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

Комплексное обеспечение информационной безопасности Б3.В.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 922216

Казань
2016

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

Специальный курс предполагает изучение различных методов и средств по построению комплексной системы информационной безопасности современной организации.

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

Данная учебная дисциплина включена в раздел " Б3.В.5 Профессиональный" основной образовательной программы 090900.62 Информационная безопасность и относится к вариативной части. Осваивается на 4 курсе, 7 семестр.

Программа курса предназначена для изучения программных и технических средств комплексной защиты информации.

Изучаются вопросыпостановка проблемы комплексного обеспечения информационной безопасности автоматизированных систем;

состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ), функциональные и обеспечивающие подсистемы,

технология, управление; методология формирования задач защиты; интеграция средств информационной безопасности в технологическую среду;

этапы проектирования КСИБ и требования к ним: предпроектное обследование, техническое задание, техническое проектирование, рабочее

проектирование, испытания и внедрение в эксплуатацию, сопровождение; особенности проектирования на современном уровне и синтез КСИБ;

типовая структура комплексной системы защиты информации от несанкционированного доступа (НСД), применения шифровальных (криптографических)

средств (средств криптографической защиты информации).

Данная дисциплина относится к профессиональным дисциплинам. Читается на 4 курсе в 7 семестре для студентов обучающихся по направлению

"Информационная безопасность".

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-5 (общекультурные компетенции)	способность к кооперации с коллегами, работе в коллективе
ОК-6 (общекультурные компетенции)	способность находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность

Шифр компетенции	Расшифровка приобретаемой компетенции
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 положения нормативно-правовых документов по обеспечению ин-формационной безопасности;

основные положения нормативно-правовых документов по обеспечению юридической значимости электронного документооборота;

основные требования нормативно-методических документов ФСБ России по организации и обеспечению функционирования шифровальных (криптографических) средств;

основные положения о лицензировании отдельных видов деятельности, свя-занных с шифровальными (криптографическими) средствами;

методы и способы криптографической защиты информации;

принципы функционирования инфраструктуры открытых ключей;

2. должен уметь:

определять необходимость применения шифровальных (криптографиче-ских) средств в системе защиты информации организации (предприятия);

оценивать и выбирать шифровальные (криптографические) средства, кото-рые могут быть использованы при создании (дооборудовании) и дальнейшей эксплуатации информационных систем;

определять комплекс мероприятий по организации и обеспечению функционирования шифровальных (криптографических) средств;

устанавливать, настраивать и эксплуатировать сертифицированные шифро-вальные (криптографические) средства.

3. должен владеть:

навыками работы с правовыми базами данных;

навыками разработки необходимых документов в интересах организации работ по защите информации ограниченного доступа с использованием

шифровальных (криптографических) средств;
навыками применения сертифицированных шифровальных (криптографических) средств;
практическими навыками построения модели угроз и нарушителей ИБ на предприятии.

Определять и обосновывать необходимость применения средств криптографической защиты информации;
аргументированно выбирать средства криптографической защиты информации, удовлетворяющие потребностям организации - обладателя информации;
правильно организовать эксплуатацию средств криптографической информации;
самостоятельно разрабатывать требуемую организационно-распорядительную документацию;

успешно эксплуатировать шифровальные (криптографические) средства;

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 4 зачетных(ые) единиц(ы) 144 часа(ов).
Форма промежуточного контроля дисциплины экзамен в 7 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. Понятия безопасности информационных технологий.	7		4	0	3	домашнее задание
2.	Тема 2. Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи.	7		6	0	2	домашнее задание
3.	Тема 3. Нормативная база обеспечения информационной безопасности	7		4	0	3	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. Конфиденциальная информация. Конфиденциальный документооборот.	7		6	0	2	контрольная работа
5.	Тема 5. Модель угроз и модель нарушителей информационной безопасности	7		4	0	2	домашнее задание
6.	Тема 6. Аудит и оценка возможных рисков ИБ	7		4	0	3	домашнее задание
7.	Тема 7. Основные типы атак на информационные системы, основные меры противодействия	7		8	0	3	контрольная работа
.	Тема . Итоговая форма контроля	7		0	0	0	экзамен
	Итого			36	0	18	

4.2 Содержание дисциплины

Тема 1. Понятия безопасности информационных технологий.

лекционное занятие (4 часа(ов)):

Актуальность проблемы обеспечения информационной безопасности. Термины и определения в области информационной безопасности. Правовое регулирование применения СКЗИ и ЭП в корпоративных информационных системах. Специальные нормативные и методические документы ФСБ России по использованию шифровальных(криптографических) средств.

лабораторная работа (3 часа(ов)):

Изучение правовой литературы по теме занятия.

