодекс Российской Федерации, Гражданский кодекс Российской Федерации об ответсвенности в области информационной безопасности.	4		подготовка домашнего задания	2	домашнее задание
6.	Тема 6. Изучение алгоритмов построени цифровой подписи.	4		подготовка к контрольной работе	2	контрольная работа
	Итого				36	

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лекционных и практических занятий, а также самостоятельной работы студентов.

Теоретический материал излагается на лекциях. Причем конспект лекций, который остается у студента в результате прослушивания лекции не может заменить учебник. Его цель - формулировка основных утверждений и определений. Прослушав лекцию, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи зачета минимум и дополнительная литература.

Изучение курса подразумевает не только овладение теоретическим материалом, но и получение практических навыков для более глубокого понимания разделов дисциплины "Основы информационной безопасности" на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать частные утверждения.

Самостоятельная работа предполагает выполнение домашних работ. Практические задания, выполненные в аудитории, предназначены для указания общих методов решения задач определенного типа. Закрепить навыки можно лишь в результате самостоятельной работы.

Кроме того, самостоятельная работа включает подготовку к зачету. При подготовке к сдаче зачета весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки к зачету, контролировать каждый день выполнения работы. Лучше, если можно перевыполнить план. Тогда всегда будет резерв времени.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Законодательный уровень защиты информации.

домашнее задание , примерные вопросы:

Обсуждение российского законодательства в области защиты информации. Дать расширенную характеристику понятий государственная, коммеческая, личная тайна, персональные данные.

Тема 2. Основные положения Конституции РФ и Федерального Закона "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года.

домашнее задание , примерные вопросы:

Обсуждение ФЗ "Об информации, информационных технологиях и о защите информации" . Разобрать и дать развернутую характеристику понятий: 1. информационная технология 2. информаионная система 3. документированная информация. 4. конфиденциальная информация.

Тема 3. Основные положения ФЗ "Об электронной подписи" в редакции от 5 апреля 2013 г.

домашнее задание , примерные вопросы:

Разобрать и дать развернутую характеристику понятий: 1. Электронная подпись 2. Открытый ключ ЭП 3. Порядок построения ЭП 4. Сертификат открытого ключа.

Тема 4. Основные положения ФЗ "О лицензировании отдельных видов деятельности" от 20.07.2001 и ФЗ "О персональных данных" от 27.07.2006.

домашнее задание , примерные вопросы:

Дать характеристику понятия персональных данных, описать сведения, отнесенные к персональным данным, порядок обработки ПД в автоматизированных системах.

Тема 5. Основные положения Уголовный кодекс РФ, Кодекс Российской Федерации об административных правонарушениях, Трудовой кодекс Российской Федерации, Гражданский кодекс Российской Федерации об ответсвенности в области информационной безопасности.

домашнее задание , примерные вопросы:

Разобрать положения статей 272-274 УК РФ о правонарушениях в области информационной безопасности, описать виды правонарушений в области ИБ, ответственность за разработку и распространенние вредоносных программ, за блокирование каналов передачи информации.

Тема 6. Изучение алгоритмов построени цифровой подписи.

контрольная работа , примерные вопросы:

1. Раскрыть основные положения Конституции РФ в области информационной безопасности. 2. Раскрыть основные положения ст.272 УК РФ. 3. Раскрыть основные положения закона 2011 года "Об электронной подписи".

