МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФГБОУ ВО «ИГУ»

Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ
проф. Бурков И.М.
"28" 06 2016 г.

Рабочая программа дисциплины (модуля)

Наименование дисциплины (модуля) Б1.В.ОД.5 «Экспертные системы комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем»

Направление подготовки - 03.04.03 «Радиофизика»

Тип образовательной программы - академическая

Направленность (профиль) подготовки «Информационные процессы и системы»

Квалификация (степень) выпускника - Магистр

Форма обучения - очная

Согласовано с УМК физического факультета
Протокол №3 от «28» 06 2016г.
Председатель

Рекомендовано кафедрой:
Протокол № 12
От «28» 06 2016г.
И.О.Зав. кафедрой
Колесник С.Н.

Иркутск 2016 г.

Содержание

Стр.

1. Цели и задачи дисциплины (модуля):

Целью изучения учебной дисциплины «Экспертные системы комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем» является изложение основ методики проектирования экспертных систем, а также принципов работы и возможностей современных интеллектуальных систем в области информационной безопасности. Подготовка к научным исследованиям с использованием и разработкой экспертных систем, а также приобретение навыков применения в инженерной практике современных интеллектуальных систем в области защиты информации.

2. Место дисциплины в структуре ООП:

Учебная дисциплина «Экспертные системы комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем» входит в вариативную часть обязательных дисциплин.

Дисциплина базируется на содержании следующих дисциплин, изучаемых в период подготовки бакалавров: теория информации и базы данных, компьютерные вычислительные сети Ч1.

3. Требования к результатам освоения дисциплины (модуля):

Процесс изучения дисциплины (модуля) направлен на формирование следующих компетенций:

общекультурной компетенции:

способностью к абстрактному мышлению, анализу, синтезу (ОК-1).

общепрофессиональной компетенции:

способностью к свободному владению профессионально-профилированными знаниями в области информационных технологий, использованию современных компьютерных сетей, программных продуктов и ресурсов Интернет для решения задач профессиональной деятельности, в том числе находящихся за пределами профильной подготовки (ОПК-4).

В результате изучения дисциплины студент должен:

Знать:

Индекс компетенции	Индекс образовательного результата	Образовательный результат
ОК-1	З-1	функции и структуру экспертных систем, области применения экспертных систем, тенденции развития экспертных систем, функциональную, логическую и объектно-ориентированную парадигмы программирования, программные и технические средства разработки экспертных систем, технологию разработки экспертных систем, методы извлечения и модели представления знаний, методы поиска решений в экспертных системах, а также основные технические характеристики и принципы работы современных интеллектуальных систем в области информационной безопасности.

Уметь:

Индекс компетенции	Индекс образовательного результата	Образовательный результат
ОК-1	У-1	обоснованно выбирать модель представления знаний и программные средства разработки экспертных систем;

		учитывать неопределенность знаний в процессе принятия решений, а также применять на практике современные интеллектуальные системы в области защиты информации.
ОПК-4	У-3	использовать современные компьютерные сети, программные продукты и ресурсы информационно-телекоммуникационной сети «Интернет» для изучения экспертных систем комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем.

Владеть:

Индекс компетенции	Индекс образовательного результата	Образовательный результат
ОК-1	В-1	методами поиска решений в экспертных системах; навыками проектирования экспертных систем и эксплуатации современных интеллектуальных систем в области информационной безопасности.

4. Объем дисциплины (модуля) и виды учебной работы (разделяется по формам обучения)

Вид учебной работы	**Всего часов / зачетных единиц**	**Семестры**			
		1			
Аудиторные занятия (всего)	40/1.11	40/1.11			
В том числе:					
Лекции	18/0.5	18/0.5			
Практические занятия (ПЗ)	18/0.5	18/0.5			
Семинары (С)					
КСР	4/0,11	4/0,11			
Самостоятельная работа(всего)	68/1.88	68/1.88			
В том числе:					
Курсовой проект (работа)					
Расчетно-графические работы					
Реферат (при наличии)					
Другие виды самостоятельной работы					
Вид промежуточной аттестации: экзамен	36/1	36/1			
Вид итоговой аттестации:					
Контактная работа	47	47			
Общая трудоемкость: часы	144	144			
зачетные единицы	4	4			

5. Содержание дисциплины (модуля)

5.1. Содержание разделов и тем дисциплины (модуля).

Т1. Основы безопасности информационных технологий.

Основные понятия в области безопасности информационных технологий. Угрозы безопасности информационных технологий. Принципы обеспечения безопасности

информационных технологий.