Тема 2. Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи.

лекционное занятие (6 часа(ов)):

Защита от несанкционированного доступа к информации. Организация безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

лабораторная работа (2 часа(ов)):

Разбор метотов и средств защиты от несанкционированного доступа к информации.

Тема 3. Нормативная база обеспечения информационной безопасности

лекционное занятие (4 часа(ов)):

Изучение федральных законов в области информационной безопасности: "Об электронной подписи" 2011 года, "О персональных данных", "Об информации, информационых технологиях и защите информациии" 2006 года с дополнениями 2014 года.

лабораторная работа (3 часа(ов)):

Разбор основных понятий ФЗ "Об электронной подписи".

Тема 4. Конфиденциальная информация. Конфиденциальный документооборот.

лекционное занятие (6 часа(ов)):

Конфиденциальная информация. Изучение понятий государственная тайна, коммеческая тайна, персональные данные, данные ограниченного доступа. Правовые документы в области защиты конфиденциальных сведений.

лабораторная работа (2 часа(ов)):

Разбор понятий конфиденциального документооборота.

Тема 5. Модель угроз и модель нарушителей информационной безопасности

лекционное занятие (4 часа(ов)):

Модель угроз и модель нарушителей информационной безопасности. Схема построения моделей на основе стандартов ИБ.

лабораторная работа (2 часа(ов)):

Построение модель угроз и нарушителей информационной безопасности на примере.

Тема 6. Аудит и оценка возможных рисков ИБ

лекционное занятие (4 часа(ов)):

Аудит и оценка возможных рисков ИБ. Основные понятия.

лабораторная работа (3 часа(ов)):

Аудит и оценка возможных рисков ИБ предприятия на примере.

Тема 7. Основные типы атак на информационные системы, основные меры противодействия

лекционное занятие (8 часа(ов)):

Основные типы атак на информационные системы и меры их защиты. Протокол IPsec. Методы аутентификация и шифрования протокола IPsec.

лабораторная работа (3 часа(ов)):

Изучение протокола IPsec. Разбор на примерах.

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. Понятия безопасности информационных технологий.	7		подготовка домашнего задания	7	домашнее задание
2.	Тема 2. Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи.	7		подготовка домашнего задания	8	домашнее задание
3.	Тема 3. Нормативная база обеспечения информационной безопасности	7		подготовка домашнего задания	7	домашнее задание
4.	Тема 4. Конфиденциальная информация. Конфиденциальный документооборот.	7		подготовка к контрольной работе	8	контрольная работа

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
5.	Тема 5. Модель угроз и модель нарушителей информационной безопасности	7		подготовка домашнего задания	2	домашнее задание
6.	Тема 6. Аудит и оценка возможных рисков ИБ	7		подготовка домашнего задания	2	домашнее задание
7.	Тема 7. Основные типы атак на информационные системы, основные меры противодействия	7		подготовка к контрольной работе	2	контрольная работа
	Итого				36	

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лекций, лабораторных занятий, а также самостоятельной работы студентов.

Изучение курса подразумевает овладение теоретическим материалом и получение практических навыков для глубокого понимания дисциплины

"Комплексное обеспечение информационной безопасности". Практические знания студенты получают на основе решения задач и упражнений,

иллюстрирующих доказываемые теоретические положения, выполнения лабораторных занятий. Кроме того, курс помогает студентам развивать

теоретические знания в обюласти построения систем защит и способность самостоятельно оценивать степень защищенности информационных объектов

и выбирать адекватные средства защиты.

Самостоятельная работа предполагает выполнение домашних работ, подготовку к лабораторным занятиям.

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 текущие темы курса.

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

Тема 1. Понятия безопасности информационных технологий.

домашнее задание , примерные вопросы:

Углубленное изучение литературы. Обсуждение современных требований к обеспечению комплексной защиты информации, анализ угроз.

Тема 2. Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи.

домашнее задание , примерные вопросы:

Углубленное изучение литературы. Обсуждение проблем передачи информации по сетям.

Тема 3. Нормативная база обеспечения информационной безопасности

домашнее задание , примерные вопросы:

Углубленное изучение литературы. Обсуждение основных законов и нормативных актов в области комплексной защиты информации.

Тема 4. Конфиденциальная информация. Конфиденциальный документооборот.

контрольная работа , примерные вопросы:

Вариант контрольной работы 1. Контрольная работа 1. Шифрование RSA. 1. Проверить число n=57 на простоту, используя одну итерацию теста Миллера-Рабина с базой a=2. 2. Используя заданные значения p, q и e, вычислить остальные параметры RSA и расшифровать число m. Для вычисления d использовать расширенный алгоритм Евклида: p=17, q=29, e=239, m=24.