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

ВОПРОСЫ К ЗАЧЕТУ

1. Введение в защиту информации.
2. Роль информации в жизнедеятельности современного общества.
3. Влияние информации на современное общество и повышение в связи с этим интерес к ней.
4. Определение информационной безопасности.
5. Современная постановка задачи защиты информации.
6. Основные составляющие информационной безопасности: конфиденциальность, целостность и доступность информации.
7. Угрозы безопасности информационным системам и их классификация. Угрозы конфиденциальности, целостности и доступности информации.
8. Меры противодействия угрозам безопасности ИС.
9. Классификация средств и методов защиты: административные, технические, организационно-правовые, физические методы защиты, их подразделение на предупреждающие, выявляющие (обнаруживающие), корректирующие средства.
10. Методы идентификации и аутентификации пользователей, технических средств обработки, программ и баз данных.
11. Метод паролей.
12. Биометрическая аутентификация.
13. Способы разграничения доступа, методы и средства их реализации.
14. Краткая характеристика современных средств разграничения доступа. Дискреционный и мандатный методы доступа.
15. Классификация информационных систем по степени защищенности.
16. "Оранжевая книга" США как критерий классификации систем информационной безопасности.
17. "Общие критерии" стран Европейского сообщества, их основные по-ложения.
18. Парольная идентификация и аутентификация в сетевых операционных системах: многоразовые и одноразовые пароли, смарт-карты, аутентификация на основе сертификатов.
19. Законодательный уровень защиты информации.
20. Основные положения Конституции РФ о защите информации, правах граждан на получение и распространение информации, законы и законодательные акты Российской Федерации в области защиты информации.
21. Основные положения закона Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года, определение понятия информации и документированной информации (документа), информационных процессов, информационной системы, информационных ресурсов.
22. Закон "О лицензировании отдельных видов деятельности" от 8 августа 2001 г. определение понятий лицензии, лицензируемого вида деятельности, лицензирования, лицензирующие органов, лицензиата. Положение статьи 17 Закона о видах деятельности, на осуществление которых требуются лицензии.

23. Основные положения закона РФ "Об электронной цифровой подписи" (от 5 апреля 2013 года) об электронном документе и электронной цифровой подписи, сертификате ЭЦП, владельце ЭЦП, закрытом и открытом ключе ЭЦП.
24. Криптографические средства защиты информации.
25. Основные понятия и задачи криптологии (криптографии).
26. Краткий исторический экскурс развития.
27. Примеры шифров замены и перестановки. Методы их дешифрования.
28. Криптосистемы с секретным ключом (симметричные).
29. Криптографические примитивы: перестановки, подставки, гаммирование.
30. Блочные и потоковые криптосистемы.
31. Проблема распределения ключей.
32. Математические основы современной криптологии.
33. Криптосистемы с открытым ключом (ассиметричные).
34. Система RSA.
35. Хэш-функции. Их свойства.
36. Использование хэш-функций для защиты паролей, целостности и конфиденциальности информации.
37. Открытое распределение ключей.
38. Использование RSA для защиты конфиденциальности сообщений, целостности данных и определения авторства сообщения.
39. Математические основы построения эллиптических кривых.
40. Прямые и обратные операции в конечных полях.
41. Система шифрования Эль-Гамаля.
42. Реализации системы Эль - Гамаля на ЭК.
43. Алгоритм электронной подписи на ЭК

7.1. Основная литература:

1. Расторгуев, С. П. Основы информационной безопасности: учебное пособие / С.П. Расторгуев.?Москва: Академия, 2007.?186 с.

2. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с. URL: http://znanium.com/bookread.php?book=335362

3. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с. URL: http://znanium.com/bookread.php?book=402686

4. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. URL: http://znanium.com/bookread.php?book=405000

7.2. Дополнительная литература:

1. Партыка Т. Л. Информационная безопасность: Учебное пособие для студентов учреждений среднего проф. обр. / Т.Л. Партыка, И.И. Попов. - 3-е изд., перераб. и доп. - М.: Форум, 2014. - 432 с. - ЭБС "Знаниум": http://znanium.com/bookread.php?book=420047

2. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с. - ЭБС "Знаниум": http://znanium.com/bookread.php?book=491597

3. Хорев П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. - 352 с. - ЭБС "Знаниум": http://znanium.com/bookread.php?book=169345

7.3. Интернет-ресурсы:

Википедия - http://ru.wikipedia.org

Законы РФ в области защиты информации - http://www.security.ru/legislation.php

Интернет-портал образовательных ресурсов по ИТ - http://www.intuit.ru

Сайт Консультант Плюс - http://consultant.ru

Сайт системы Гарант - http://garant.ru

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Организационное и правовое обеспечение информационной безопасности" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение.

Лекции по дисциплине проводятся в аудитории, оснащенной доской и мелом(маркером).

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 090900.62 "Информационная безопасность" и профилю подготовки Математические и программные средства защиты информации .

Автор(ы):
Ишмухаметов Ш.Т. _____
"__" _____ 201 __ г.

Рецензент(ы):
Латыпов Р.Х. _____
"__" _____ 201 __ г.