Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Иркутский государственный университет»
(ФГБОУ ВО «ИГУ»)

Факультет (институт) физический
Кафедра радиофизики и радиоэлектроники

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине **Б1.В.ОД.5 «Экспертные системы комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем»**

направление подготовки - 03.04.03 «Радиофизика»
направленность (профиль) «Информационные процессы и системы»

Иркутск, 2016

Разработан в соответствии с ФГОС ВО по направлению подготовки 03.04.03 от 28 ноября 2014 г. N 1417

с учетом требований проф. стандарта: Научный работник (научная (научно-исследовательская) деятельность).

Одобрен
УМК физического факультета
Протокол №3 от «28.06.2016»

Председатель УМК декан, д.ф.-м.н., проф _____ Буднев Н.М.
ФИО, должность, ученая степень, звание *подпись*

Разработчик Колесник С.Н. доц, к.ф.-м.н., доц. _____
ФИО, должность, ученая степень, звание *подпись*

Декан, д.ф.-м.н., профессор _____ Буднев Н.М.
ФИО, должность, ученая степень, звание *подпись*

ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине

Б1.В.ОД.5 «Экспертные системы комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем»
03.04.03 «Радиофизика», «Информационные процессы и системы»

1. **Компетенции (дескрипторы компетенций), формируемые в процессе изучения дисциплины** (курс 1 семестр 1):

Индекс и наименование компетенции (в соответствии с ФГОС ВО (ВПО)	Признаки проявления компетенции/ дескриптора (ов) в соответствии с уровнем формирования в процессе освоения дисциплины
способностью к абстрактному мышлению, анализу, синтезу (ОК-1).	**Знать:** (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:** (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. **Владеть:** (В-1) методами поиска решений в экспертных системах; навыками проектирования экспертных систем и эксплуатации современных интеллектуальных систем в области информационной безопасности.
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)	**Знать :** (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.

2. В результате освоения дисциплины обучающийся должен

Знать: 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: 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; 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: методами поиска решений в экспертных системах; навыками проектирования экспертных систем и эксплуатации современных интеллектуальных систем в области информационной безопасности.

3. Программа оценивания контролируемой компетенции:

Тема или раздел дисциплдины	Формируемый признак компетен-ции	Показатель	Критерий оценивания	Наименование ОС	
				ТК	ПА
Тема 1. Основы безопасности информационных технологий	З-1, У-1, У-3	Показывает знания и умения использования основные понятий в области безопасности информационных технологий. Демонстрирует знания об угрозах информационной безопасности. Показывает знание принципов обеспечения безопасности.	Таблица 1, таблица 2.	УК, ПК	Экз
Тема 2. Обеспечение безопасности информационных технологий	З-1, У-1, У-3	Показывает знание организационной структуры системы обеспечения безопасности информационных технологий (ИТ). Показывает знание обязанностей пользователей и ответственных за обеспечение безопасности ИТ. Знает и умеет использовать документы, регламентирующие правила парольной и	Таблица 1, таблица 2.	УК, ПК	Экз

		антивирусной защиты.			
Тема 3. Средства защиты информации от несанкционированного доступа	З-1, У-1, У-3	Демонстрирует знание назначения и возможности средств защиты информации и умение использовать эти средства. Может дать квалифицированные рекомендации по выбору средств защиты информации от несанкционированного доступа.	Таблица 1, таблица 2.	УК, ПК	Экз
Тема 4. Обеспечение безопасности компьютерных систем и сетей	З-1, У-1, У-3, В-1	Показывает знание проблем обеспечения в компьютерных сетях и системах. Знает назначение, возможности и защитные механизмы межсетевых экранов. Владеет особенностями анализа содержимого почтового и WEB – трафика. Владеет способами обнаружения и устранения уязвимостей.	Таблица 1, таблица 2.	УК, ПК	Экз
Тема 5. Основы информационной безопасности	З-1	Показывает знание места информационной безопасности в системе национальной безопасности. Знает основные составляющие национальных интересов РФ в информационной сфере. Знает виды и источники угроз информационной безопасности РФ.	Таблица 1, таблица 2.	УК, ПК	Экз
Тема 6. Комплексная система защиты информации	З-1, У-1, У-3, В-1	Знать общую характеристику комплексной защиты информации. Уметь использовать системы физической защиты. Знать о подсистемах инженерной защиты. Владеть способами и средствами обнаружения угроз	Таблица 1, таблица 2.	УК, ПК	Экз
Тема 7. Инженерно-техническая защита информации	З-1, У-1, У-3, В-1	Показывает знания основ инженерно-технической защиты информации. Владеет понятием несанкционированного	Таблица 1, таблица 2.	УК, ПК	Экз

		доступа к защищаемой информации. Знает технические каналы утечки информации.			
Тема 8. Криптографическая защита информации	З-1, У-1, У-3, В-1	Знает основы криптографии. Знает и умеет использовать симметрические криптосистемы, криптосистемы с открытым ключом. Уметь использовать системы электронной подписи. Владеть криптоанализом.	Таблица 1, таблица 2.	УК, ПК	Экз

УК – устный контроль, ПК – письменный контроль, Экз - экзамен

Оценочные средства для проведения 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.

