МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
"Казанский (Приволжский) федеральный университет"
Факультет математики и естественных наук

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
Проф. Д.А. Таюрский
_____ «___»_____20__г.

подписано электронно-цифровой подписью

Программа дисциплины

Информационная безопасность Б1.В.ДВ.15

Направление подготовки: 44.03.04 - Профессиональное обучение (по отраслям)
Профиль подготовки: Информатика, вычислительная техника и компьютерные технологии
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Галимуллина Э.З.

Рецензент(ы):

Ибатуллин Р.Р.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Анисимова Т. И.
Протокол заседания кафедры No ___ от "____" _____ 201__г

Учебно-методическая комиссия Елабужского института КФУ (Факультет математики и естественных наук):
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 1016765219

Казань
2019

Содержание

Программу дисциплины разработал(а)(и) старший преподаватель, б/с Галимуллина Э.З.
Кафедра математики и прикладной информатики Факультет математики и естественных наук , EZGalimullina@kpfu.ru

1. Цели освоения дисциплины

Целью изучения дисциплины 'Информационная безопасность' является ознакомление студентов с основными понятиями и определениями информационной безопасности; источниками, рисками и формами атак на информацию; угрозами, которыми подвергается информация; вредоносными программами; защитой от компьютерных вирусов и других вредоносных программам; методами и средствами защиты информации; политикой безопасности компании в области информационной безопасности; стандартами информационной безопасности; криптографическими методами и алгоритмами шифрования информации; алгоритмами аутентификации пользователей; требованиям к системам защиты информации.

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

Данная учебная дисциплина включена в раздел "Б1.В.ДВ.15 Дисциплины (модули)" основной образовательной программы 44.03.04 Профессиональное обучение (по отраслям) и относится к дисциплинам по выбору. Осваивается на 4 курсе, 8 семестр.

Для освоения дисциплины 'Информационная безопасность' студенты используют знания, умения и виды деятельности, сформированные в процессе изучения предмета 'Информатика и программирование', 'Информационные технологии' и др. на предыдущем уровне образования. Помимо ее важности как самостоятельной дисциплины, она является основой для изучения других дисциплин.

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-10 (профессиональные компетенции)	владением системой эвристических методов и приемов;
ОПК-9 (профессиональные компетенции)	готовностью анализировать информацию для решения проблем, возникающих в профессионально-педагогической деятельности;
ПК-9 (профессиональные компетенции)	готовностью к формированию у обучающихся способности к профессиональному самовоспитанию.

В результате освоения дисциплины студент:

1. должен знать:

виды угроз ИС и методы обеспечения информационной безопасности;

технические и программные средства обеспечения безопасности информационных систем;

методику выбора оптимального решения по уровню информационной безопасности как компромисса между различными требованиями, связанными с безопасностью, качеством разработки, стоимостью и сроками выполнения работ;

основные понятия и задачи криптографии;

способы разграничения доступа и средства их реализации;

отечественные и зарубежные стандарты в области информационной безопасности;

2. должен уметь:

использовать в практической деятельности существующие методы и средства контроля и защиты информации;

применять программные пакеты для шифрования;

владеть средствами борьбы с компьютерными вирусами.

3. должен владеть:

инструментальными средствами проектирования баз данных и знаний, управления проектами ИС и защиты информации, а также иметь представление о перспективах развития и организации систем комплексной защиты информации;

методами анализа программных реализаций алгоритмов защиты.

4. должен демонстрировать способность и готовность:

реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов;

использовать систематизированные теоретические и практические знания для постановки и решения исследовательских задач в области образования.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 3 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. Основные понятия и анализ угроз информационной безопасности.	8		2	0	0	Устный опрос Реферат
2.	Тема 2. Политики безопасности. Модели политик безопасности	8		4	0	6	Реферат Лабораторные работы

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
3.	Тема 3. Стандарты информационной безопасности	8		2	0	0	Устный опрос Реферат
4.	Тема 4. Криптографическая защита информации.	8		6	0	16	Лабораторные работы Реферат
5.	Тема 5. Технологии аутентификации.	8		4	0	14	Лабораторные работы Реферат
.	Тема . Итоговая форма контроля	8		0	0	0	Зачет
	Итого			18	0	36	

4.2 Содержание дисциплины

Тема 1. Основные понятия и анализ угроз информационной безопасности.