Тема 5. Модель угроз и модель нарушителей информационной безопасности

домашнее задание , примерные вопросы:

Виды угроз ИБ и их классификация. Антропогенные источники, криминальные структуры, потенциальные преступники и хакеры, недобросовестные партнеры, технический персонал поставщиков телекоммуникационных услуг, представители надзорных организаций и аварийных служб, представители силовых структур,внутренний персонал (пользователи, программисты, разработчики). Представители службы защиты информации (администраторы).

Тема 6. Аудит и оценка возможных рисков ИБ

домашнее задание , примерные вопросы:

Анализ внешних и внутренних угроз информационной системе предприятия. Выполнить разбор построения системы аудита на примере.

Тема 7. Основные типы атак на информационные системы, основные меры противодействия

контрольная работа , примерные вопросы:

Вариант контрольной работы 2. 1. Выполнить анализ системы внешних и внутренних угроз информационной системе предприятия. 2. Построить модель нарушителя для информационной системы вуза.

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

По данной дисциплине предусмотрено проведение зачета. Примерные вопросы для зачета - Приложение1.

1. Комплексная информационная безопасность автоматизированных систем

1.1 Понятие информационной безопасности;

1.2 Информационные технологии и автоматизированные системы (АС);

1.3 Методологическая основа и принципы построения систем безопасности в АС;

1.4 Системы защиты информации в АС

2. Защита АС с помощью криптографических методов

2.1 Симметричные системы шифрования

Фундаментальная основа симметричных систем шифрования;

Поточные шифры (RC4, SEAL и др.) Алгоритмы, методы реализации, применение;

Блочные шифры (AES, DES, ГОСТ 28147-89.) Алгоритмы, методы реализации, применение;

Хеш - функция

2.2 Системы шифрования с открытом ключом

Фундаментальная основа систем шифрования с открытым ключом;

Особенности системы, алгоритмы, методы и применение;

Ассиметричные шифры (RSA, DSA, Elgamal (Эль-Гамаля), Diffie-Hellman, ГОСТ Р34.11);

2.3 Инфраструктура открытых ключей (PKI) и ЭЦП

Использование Электронной цифровой подписи (ЭЦП)

Архитектура Инфраструктуры открытых ключей (ИОК\PKI);

Управление отрытыми ключами. Удостоверяющий центр. Сертификаты.
Аутентификация с использованием отрытых ключей
2.4 Правовое регулирование вопросов криптографической защиты
Российская законодательная база в области криптографической защиты информации;
Международные стандарты и соглашения в области криптографии;
Специальные требования ФСБ к ФСТЭК к криптосредствам;
Сертификация, аттестация и лицензирование СКЗИ
3. Защита обрабатываемы данных в АС в сетевом взаимодействии
3.1 Технологии защита АС на платформе ОС MS Windows;
3.2 Технологии защита АС на платформе ОС GNU\Linux, Unix;
4. Специализированное ПО и программно-аппаратные комплексы защиты в АС
4.1 Программно-аппаратные комплексы защиты от НСД;
4.2 Сравнение отечественного рынка продуктов
5. Система Управления Базами Данных (СУБД)
5.1 Управление доступом в СУБД;
5.2 Управление целостностью в СУБД;
5.3 Транзакции и операции в СУБД;
5.4 Ролевая модель, иерархия ролей, пользователи и привилегиями ;
5.5 Восстановление и безопасность хранения данных
6. Безопасность в СУБД Microsoft SQL Server
6.1 Управление правами и доступом, пользователи и роли;
6.2 Аудит безопасности;
6.3 Физическая безопасность сервера;
6.4 Атаки на SQL. Методы взлома;
6.5 Защита СУБД MS SQL Server
7. Технические мероприятия по обеспечению безопасности автоматизированных систем
7.1 Требования к системе защиты АС;
7.2 Специальные методические документы ФСБ и ФСТЭК;
7.3 Сертификация, Аттестация по требованиям ФСБ и ФСТЭК;
7.4 Технические мероприятия по обеспечению безопасности АС;

7.1. Основная литература:

1. 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
2. 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
3. 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

Интернет-портал образовательных ресурсов по ИТ - http://www.intuit.ru/studies/courses?service=0&option_id=9&service_path=1

Информационный портал по защите информации - http://all-ib.ru/

Портал с ресурсами по алгоритмике и защите информации - http://algolist.manual.ru/

Учебник "Комплексная защита информации в компьютерных системах" - http://lib.tuit.uz/books/kitob/.И.%20Завгородний%20-%20Комплексная%20защита%20информации%20

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Комплексное 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.

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.

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

Лабораторные занятия по дисциплине проводятся в компьютерном классе.

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.