Т2. Обеспечение безопасности информационных технологий.

Организационная структура системы обеспечения безопасности информационных технологий. Обязанности пользователей и ответственных за обеспечение безопасности информационных технологий. Документы, регламентирующие правила парольной и антивирусной защиты.

Т3. Средства защиты информации от несанкционированного доступа.

Назначение и возможности средств защиты информации от несанкционированного доступа. Рекомендации по выбору средств защиты информации от несанкционированного доступа.

Т4. Обеспечение безопасности компьютерных систем и сетей.

Проблемы обеспечения безопасности в компьютерных системах и сетях. Назначение, возможности и защитные механизмы межсетевых экранов. Анализ содержимого почтового и WEB-трафика. Виртуальные частные сети. Обнаружение и устранение уязвимостей.

Т5. Основы информационной безопасности.

Значение информационной безопасности и ее место в системе национальной безопасности. Основные составляющие национальных интересов Российской Федерации в информационной сфере. Виды и источники угроз информационной безопасности Российской Федерации.

Т6. Комплексная система защиты информации.

Общая характеристика комплексной защиты информации. Конфиденциальные сведения. Система физической защиты. Подсистема инженерной защиты. Способы и средства обнаружения угроз.

Т7. Инженерно-техническая защита информации.

Основы инженерно-технической защиты информации. Понятие несанкционированного доступа к защищаемой информации. Технические каналы утечки информации.

Т8. Криптографическая защита информации.

Основы криптографии. Симметричные криптосистемы. Криптосистемы с открытым ключом. Системы электронной подписи. Криптоанализ.

5.2 Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№ № разделов и тем данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин (вписываются разработчиком)						
1.	НИР	Р1	Р2	Р3	Р4	Р5		
2.	Государственная итоговая аттестация (государственный экзамен)	Р1	Р2	Р3	Р4	Р5		

5.3. Разделы и темы дисциплин (модулей) и виды занятий

№ п/п	Наименование раздела Наименование темы	Виды занятий в часах					
		Лекц.	Практ. зан.	Семин	КСР.	СРС	Всего
1	Тема 1. Основы безопасности информационных технологий	2	2			8	12
2	Тема 2. Обеспечение безопасности информационных	4	4			10	18

	технологий						
3	Тема 3. Средства защиты информации от несанкционированного доступа	2	2			8	12
4	Тема 4. Обеспечение безопасности компьютерных систем и сетей	2	2		2	8	14
5	Тема 5. Основы информационной безопасности	2	2			8	12
6	Тема 6. Комплексная система защиты информации	2	2			8	12
7	Тема 7. Инженерно-техническая защита информации	2	2			10	14
8	Тема 8. Криптографическая защита информации	2	2		2	8	14

6. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы дисциплины	Наименование семинаров, практических и лабораторных работ	Трудоемкость (часы)	Оценочные средства	Формируемые компетенции
1	**2**	**3**	**4**	**5**	**6**
1	Т1.	Изучение программы «РЕВИЗОР -1 XP»	2	Письменный текущий контроль	ОК-1, ОПК-4
2	Т2.	Изучение программы «СТРАЖ NT»	2	Письменный текущий контроль	ОК-1, ОПК-4
3	Т2.	Изучение программы «СТРАЖ NT»	2	Письменный текущий контроль	ОК-1, ОПК-4
4	Т3.	Изучение программы «Гроза-К», «Ревизор-2XP»	2	Письменный текущий контроль	ОК-1, ОПК-4
5	Т4.	Изучение программы «SecretNET»	2	Письменный текущий контроль	ОК-1, ОПК-4
6	Т5	Изучение аппаратуры «NR-900EMS», «Аврора-3», «Крона-ПРО».	2	Письменный текущий контроль	ОК-1, ОПК-4
7	Т6.	Изучение аппаратуры «Соната-Р2»	2	Письменный текущий контроль	ОК-1, ОПК-4
8	Т7.	Изучение системы «Талис-нч –лайт»	2	Письменный текущий контроль	ОК-1, ОПК-4
9	Т8.	Изучение аппаратуры «Ладья-ИВТ», «Кедр-1М»	2	Письменный текущий контроль	ОК-1, ОПК-4

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1	Т1.	Работа с учебником, справочной литературой, первоисточниками, конспектом	Изучение, повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	Источники 1 -4 из основной и 1-9 из дополнительной литературы; Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ	8
2	Т2.				5
3	Т2.				5
4	Т3.				8
5	Т4.				8
6	Т5.				8
7	Т6.				8
8	Т.7				10
9	Т.8				8

6.2. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа магистров – индивидуальная учебная деятельность, осуществляемая без непосредственного руководства преподавателя (научного руководителя (консультанта)), в ходе которой магистр активно воспринимает, осмысливает полученную информацию, решает теоретические и практические задачи. В процессе проведения самостоятельной работы формируется компетенция ОПК-4.