лекционное занятие (2 часа(ов)):

Основные понятия и анализ угроз информационной безопасности. Основные понятия информационной безопасности. Общие понятия информационной безопасности. Анализ угроз информационной безопасности. Классификация угроз информационным системам. Основные методы обеспечения информационной безопасности информационных систем.

Тема 2. Политики безопасности. Модели политик безопасности

лекционное занятие (4 часа(ов)):

Политика безопасности. Общие принципы моделей политик безопасности. Классификация существующих моделей политики информационной безопасности. Свободные и мандатные модели политик безопасности. Модель Белла - Ла-Падулы. Модель Биба. Модель контроля целостности Кларка-Вилсона. Политика избирательного разграничения доступа. Анализ моделей политик безопасности.

лабораторная работа (6 часа(ов)):

Модель Белла - Ла-Падулы. Модель Биба. Модель контроля целостности Кларка-Вилсона. Политика избирательного разграничения доступа. Анализ моделей политик безопасности.

Тема 3. Стандарты информационной безопасности

лекционное занятие (2 часа(ов)):

Стандарты информационной безопасности. Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Отечественные стандарты безопасности информационных технологий. Государственные (национальные) стандарты РФ. Руководящие документы. Нормативные документы информационной безопасности.

Тема 4. Криптографическая защита информации.

лекционное занятие (6 часа(ов)):

Криптографическая защита информации. Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Функция хэширования. Электронная цифровая подпись. Методы криптографической защиты информации. Простейшие алгоритмы шифрования (Система шифрования Цезаря, Простая моноалфавитная замена, G-контурная многоалфавитная замена, Простая перестановка, Перестановки Гамильтона). Элементы криптоанализа. Оценка частотности символов в тексте.

лабораторная работа (16 часа(ов)):

Простейшие алгоритмы шифрования (Система шифрования Цезаря, Простая моноалфавитная замена, G-контурная многоалфавитная замена, Простая перестановка, Перестановки Гамильтона). Элементы криптоанализа. Оценка частотности символов в тексте.

Тема 5. Технологии аутентификации.

лекционное занятие (4 часа(ов)):

Технологии аутентификации. Аутентификация, авторизация и администрирование действий пользователей. Методы аутентификации, использующие пароли и PIN-коды. Биометрическая аутентификация пользователя. Аппаратно-программные системы идентификации и аутентификации. Подсистемы парольной аутентификации пользователей. Генераторы паролей. Оценка степени стойкости парольной защиты. Биометрическая аутентификация пользователя по клавиатурному почерку. Анализ динамики нажатия клавиш.

лабораторная работа (14 часа(ов)):

Подсистемы парольной аутентификации пользователей. Генераторы паролей. Оценка степени стойкости парольной защиты. Биометрическая аутентификация пользователя по клавиатурному почерку. Анализ динамики нажатия клавиш.

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. Основные понятия и анализ угроз информационной безопасности.	8		подготовка к реферату	6	Реферат
				подготовка к устному опросу	6	Устный опрос
2.	Тема 2. Политики безопасности. Модели политик безопасности	8			6	Лабораторные работы
				подготовка к реферату	4	Реферат
3.	Тема 3. Стандарты информационной безопасности	8		подготовка к реферату	6	Реферат
				подготовка к устному опросу	4	Устный опрос
4.	Тема 4. Криптографическая защита информации.	8			8	Лабораторные работы
				подготовка к реферату	4	Реферат
5.	Тема 5. Технологии аутентификации.	8			6	Лабораторные работы
				подготовка к реферату	4	Реферат
	Итого				54	

5. Образовательные технологии, включая интерактивные формы обучения

Лекционные занятия планируется проводить с применением интерактивных средств обучения, позволяющих эффективно осуществлять обратную связь со студентами, варьировать частные решения с опорой на имеющиеся готовые 'шаблоны', а также широко использовать мультимедийные возможности (нетрадиционное представление информации в различных формах - с помощью фото, видео, графики, анимации, звука), делая процесс обучения ярким, наглядным и динамичным. Также следует отметить, что использование интерактивной доски повышает интерес к дисциплине и позволяет повысить заинтересованность студентов за счет новизны способа изложения материала. Следовательно, уровень усвоения учебного материала значительно повышается.