Таблица 1. Параметры оценочного средства для промежуточной аттестации

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 норм литературного языка	Соблюдает нормы литературного языка, преобладает научный стиль изложения **(3-4 балла)**	Соблюдает нормы литературного языка, допускает единичные ошибки **(2- 3 балла)**	Допускает множественные речевые ошибки при изложении материала **(1-2 балл)**	Косноязычная речь 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.

Оценочные средства для оценки текущей успеваемости студентов

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).

Таблица 2. 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.

1. Характеристика ОС для обеспечения текущего контроля по дисциплине

Раздел/ Тема*	Индекс и уровень формируемой компетенции или дескриптора	ОС	Содержание задания
Пз.1. Т1.	Изучение программы «РЕВИЗОР -1 XP»	ПК, УК	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. Т2.	Изучение программы «СТРАЖ NT»	ПК, УК	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. Т2.	Изучение программы «СТРАЖ NT»	ПК, УК	Инструкция по организации парольной защиты. Инструкция по организации антивирусной защиты.
Пз.4. Т3.	Изучение программы «Гроза-К», «Ревизор-2XP»	ПК, УК	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 Т4.		ПК, УК	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 крипто шлюза «Континент-К». Назначение и особенности работы программы «СТРАЖ NT».
Пз. 5 Т4.	Изучение программы «SecretNET»	ПК, УК	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 Т5.	Изучение аппаратуры «NR-900EMS», «Аврора-3», «Крона-ПРО».	ПК, УК	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 Т6.	Изучение аппаратуры «Соната-Р2»	ПК, УК	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 Т7	Изучение системы «Талис-нч –лайт»	ПК, УК	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 Т8	Изучение аппаратуры «Ладья-ИВТ», «Кедр-1М»	ПК, УК	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 Т8		ПК, УК	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».

ПК – письменный контроль, УК – устный контроль

2. Оценочные средства, обеспечивающие диагностику сформированности компетенций, заявленных в рабочей программе дисциплины (модуля)

Результат диагностики сформированности компетенций ОК-1, ОПК-4	Показатели	Критерии	Соответствие/ несоответствие	Зачет
ОК-1 Знать: 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.	Показывает знания использования основные понятий в области безопасности информационных технологий. Демонстрирует знания об угрозах информационной безопасности. Показывает знание принципов обеспечения безопасности. Показывает знание организационной структуры системы обеспечения безопасности информационных технологий (ИТ). Показывает знание обязанностей пользователей и ответственных за обеспечение безопасности ИТ. Знает как использовать документы, регламентирующие правила парольной и антивирусной защиты. Демонстрирует знание назначения и возможности средств защиты информации. Может дать квалифицированные рекомендации по выбору средств защиты информации от несанкционированного доступа. Показывает знание проблем обеспечения в компьютерных сетях и системах. Знает назначение, возможности и защитные механизмы межсетевых экранов, умеет их использовать. Показывает знание места информационной безопасности в системе национальной безопасности. Знает основные составляющие национальных интересов РФ в информационной сфере. Знает виды и источники угроз информационной безопасности РФ. Знает общую характеристику комплексной защиты информации. Знает о подсистемах инженерной защиты. Показывает знания основ инженерно-технической защиты информации. Знает технические каналы утечки информации. Знает основы криптографии. Знает и умеет использовать симметрические криптосистемы, криптосистемы с открытым ключом.	Таблица 1, таблица 2.		
ОК-1. Уметь: 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.	Показывает умение использовать основные понятий в области безопасности информационных технологий. Умеет использовать документы, регламентирующие правила парольной и антивирусной защиты. Показывает умение использовать средства защиты информации. Умеет использовать системы физической защиты. Умеет использовать системы электронной подписи.	Таблица 1, таблица 2.		
ОПК-4. Уметь: использовать современные компьютерные сети,	Умеет использовать современные информационные ресурсы для поиска информации в сфере оценки безопасности информационных систем, для	Таблица 1, таблица 2.		

программные продукты и ресурсы информационно-телекоммуникационной сети «Интернет» для изучения экспертных систем комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем.	дополнительной проработки лекционных вопросов и тем практических занятий.			
ОК-1. Владеть: методами поиска решений в экспертных системах; навыками проектирования экспертных систем и эксплуатации современных интеллектуальных систем в области информационной безопасности.	Владеет особенностями анализа содержимого почтового и WEB – трафика. Владеет способами обнаружения и устранения уязвимостей. Владеет способами и средствами обнаружения угроз. Владеет понятием несанкционированного доступа к защищаемой информации. Владеет криптоанализом.	Таблица 1, таблица 2.		