На самостоятельную работу выносятся следующие вопросы по темам дисциплины:

Т1. Принципы обеспечения безопасности информационных технологий (4ч). Проработка лекционного материала и материала практических занятий (4ч).

Т2. Обязанности пользователей и ответственных за обеспечение безопасности информационных технологий. Документы, регламентирующие правила парольной и антивирусной защиты (4ч). Проработка лекционного материала и материала практических занятий (6ч).

Т3. Рекомендации по выбору средств защиты информации от несанкционированного доступа (4ч). Проработка лекционного материала и материала практических занятий (4ч).

Т4. Анализ содержимого почтового и WEB-трафика. Виртуальные частные сети. Обнаружение и устранение уязвимостей (4ч). Проработка лекционного материала и материала практических занятий (4ч).

Т5. Виды и источники угроз информационной безопасности Российской Федерации (4ч). Проработка лекционного материала и материала практических занятий (4ч).

Т6. Подсистема инженерной защиты. Способы и средства обнаружения угроз (4ч). Проработка лекционного материала и материала практических занятий (4ч).

Т7. Технические каналы утечки информации (4ч.). Проработка лекционного материала и материала практических занятий (6ч).

Т8. Криптосистемы с открытым ключом. Системы электронной подписи. Криптоанализ (4ч). Проработка лекционного материала и материала практических занятий (4ч).

Контроль самостоятельной работы проводится на практических занятиях и на КСР по окончании Т4 и Т8.

7. Примерная тематика курсовых работ (проектов) (при наличии)

Планом не предусмотрено

8. Учебно-методическое и информационное обеспечение дисциплины (модуля):

а) основная литература

1. Глухих В. И. Информационная безопасность и защита данных: учеб. пособие для студ. вузов/ В. И. Глухих ; рец.: Б. В. Агалаков, Р. В. Мещеряков, Е. А. Черкашин; Иркут. гос. техн. ун-т. – Иркутск: Изд-во ИрГТУ, 2012. – 244 с.: а-ил.. – Библиогр.: с. 242-244. (1 экземпляр) ISBN 978-5-8038-08-05-3

2. Мезенцев, Александр Владимирович. Технологии защищенной обработки информации: учеб. пособие/ А. В. Мезенцев, Н. И. Синадский, Д. А. Хорьков ; рец.: Ф. И. Иванов, О. Н. Соболев; Иркутский гос. ун-т, Ин-т мат., экон. и информ.. – Иркутск: Изд-во ИГУ, 2013. – 120 с.: а-ил. (2 экземпляр) ISBN 978-5-9624-07-93-7

3. Мельников Д. А. Организация и обеспечение безопасности информационно-технологических сетей и систем: учеб. для студ. вузов, обуч. по спец. 080801 "Прикладная информатика (по обл.)" и др. экон. спец./ Д. А. Мельников. – М.: Университет. кн., 2012. – 598 (1 экземпляр) ISBN 978-5-91304-246-0

б) дополнительная литература

1. Сердюк, Виктор Александрович. Организация и технология защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учеб. пособие/ В. А. Сердюк; Гос. ун-т - Высш. шк. экономики. – М.: Изд-во ГУ ВШЭ, 2011. – 572 с.: а-ил.. – Библиогр.: с. 541-567 (2 экземпляров)

2. Ярочкин В.И. Информационная безопасность : учеб. для студ. вузов, обуч. по гуманитар. и социально-экон. спец. / В.И. Ярочкин. - М.: Мир: Академ. проект, 2003. - 639 с.: ил. (1 экземпляр)

3. Гришина Н. В. Организация комплексной системы защиты информации [Текст] / Н. В. Гришина. - М. : Гелиос АРВ, 2007. - 255 с. (1 экземпляр)

4. Максимов, Н.В. Современные информационные технологии [Текст] : учебник для студ. учрежд. сред. проф. образ. / Н. В. Максимов, Т. Л. Партыка, И. И. Попов. - М. : Форум, 2012. - 509 с. : ил. (1 экземпляр)

5. Корнеев И. К., Степанов Е. А. Защита информации в офисе. - М.: Проспект, 2010. (1 экземпляр)

6. Куприянов А. И., Шевцов В. А., Сахаров А. В. Основы защиты информации. - М.: Академия, 2010. (2 экземпляра)

Сверено с НБ ИГУ

в) программное обеспечение

1. Microsoft PowerPoint

г) базы данных, информационно-справочные и поисковые системы

1. Поисковые системы Google, Yandex.