На лабораторных занятиях по дисциплине планируется использовать проектную технологию, так как благодаря этому увеличивается возможность внедрения инновационных методов и технологий в процесс обучения, основанных на активизации самостоятельной работы студентов и формировании у них определенных методических навыков при изучении дисциплин. Одной из наиболее эффективных моделей образования в условиях применения инноваций в педагогической деятельности является организация работы студентов в малых группах и использование приемов самооценки результативности педагогического взаимодействия как овладение технологией формирования команды, целостного восприятия процесса и результата обучения, а также повышение его качества.

Для развития прогрессивных методов и приемов ведения научного и образовательного процессов в совершенствовании технологий научных исследований и проведения опережающей подготовке высококвалифицированных специалистов основывается на формировании единой информационной базы, что позволяет внедрить различные виды дистанционного обучения, организованные в стандартной форме.

Новшеством, активно применяемым в учебном процессе вуза, является технология опережающей самостоятельной работы, которая заключается в изучении студентами нового материала до его изучения в рамках аудиторных занятий. Такая форма обучения способствует развитию и закреплению системного подхода к изучению дисциплин, стимулирует самостоятельную систематическую работу.

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

Тема 1. Основные понятия и анализ угроз информационной безопасности.

Реферат , примерные вопросы:

1. Технические каналы утечки информации. 2. Выявление технических каналов утечки информации. 3. Организация и проведение поисковых мероприятий на объекте с целью обнаружения каналов утечки информации, выявления средств съема информации. 4. Методы и средства защиты информации от утечки по техническим каналам. 5. Информационная безопасность в среде Windows NT. 6. Информационная безопасность на основе Novell NetWare 7. Информационная безопасность на основе Unix. 8. Вопросы безопасности электронной торговли. 9. Защита Internet-торговли: инфраструктура и стандарты. 10. Криптография для электронной коммерции. 11. Нормативно-правовые аспекты электронного бизнеса. 12. Безопасность при работе в Интернет. 13. Стеганография - искусство сокрытия самого факта передачи информации 14. Интеллектуальная собственность в области программных продуктов. 15. Защита баз данных.

Устный опрос , примерные вопросы:

1. Основные понятия информационной безопасности. 2. Классификация угроз информационным системам. Неумышленные и умышленные угрозы. 3. Классификация угроз информационным системам (отказ в услуге, незаконное использование привилегий, "скрытые каналы", "маскарад", "сборка мусора", "люки"). 4. Классификация угроз информационным системам (вредоносные программы: "вирус", "троянский конь", "червяк", "жадная" программа, "бактерия", "логическая бомба", "лазейки"). 5. Основные методы обеспечения безопасности информационных систем. Правовое обеспечение безопасности. 6. Основные методы обеспечения безопасности информационных систем. Организационно-административное обеспечение. 7. Основные методы обеспечения безопасности информационных систем. Инженерно-технические меры обеспечения безопасности. 8. Основные методы обеспечения безопасности информационных систем. Основные функции технических средств подсистем безопасности. 9. Основные методы обеспечения безопасности информационных систем. Механизмы реализации функций технических средств подсистем безопасности. 10. Модели политик безопасности. Свободный и мандатный контроли за доступом.

Тема 2. Политики безопасности. Модели политик безопасности

Лабораторные работы , примерные вопросы:

Модель Белла - Ла-Падулы. Модель Биба. Модель контроля целостности Кларка-Вилсона. Политика избирательного разграничения доступа. Анализ моделей политик безопасности.

Реферат , примерные вопросы:

1. Защита от несанкционированного доступа. 2. Вирусы и вредоносные программы. 3. Комплексное обеспечение информационной безопасности в коммерческих структурах. 4. Исследование места и роли проблем информационной безопасности в становлении современного информационного общества. 5. Исследование проблем обеспечения баланса интересов личности, общества и государства в информационной сфере. 6. Исследование роли и места информационной безопасности в обеспечении военной, экономической, экологической, иных видов национальной безопасности. 7. Национальные интересы России и информационное противостояние в современном мире. 8. Ценностная ориентация личности, ее информационное обоснование. 9. Информационная безопасность и политическая этика. 10. Информационное пространство и проблема целостности российского государства. 11. Исследование места и роли СМИ в решении задач информационного обеспечения государственной политики Российской Федерации. 12. Правовые механизмы регулирования в сфере производства и эксплуатации криптографических продуктов. 13. Разработка правовых механизмов регулирования электронного документооборота. 14. Проблемы правового обеспечения создания и функционирования системы мониторинга угроз информационных атак на критически важные сегменты информационной инфраструктуры Российской Федерации. 15. Разработка и научное обоснование путей обеспечения информационно-психологической безопасности личности и общества.

