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

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
Проф. Д.А. Таюрский
ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ (ДО КФУ)
«___»_____20__г.

подписано электронно-цифровой подписью

Программа дисциплины

Основы управления информационной безопасностью Б1.Б.13

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность компьютерных систем
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 947018

Казань
2018

Содержание

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 - сформировать систему знаний о принципах, методах, подходах и инструментах эффективного управления информационной безопасностью

в современной организации. В рамках данного курса рассматриваются основные принципы и правила управления обеспечением информационной безопасности

на предприятиях и организациях, которые позволят повысить эффективность функционирования предприятия

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

Данная учебная дисциплина включена в раздел " Б1.Б.13 Дисциплины (модули)" основной образовательной программы 10.03.01 Информационная безопасность и относится к базовой (общепрофессиональной) части. Осваивается на 4 курсе, 8 семестр.

Дисциплина входит в группу базовых дисциплин профессионального цикла по направлению "Информационная безопасность".

Изучается в 8 семестре на 4 курсе обучения бакалавров. Основывается на курсах "Основы информационной безопасности",

"Организационное и правовое обеспечение информационной безопасности", "Техническая защита информации", "Комплексное обеспечение

информационной безопасности" и других профессиональных дисциплин.

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-4 (общекультурные компетенции)	способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики
ПК-13 (профессиональные компетенции)	способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов
ПК-14 (профессиональные компетенции)	способностью принимать участие в проведении экспериментальных исследований системы защиты информации
ПК-18 (профессиональные компетенции)	способностью организовать работу малого коллектива исполнителей в профессиональной деятельности
ПК-2 (профессиональные компетенции)	способностью принимать участие в эксплуатации подсистем управления информационной безопасностью объекта защиты

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-6 (профессиональные компетенции)	способностью принимать участие в организации и сопровождении аттестации объекта информатизации на предмет соответствия требованиям защиты информации
ПК-7 (профессиональные компетенции)	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
ПК-8 (профессиональные компетенции)	способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
ПК-9 (профессиональные компетенции)	способностью участвовать в разработке подсистемы управления информационной безопасностью

В результате освоения дисциплины студент:

1. должен знать:

Знать структуру нормативных актов и стандартов в области управления информационной безопасностью, а также соответствующую систему терминов и понятий;

2. должен уметь:

уметь управлять основными процессами реализации системы информационной безопасности: планирования, идентификации и анализа рисков,
выработки и реализации комплекса контрмер, а также мониторинга и актуализации реестра рисков.

3. должен владеть:

пониманием структуры и системы взаимосвязи процессов управления информационной безопасностью, а также место системы
информационной безопасности в общей системе корпоративной безопасности и системе управления рисками компании;

4. должен демонстрировать способность и готовность:

применять полученные знания и навыки в своей дальнейшей профессиональной деятельности

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) 108 часа(ов).

Форма промежуточного контроля дисциплины зачет в 8 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. Принципы и приемы корпоративной информационной безопасности	8		4	4	0	Письменное домашнее задание
2.	Тема 2. Правовые методы защиты информации	8		2	2	0	Письменное домашнее задание Контрольная работа
3.	Тема 3. Порядок построения системы информационной безопасности на предприятии	8		4	4	0	Письменное домашнее задание
4.	Тема 4. Международные и российские стандарты в области информационной безопасности.	8		4	4	0	Письменное домашнее задание
5.	Тема 5. Основные подходы к управлению доступом к ресурсам ИС.	8		6	6	0	Контрольная работа Письменное домашнее задание
.	Тема . Итоговая форма контроля	8		0	0	0	Зачет
	Итого			20	20	0	

4.2 Содержание дисциплины

Тема 1. Принципы и приемы корпоративной информационной безопасности

лекционное занятие (4 часа(ов)):

Принципы построения корпоративной подсистемы информационной безопасности. Управление рисками нарушения информационной безопасности. Определение целей и задач управления.

практическое занятие (4 часа(ов)):

Изучение основных понятий и терминов системы управления: -доступ к информации и его виды; классификация угроз информации; субъекты информационной безопасности и их обязанности: распределение обязанностей по обеспечению информационной безопасности в рамках предприятия; согласование правил безопасности между логическими структурами предприятия; право на информацию; классификация нарушителей. Задачи информационной безопасности.

Тема 2. Правовые методы защиты информации

лекционное занятие (2 часа(ов)):

Охраняемая информация. Охрана персональных данных, охрана коммерческой тайны и секретов производства, охрана конфиденциальной информации, документообеспечение системы безопасности

практическое занятие (2 часа(ов)):

Концепция безопасности Российской Федерации. Регулирующие органы и их функции. Решение задач информационной безопасности.

Тема 3. Порядок построения системы информационной безопасности на предприятии

лекционное занятие (4 часа(ов)):

Защита носителей информации, каналов связи, акустической информации. Построение комплексной системы защиты данных. Правовые (законодательные), организационные (административные и процедурные), физические и технические (аппаратурные и программные) методы защиты.

практическое занятие (4 часа(ов)):

Изучение процедур инвентаризации, определение и оценка рисков, управление рисками. Рассмотрение примеров.

Тема 4. Международные и российские стандарты в области информационной безопасности.