2. Электронные ресурсы доступные по логину и паролю, предоставляемые Научной библиотекой ИГУ.

9. Материально-техническое обеспечение дисциплины (модуля):

Чтение лекций сопровождается демонстрацией информации (мультимедийный проектор, офисное оборудование для оперативного размножения иллюстративного и раздаточного лекционного материалов).

10. Образовательные технологии:

На лекциях используются активные методы обучения (компьютерных симуляций, разбор конкретных ситуаций). Практические занятия 1-9 проводятся в интерактивной форме.

11. Оценочные средства (ОС):

11.1. Оценочные средства для входного контроля

Не предусмотрено.

11.2 Оценочные средства текущего контроля

Текущий контроль реализуется в виде письменного текущего контроля на ПЗ1-ПЗ9. Текущий контроль направлен на выявление сформированности компетенций ОК-1, ОПК-4.

Для реализации текущего контроля используется балльно-рейтинговая система оценки, принятая в университете.

Усвоение магистрантом изучаемой дисциплины максимально оценивается 100 баллами. Максимальное количество баллов за текущую работу в семестре ограничивается 60-ю баллами, на оценку экзамена максимально предусмотрено 30 баллов. Возможны «премиальные» баллы (от 0 до 10), которые могут быть добавлены магистру за активные формы работы, высокое качество выполненных практических работ и т.д.

За посещение одного вида занятия дается 0.5 балла (20 занятий (Л+Пз+СКР) * 0.8 балла = 16 баллов), максимальное количество баллов за письменный контроль на одном СКР или одном Пз – 4 балла (11 занятий (КСР+ПЗ)*4 балла = 44 балла).

Параметры оценочного средства для письменного текущего контроля на ПЗ1-ПЗ9, КСР1-КСР2.

Критерии оценки	Оценка / баллы			
	Отлично 4 балла.	Хорошо 2.7 балла	Удовлетв. 1.3 балла.	Неудовл. 0 баллов
Выполнение заданий	Полностью и корректно выполнены все задания.	Полностью выполнены все задания, допущены одна – две ошибки.	Не полностью выполнены задания, допущены одна – две ошибки.	Задание не выполнены или задание выполнено не полностью и допущено более 3-х ошибок.

Вопросы для письменного текущего контроля приведены ниже:

Пз.1. Информация и информационные отношения. Субъекты информационных отношений, их безопасность. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Классификация угроз безопасности. Виды мер противодействия угрозам безопасности. Достоинства и недостатки различных видов мер защиты. Принципы построения системы обеспечения безопасности информации в автоматизированной системе.

Пз.2. Понятие технологии обеспечения безопасности информации. Влияние на безопасность со стороны руководства организаций. Институт ответственных за обеспечение безопасности ИТ. Общие правила обеспечения безопасности ИТ при работе сотрудников. Ответственность за нарушения. Порядок работы с носителями ключевой информации.

Назначение, особенности работы программы «Ревизор-1XP».

Пз.3. Инструкция по организации парольной защиты. Инструкция по организации антивирусной защиты.

Пз.4. Защита от вмешательства в процесс функционирования АС посторонних лиц. Регистрация действий пользователей. Обеспечение аутентификации абонентов. Распределение показателей защищенности по классам для автоматизированных систем. Требования руководящих документов ФСТЭК к средствам защиты информации.

КСР1 Типовая корпоративная сеть. Уязвимости и их классификация. Угрозы, связанные с периметром сети. Типы межсетевых экранов. Сертификация межсетевых экранов. HTTP-трафик. Виртуальные частные сети: решение на базе ОС Windows 2003; VPN на основе криптошлюза «Континент-К».
Назначение и особенности работы программы «СТРАЖ NT».

Пз. 5 Значение информационной безопасности и ее место в системе национальной безопасности: роль информационной безопасности; национальная безопасность РФ. Доктрина информационной безопасности Российской Федерации.
Назначение и особенности работы программы «Гроза-К», «Ревизор-2XP».