Тема 3. Стандарты информационной безопасности

Реферат , примерные вопросы:

1. Исследование проблем обеспечения информационной безопасности национальных платежных систем на базе российских интеллектуальных карт. 2. Исследование проблем создания и развития национальной системы управления цифровыми сертификатами. 3. Разработка методов и средств проведения экспертизы и контроля качества защиты информации и информационных ресурсов, в том числе вопросов оценки базовых общесистемных программных средств на соответствие требованиям информационной безопасности. 4. Разработка методов и средств обеспечения информационной безопасности информационных и телекоммуникационных систем, в том числе автоматизированных систем управления безопасностью, методов и средств распределения ключей и защиты информации и информационных ресурсов от несанкционированного доступа и разрушающего информационного воздействия, антивирусных технологий, решение проблемы гарантированного уничтожения остаточной информации на магнитных носителях, исследование и развитие методов построения защищенных систем, использующих ненадежные (с точки зрения информационной безопасности) элементы, включая проблему их тестирования. 5. Исследование проблем безопасности общероссийской информационной инфраструктуры в условиях ее вхождения в глобальные инфраструктуры. 36. Исследование проблем обеспечения информационной безопасности ИТКС, в том числе разработка нормативно-технической документации по безопасности, автоматизированных систем управления безопасностью, унифицированного ряда средств процесса защиты с учетом используемых в ИТКС технологий обработки информации. 7. Исследование проблем информационной безопасности корпоративных сетей, в том числе сетей науки и образования. 8. Проблемы лицензирования деятельности в области информационно-телекоммуникационных систем. 9. Анализ тенденций в развитии глобальной информационной сети и состояния участия в ней России. 10. Разработка фундаментальных проблем теоретической криптографии и смежных с ней областей математики. 11. Разработка криптографических проблем создания перспективных отечественных шифрсистем (в частности, высокоскоростных). 12. Разработка и обоснование новых методов криптографического анализа современных шифрсистем. 13. Разработка перспективных криптографических протоколов взаимодействия абонентов в сложных иерархических глобальных сетях и распределенных информационно-аналитических системах. 14. Исследование существующих и разработка новых систем с открытым ключом, соответствующих этим системам схем аутентификации и электронной цифровой подписи. 15. Совершенствование нормативно-методической базы по вопросам защиты информации с применением криптографических средств.

Устный опрос , примерные вопросы:

1. Критерий оценки надежности компьютерных систем "Оранжевая книга" (США). 2. Гармонизированные критерии европейских стран. 3. Рекомендации X.800. 4. Германский стандарт BSI. 5. Британский стандарт BS7799. 6. Стандарт ISO17799. 7. Стандарт "Общие критерии" ISO15408. 8. Стандарт COBIT.

Тема 4. Криптографическая защита информации.

Лабораторные работы , примерные вопросы:

Методы криптографической защиты информации. Простейшие алгоритмы шифрования (Система шифрования Цезаря, Простая моноалфавитная замена, G-контурная многоалфавитная замена, Простая перестановка, Перестановки Гамильтона). Элементы криптоанализа. Оценка частотности символов в тексте.

Реферат , примерные вопросы:

1. Анализ основных направлений и тенденций развития отечественных и зарубежных средств криптографической защиты информации. 2. Анализ возможности использования достижений физики и техники для получения доступа к информации, обрабатываемой на современных технических средствах, в том числе исследование физических основ утечки информации от технических средств по побочным каналам, разработку проблем аналитической обработки побочных сигналов. 3. Исследование алгоритмических и технологических особенностей новейших зарубежных и отечественных технических средств обработки информации. 4. Исследование проблем и методов информационного доступа к каналам связи. 5. Разработка методологии оценивания защищенности, комплексных методов и средств защиты технических средств обработки информации от физико-технических методов несанкционированного доступа, совершенствование соответствующей нормативной базы. 6. Разработка проблем создания технических средств обработки информации, защищенных от физико-технических методов информационного доступа. 7. Сравнительный анализ тенденций развития физико-технических проблем защиты информации в стране и за рубежом. 8. Исследование архитектурных вариантов построения вычислительных систем высокой производительности, алгоритмического и программного обеспечения с учетом особенностей криптографических задач. 9. Исследование проблем построения автоматизированных систем обработки криптографической информации в неоднородной вычислительной среде. 10. Исследование проблем управления распределенными вычислительными процессами.