лекционное занятие (4 часа(ов)):

Изучение оценочного стандарта "Common Criteria" (отечественный аналог - ГОСТ Р ИСО/МЭК 15408-2002 и британского стандарта "BS 7799" (отечественный аналог - ГОСТ Р ИСО/МЭК 17799).

практическое занятие (4 часа(ов)):

Изучение понятий жизненного цикла информационной системы, цели правил безопасности, архитектур защиты, содержания понятий физической защиты, аутентификации, шифрования, управление персоналом.

Тема 5. Основные подходы к управлению доступом к ресурсам ИС.

лекционное занятие (6 часа(ов)):

Мандатный и дискреционный подходы к управлению доступом. Требования к мандатному и дискреционному подходу. Управление персоналом. Задачи, решаемые при приеме и увольнении сотрудников.

практическое занятие (6 часа(ов)):

Контрольная работе по теме занятия.

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. Принципы и приемы корпоративной информационной безопасности	8		подготовка домашнего задания	11	Письменное домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
2.	Тема 2. Правовые методы защиты информации	8		подготовка домашнего задания	11	Письменное домашнее задание
				подготовка к контрольной работе	4	Контрольная работа
3.	Тема 3. Порядок построения системы информационной безопасности на предприятии	8		подготовка домашнего задания	10	Письменное домашнее задание
4.	Тема 4. Международные и российские стандарты в области информационной безопасности.	8		подготовка домашнего задания	10	Письменное домашнее задание
5.	Тема 5. Основные подходы к управлению доступом к ресурсам ИС.	8		подготовка домашнего задания	10	Письменное домашнее задание
				подготовка к контрольной работе	12	Контрольная работа
	Итого				68	

5. Образовательные технологии, включая интерактивные формы обучения

Занятия проводятся в форме лекционных и практических занятий.

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

Тема 1. Принципы и приемы корпоративной информационной безопасности

Письменное домашнее задание , примерные вопросы:

Изучить меры организационного и программно-технического уровня, направленных на защиту информационных ресурсов предприятия от угроз информационной безопасности.

Тема 2. Правовые методы защиты информации

Контрольная работа , примерные вопросы:

Вариант контрольной работы 1. 1. Перечислить и раскрыть основные свойства подписи. 2. Дать определение основных понятий, связанных с ЭП на основе ФЗ РФ "Об электронной подписи" 2011 года. 3. Описать состав сертификата открытого ключа.

Письменное домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме. Изучить основные положения ФЗ РФ "Об электронной подписи" 2011 и сделать анализ основных понятий, содержащихся в законе.

Тема 3. Порядок построения системы информационной безопасности на предприятии

Письменное домашнее задание , примерные вопросы:

Изучить систему требований к информационным ресурсам: принципы доступности информации (возможность за приемлемое время получить требуемую информационную услугу), ее целостности (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения), конфиденциальности (защита от несанкционированного ознакомления), неотказуемость (невозможность отрицания совершенных действий), аутентичность (подтверждение подлинности и достоверности электронных документов).

Тема 4. Международные и российские стандарты в области информационной безопасности.

Письменное домашнее задание , примерные вопросы:

Изучить основные положения стандартов РФ: ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения", ГОСТ Р 51275-2006 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения"

Тема 5. Основные подходы к управлению доступом к ресурсам ИС.

Контрольная работа , примерные вопросы:

Вариант контрольной работы 2. 1. Раскрыть содержимое понятий аутентификации, авторизации и аудита, дать примеры. 2. Роль Технической Комиссии при сертификации аппаратных средств ЗИ. 3. Функции ФСБ при лицензировании и сертификации программных криптографических продуктов.

Письменное домашнее задание , примерные вопросы:

Изучить мандатный и дискреционный подходы к управлению лоступом на примере MS SQL Server 2012.

Итоговая форма контроля

зачет

Примерные вопросы к зачету:

1. Основные понятия информационной безопасности.
2. Угрозы информационной безопасности в информационных системах.
3. Оценочные стандарты в информационной безопасности.
4. Стандарты управления информационной безопасностью.
5. Создание СУИБ на предприятии.
6. Методика оценки рисков информационной безопасности компании Digital Security.
7. Методики и технологии управления рисками.
8. Разработка корпоративной методики анализа рисков.
9. Современные методы и средства анализа и управление рисками информационных систем компаний.
10. Правовые меры обеспечения информационной безопасности.
11. Организационные меры обеспечения безопасности компьютерных информационных систем.
12. Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом.
13. Протоколирование и аудит, шифрование, контроль целостности.

7.1. Основная литература:

1. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. URL: http://www.znanium.com/bookread.php?book=420047

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

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

7.2. Дополнительная литература:

1. 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

2. 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

3. 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

7.3. Интернет-ресурсы:

Википедия - http://ru.wikipedia.org

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

Интернет-портал по информационной безопасности - http://all-ib.ru/

Интернет-портал со статьями по алгоритмике и программированию - http://algolist.manual.ru/

Электронная библиотека по техническим наукам - http://techlibrary.ru

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Основы управления информационной безопасностью" 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.

Компьютерный класс, представляющий собой рабочее место преподавателя и не менее 15 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети КФУ и находятся в едином домене.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

Для проведения занятий требуется наличие мультимедийного оборудования, а также доска (с маркером или мелом).

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 10.03.01 "Информационная безопасность" и профилю подготовки Безопасность компьютерных систем .

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

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