Пз. 6 Основы обеспечения комплексной защиты информации. Сущность и задачи комплексной защиты информации. Стратегии комплексной защиты информации. Структура и основные характеристики комплексной защиты информации. Периметровая сигнализация и ограждение.
Периметровое освещение. Комплексное обследования защищенности информационной системы. Средства нейтрализации угроз.
Назначение и особенности работы программы «SecretNET»

Пз.7 Понятие технической защиты информации и их основные задачи. Механические системы защиты. Понятие несанкционированного доступа к информации. Виды несанкционированного доступа к информации. Общая структура канала утечки информации. Классификация каналов утечки информации.
Назначение и особенности работы программы «NR-900EMS», «Аврора-3», «Крона-ПРО».

Пз.8 Структура криптосистемы. Основные методы криптографического преобразования данных. Шифрование методом замены. Шифрование методом перестановки. Шифрование методом гаммирования.
Назначение и особенности работы аппаратуры «Соната-Р2».

Пз.9 Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом.
Назначение и особенности работы системы «Талис-нч –лайт».

КСР2 Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи. Безопасные хеш-функции, алгоритмы хеширования. Контрольное значение циклического избыточного кода CRC. Цифровые сертификаты. Отечественный стандарт цифровой подписи. Понятие криптоанализа.
Назначение и особенности работы аппаратуры «Ладья-ИВТ», «Кедр-1М».

11.3 Оценочные средства для промежуточной аттестации

Промежуточная аттестация направлена на проверку сформированности компетенций ОК-1, ОПК-4 и проводится в форме экзамена. Форма проведения экзамена – устный по билетам или письменный по билетам. Экзамены проводятся во время экзаменационных сессий в соответствии с расписанием.

Экзаменационный билет состоит из одного теоретического и одного практического вопроса. Экзаменационные задания (билеты) для приема экзаменов выполнены многовариантными, чтобы исключить возможность списывания и обмена информацией в

ходе экзамена. Вопросы для самостоятельной подготовки студентов к экзамену приведены в приложении 1.

Магистрант допускается к экзамену в том случае, если в течение семестра за текущую работу набрано 40 баллов и более. В противном случае выставляется 0 сессионных баллов. Во время экзамена магистрант может набрать до 30 баллов. Если на экзамене ответ студента оценивается менее чем 10-ю баллами, то экзамен считается не сданным, магистранту выставляется 0 баллов, а в ведомость выставляется оценка «неудовлетворительно».

Если на экзамене студент набирает 10 и более баллов, то они прибавляются к сумме баллов за текущую работу и переводятся в академическую оценку, которая фиксируется в ведомости и зачетной книжке студентов.

Итоговый семестровый рейтинг	Академическая оценка
60-70 баллов	«удовлетворительно»
71-85 баллов	«хорошо»
86-100 баллов	«отлично»

Преподаватель имеет право выставить экзаменационную оценку (с согласия студента) без процедуры сдачи экзамена, если сумма баллов, набранная студентом за текущую работу составит 70 баллов. В этом случае к набранному студентом количеству баллов за текущую работу автоматически добавляется 20 баллов и выставляется соответствующая академическая оценка.

Критерии	Оценка			
	Отлично	Хорошо	Удовлетв.	Неудовлетв.
Знание	Всесторонние глубокие знания **(10 -11 баллов)**	Знание материала в пределах программы **(7 -9 баллов)**	Отмечены пробелы в усвоении программного материала **(4 -6 баллов)**	Не знает основное содержание дисциплины **(0-3 балла)**
Понимание	Полное понимание материала, приводит примеры, дополнительные вопросы не требуются **(8 -10 баллов)**	Понимает материал, приводит примеры, но испытывает затруднения с выводами, однако достаточно полно отвечает на дополнительные вопросы **(6 -8 баллов)**	Суждения поверхностны, содержат ошибки, примеры не приводит, ответы на дополнительные вопросы неуверенные **(4 -6 баллов)**	С трудом формулирует свои мысли, не приводит примеры, не дает ответа на дополнительные вопросы **(0-3 балла)**
Применение проф. терминологии	Дает емкие определения основных понятий, корректно использует профессиональную терминологию**(3-5 баллов)**	Допускает неточности в определении понятий, не в полном объеме использует профессиональную терминологию **(2-3 балла)**	Путает понятия, редко использует профессиональную терминологию **(1-2 балла)**	Затрудняется в определении основных понятий дисциплины, некорректно использует профессиональную терминологию (**0-2 балла**)
Соблюдение	Соблюдает нормы	Соблюдает нормы	Допускает	Косноязычная речь