Тема 5. Технологии аутентификации.

Лабораторные работы , примерные вопросы:

Подсистемы парольной аутентификации пользователей. Генераторы паролей. Оценка степени стойкости парольной защиты. Биометрическая аутентификация пользователя по клавиатурному почерку. Анализ динамики нажатия клавиш.

Реферат , примерные вопросы:

1. Разработка и научное обоснование моделей угроз и стратегий защиты объектов от технических разведок. 2. Разработка методов и средств противодействия техническим разведкам с учетом эффективности их функционирования. 3. Разработка методов и средств контроля состояния и достаточности принимаемых мер по противодействию техническим разведкам на объектах защиты. 4. Разработка современной методологии обеспечения противодействия техническим разведкам на объектах защиты. 5. Разработка, теоретическое и экспериментальное исследование современных методов стеганографии, других средств тайнописи и защиты от подделки. 6. Исследование и разработка отечественных защитных экранов с учетом моделей угроз для уже существующих и перспективных цифровых АТС. 7. Проблемы кадрового обеспечения информационной безопасности Российской Федерации. 8. Обоснование облика, структуры и путей реализации единой системы подготовки кадров в области современных информационных технологий и информационной безопасности. 9. Обоснование структуры и функций Учебно-методического комплекса по подготовке, повышению квалификации и переподготовке кадров в области информационной безопасности.

Итоговая форма контроля

зачет (в 8 семестре)

Примерные вопросы к зачету:

1. Основные понятия информационной безопасности.

2. Классификация угроз информационным системам. Неумышленные и умышленные угрозы.

3. Классификация угроз информационным системам (отказ в услуге, незаконное использование привилегий, "скрытые каналы", "маскарад", "сборка мусора", "люки").

4. Классификация угроз информационным системам (вредоносные программы: "вирус", "троянский конь", "червяк", "жадная" программа, "бактерия", "логическая бомба", "лазейки").

5. Основные методы обеспечения безопасности информационных систем. Правовое обеспечение безопасности.

6. Основные методы обеспечения безопасности информационных систем. Организационно-административное обеспечение.

7. Основные методы обеспечения безопасности информационных систем. Инженерно-технические меры обеспечения безопасности.

8. Основные методы обеспечения безопасности информационных систем. Основные функции технических средств подсистем безопасности.

9. Основные методы обеспечения безопасности информационных систем. Механизмы реализации функций технических средств подсистем безопасности.

10. Модели политик безопасности. Свободный и мандатный контроли за доступом.

11. Модели политик безопасности. Мандатные политики безопасности.

12. Модели политик безопасности. Модель Белла-Ла-Падулы.

13. Модели политик безопасности. Модель Биба.

14. Модели политик безопасности. Модель контроля целостности Кларка-Вилсона.

15. Модели политик безопасности. Политики избирательного разграничения доступа.

16. Идентификация и аутентификация субъектов.

17. Парольные системы идентификации и аутентификации пользователей. Основные требования к выбору и использованию паролей.

18. Парольные системы идентификации и аутентификации пользователей. Количественная оценка стойкости парольных систем.

19. Идентификация и аутентификация пользователей с использованием технических устройств.

20. Идентификация и аутентификация с использованием индивидуальных биометрических характеристик пользователя.

21. Криптографические методы защиты информации. Основные понятия криптографии.

22. Криптографические методы защиты информации. Классификация криптографических алгоритмов.

23. Криптоалгоритмы с ключом. Симметричные и асимметричные криптогалгоритмы.

24. Криптографические методы защиты информации. Виды атак на шифры.

25. Традиционные симметричные криптосистемы. Шифрование методом замены. Шифрование методом цезаря.

26. Традиционные симметричные криптосистемы. Шифрование методом замены. Простая моноалфавитная замена.

27. Традиционные симметричные криптосистемы. Шифрование методом замены. Шифрующие таблицы Трисемуса.

28. Традиционные симметричные криптосистемы. Шифрование методом замены. Многооалфавитная замена. Шифр Гронсфельда.

29. Традиционные симметричные криптосистемы. Шифрование методом замены. Многооалфавитная замена. Система шифрования Вижинера.

30. Традиционные симметричные криптосистемы. Шифрование методом замены. Многооалфавитная замена. Шифрование методом Вернама.

31. Традиционные симметричные криптосистемы. Шифрование методом замены. Многооалфавитная замена. G-контурная многоалфавитная замена.

32. Традиционные симметричные криптосистемы. Шифрование методами перестановки. Метод простой перестановки.

33. Традиционные симметричные криптосистемы. Шифрование методами перестановки по маршрутам Гамильтона.

34. Традиционные симметричные криптосистемы. Шифрование методами перестановки. Шифрование методом гаммирования.

35. Симметричные криптосистемы шифрования. Основные принципы блочного симметричного шифрования.

36. Симметричные криптосистемы шифрования. Алгоритм шифрования DES.

37. Симметричные криптосистемы шифрования. Комбинирование блочных алгоритмов.

38. Симметричные криптосистемы шифрования. Стандарт шифрования ГОСТ 28147-89.

39. Симметричные криптосистемы шифрования. Американский стандарт шифрования AES.

40. Симметричные криптосистемы шифрования. Другие симметричные криптоалгоритмы.

41. Симметричные криптосистемы шифрования. Особенности применения алгоритмов симметричного шифрования.

42. Асимметричные криптосистемы шифрования. Особенности асимметричных криптосистем шифрования.

43. Асимметричные криптосистемы шифрования. Алгоритм шифрования RSA.

44. Асимметричные криптосистемы шифрования. Прцедуры шифрования и расшифрования в алгоритме RSA.

45. Асимметричные криптосистемы шифрования. Асимметричные криптосистемы на базе эллиптических кривых.

46. Асимметричные криптосистемы шифрования. Алгоритм асимметричного шифрования ECES.

7.1. Основная литература:

1.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/bookread2.php?book=405000

2. Практическая криптография: Пособие / Масленников М.Е. - СПб:БХВ-Петербург, 2015. - URL: http://znanium.com/bookread2.php?book=944503

3. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие/ГлинскаяЕ.В., ЧичваринН.В. - М.: НИЦ ИНФРА-М, 2016. - 118 с. - URL: http://znanium.com/bookread2.php?book=507334

7.2. Дополнительная литература:

1. Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин В. Ф. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2016. - 416 с. - URL: http://znanium.com/bookread2.php?book=549989

2. Информационная безопасность: Учебное пособие / Партыка Т. Л., Попов И. И. - 5-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2016. - 432 с. - URL: http://znanium.com/bookread2.php?book=516806

3. Информационная безопасность предприятия: Учебное пособие / Гришина Н.В., - 2-е изд., доп - М.:Форум, НИЦ ИНФРА-М, 2016. - 240 с. - URL: http://znanium.com/bookread2.php?book=544554

7.3. Интернет-ресурсы:

Антивирусная защита компьютерных систем НОЧУ ВПО "Национальный открытый университет "ИНТУИТ" - http://www.intuit.ru/studies/courses/2259/155/info

Барсуков В., Физическая защита информационных систем - http://www.jetinfo.ru/1997/1/1/article1.1.1997.html

Беззубцев О., Ковалев А., О лицензировании и сертификации в области защиты информации - http://www.jetinfo.ru/1997/4/1/article1.4.1997.html

Браунли Н., Гатмэн Э., Как реагировать на нарушения информационной безопасности (RFC 2350, BCP 21) - http://www.jetinfo.ru/2000/5/1/article1.5.2000.html

Винклер А., Задание: шпионаж - http://www.jetinfo.ru/1996/19/1/article1.19.1996.html

Основы информационной безопасности В.Галатенко НОЧУ ВПО "Национальный открытый университет "ИНТУИТ" - http://www.intuit.ru/studies/courses/10/10/info

Симонов С., Анализ рисков, управление рисками - http://www.jetinfo.ru/1999/1/1/article1.1.1999.html

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Информационная безопасность" 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.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен студентам. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

Освоение данной дисциплины предполагает использование следующего материально-технического обеспечения: проектор, экран и интерактивная трибуна.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 44.03.04 "Профессиональное обучение (по отраслям)" и профилю подготовки Информатика, вычислительная техника и компьютерные технологии .

Автор(ы):
Галимуллина Э.З. _____
"__" _____ 201 __ г.

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