норм литературного языка	литературного языка, преобладает научный стиль изложения **(3-4 балла)**	литературного языка, допускает единичные ошибки **(2- 3 балла)**	множественные речевые ошибки при изложении материала **(1-2 балл)**	искажает смысл ответа (**0-1 балл**)

Приложение 1

Примерный перечень вопросов и заданий к экзамену

1. Основные причины обострения проблемы обеспечения безопасности информационных технологий.
2. Основные понятия в области безопасности информационных технологий.
3. Информация и информационные отношения.
4. Субъекты информационных отношений, их безопасность.
5. Угрозы безопасности информационных технологий.
6. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем.
7. Классификация угроз безопасности.
8. Принципы обеспечения безопасности информационных технологий.
9. Виды мер противодействия угрозам безопасности.
10. Достоинства и недостатки различных видов мер защиты.
11. Принципы построения системы обеспечения безопасности информации в автоматизированной системе.
12. Правовые основы обеспечения безопасности информационных технологий.
13. Информация в ключевых системах информационной инфраструктуры.
14. Государственная система защита информации.
15. Организация защиты информации в системах и средствах информатизации и связи.
16. Контроль состояния защиты информации.
17. Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты.
18. Идентификация и аутентификация пользователей.
19. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы.
20. Регистрация и оперативное оповещение о событиях безопасности.
21. Понятие технологии обеспечения безопасности информации.
22. Влияние на безопасность со стороны руководства организаций.
23. Институт ответственных за обеспечение безопасности ИТ.
24. Общие правила обеспечения безопасности ИТ при работе сотрудников.
25. Ответственность за нарушения.
26. Порядок работы с носителями ключевой информации.
27. Защита от вмешательства в процесс функционирования АС посторонних лиц.
28. Регистрация действий пользователей.
29. Обеспечение аутентификации абонентов.
30. Назначение и особенности применения СЗИ НСД «Страж NT.
31. Назначение и особенности применения «Ревизор -1XP».
32. Реализация схем аутентификации.
33. Программные средства, реализующие инфраструктуру открытых ключей.
34. Алгоритм генерации одноразовых паролей.
35. Формирование электронной цифровой подписи.
36. Вычисление ключа согласования Диффи-Хеллмана.
37. Избирательное разграничение доступа.
38. Полномочное разграничение доступа.

39. Регистрация событий, имеющих отношение к безопасности.
40. Назначение и особенности применения «Гроза-К».
41. Назначение и особенности применения «Ревизор -2XP».
42. Угрозы, связанные с периметром сети.
43. Типы межсетевых экранов.
44. Сертификация межсетевых экранов.
45. HTTP-трафик.
46. Решения на базе ОС Windows 2003.
47. VPN на основе криптошлюза «Континент – К».
48. Архитектура систем управления уязвимостями.
49. Особенности сетевых агентов сканирования.
50. Специализированный анализ защищенности.
51. Обзор средств анализа защищенности.
52. Инфраструктура управления журналами событий.
53. Категории журналов событий.
54. Технология обнаружения атак.
55. Классификация систем обнаружения атак.
56. Основы обеспечения комплексной защиты информации.
57. Сущность и задачи комплексной защиты информации.
58. Стратегия комплексной защиты информации.
59. Структура и основные характеристики комплексной защиты информации.
60. Конфиденциальные сведения.
61. Система физической защиты.
62. Подсистема инженерной защиты.
63. Комплексное обследование защищенности информационной системы.
64. Средства нейтрализации угроз.
65. Основы инженерно-технической защиты информации.
66. Понятие несанкционированного доступа к защищаемой информации.
67. Технические каналы утечки информации.
68. Основные способы и средства НДС к защищаемой информации.
69. Защита информации от утечки по техническим каналам передачи информации.
70. Обеспечение безопасности телефонных переговоров.
71. Защита от перехвата.
72. Акустический контроль.
73. Демаскирующие признаки закладных устройств.
74. Контроль линии связи, отходящей от технических средств.
75. Средства нелинейной радиолокации.
76. Методы поиска радиоизлучений закладных устройств.
77. Основы криптографии.
78. Симметричные криптосистемы
79. Криптосистемы с открытым ключом.
80. Системы электронной подписи. Криптоанализ.

Разработчики:

И.О. Зав.кафедры — Колесник С.Н.
(занимаемая должность) — (инициалы, фамилия)

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники
(наименование)

«28» 06 2016г.

Протокол № 12 И.О.Зав.кафедрой _____ Колесник С.Н.