ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА»

Кафедра «Информационная безопасность»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине

Б1.В.07 «Модели угроз и нарушителей безопасности информации объектов информатизации»

Направление подготовки – 10.05.00 «Информационная безопасность»

Специальность: 10.05.03 Информационная безопасность автоматизированных систем

Специализация: № 8 «Разработка автоматизированных систем в защищенном исполнении»

Квалификация выпускника – специалист

Форма обучения - очная

Рязань 2025 г.

1 ОБЩИЕ ПОЛОЖЕНИЯ

Оценочные материалы – это совокупность учебно-методических материалов (контрольных заданий, описаний форм и процедур), предназначенных для оценки качества освоения обучающимися данной дисциплины как части основной профессиональной образовательной программы.

Цель – оценить соответствие знаний, умений и уровня приобретенных компетенций, обучающихся целям и требованиям основной профессиональной образовательной программы в ходе проведения текущего контроля и промежуточной аттестации.

Основная задача – обеспечить оценку уровня сформированности общекультурных, общепрофессиональных и профессиональных компетенций, приобретаемых обучающимся в соответствии с этими требованиями.

Контроль знаний проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль успеваемости проводится с целью определения степени усвоения учебного материала, своевременного выявления и устранения недостатков в подготовке обучающихся и принятия необходимых мер по совершенствованию методики преподавания учебной дисциплины (модуля), организации работы обучающихся в ходе учебных занятий и оказания им индивидуальной помощи.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков, приобретенных обучающимися в ходе выполнения индивидуальных заданий на практических занятиях и лабораторных работах. При оценивании результатов освоения практических занятий и применяется шкала оценки «зачтено – не зачтено». Количество практических работ и их тематика определена рабочей программой дисциплины.

Результат выполнения каждого индивидуального задания должен соответствовать всем критериям оценки в соответствии с компетенциями, установленными для заданного раздела дисциплины.

Промежуточный контроль по дисциплине осуществляется проведением теоретического зачета с оценкой.

2 ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Сформированность каждой компетенции (или ее части) в рамках освоения данной дисциплины оценивается по трехуровневой шкале:

1) пороговый уровень является обязательным для всех обучающихся по завершении освоения дисциплины;

2) продвинутый уровень характеризуется превышением минимальных характеристик сформированности компетенций по завершении освоения дисциплины;

3) эталонный уровень характеризуется максимально возможной выраженностью компетенций и является важным качественным ориентиром для самосовершенствования.

Уровень освоения компетенций, формируемых дисциплиной:

Описание критериев и шкалы оценивания тестирования:

Шкала оценивания	Критерий
3 балла (эталонный уровень)	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 85 до 100%
2 балла (продвинутый уровень)	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 70 до 84%
1 балл (пороговый уровень)	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 50 до 69%
0 баллов	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 0 до 49%

Описание критериев и шкалы оценивания теоретического вопроса:

Шкала оценивания	Критерий
3 балла (эталонный уровень)	выставляется студенту, который дал полный ответ на вопрос, показал глубокие систематизированные знания, смог привести примеры, ответил на дополнительные вопросы преподавателя
2 балла (продвинутый уровень)	выставляется студенту, который дал полный ответ на вопрос, но на некоторые дополнительные вопросы преподавателя ответил только с помощью наводящих вопросов
1 балл (пороговый уровень)	выставляется студенту, который дал неполный ответ на вопрос в билете и смог ответить на дополнительные вопросы только с помощью преподавателя
0 баллов	выставляется студенту, который не смог ответить на вопрос

Описание критериев и шкалы оценивания практического задания:

Шкала оценивания	Критерий
3 балла (эталонный уровень)	Задача решена верно
2 балла (продвинутый уровень)	Задача решена верно, но имеются неточности в логике решения
1 балл (пороговый уровень)	Задача решена верно, с дополнительными наводящими вопросами преподавателя
0 баллов	Задача не решена

На промежуточную аттестацию (зачет с оценкой) выносится тест (10 вопросов), два теоретических вопроса и 2 задачи. Максимально студент может набрать 15 баллов. Итоговый суммарный балл студента, полученный при прохождении промежуточной аттестации, переводится в традиционную форму по системе «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

Оценка «отлично» выставляется студенту, который набрал в сумме 15 баллов (выполнил все задания на эталонном уровне). Обязательным условием является выполнение всех предусмотренных в течение семестра практических заданий.

Оценка «хорошо» выставляется студенту, который набрал в сумме от 10 до 14 баллов при условии выполнения всех заданий на уровне не ниже продвинутого. Обязательным условием является выполнение всех предусмотренных в течение семестра практических заданий.

Оценка «удовлетворительно» выставляется студенту, который набрал в сумме от 5 до 9 баллов при условии выполнения всех заданий на уровне не ниже порогового. Обязательным условием является выполнение всех предусмотренных в течение семестра практических заданий.

Оценка «неудовлетворительно» выставляется студенту, который набрал в сумме менее 5 баллов или не выполнил всех предусмотренных в течение семестра практических заданий.

3 ПАСПОРТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО ДИСЦИПЛИНЕ

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или её части)/ индикатора	Вид, метод, форма оценочного мероприятия
1	Описание информационной системы и особенностей ее функционирования.	ПК-4 (ПК-4.2, ПК-4.3, ПК-5.1, ПК-5.2)	зачет с оценкой
2	Цель и задачи, решаемые информационной системой.	ПК-4 (ПК-4.2, ПК-4.3, ПК-5.1, ПК-5.2)	зачет с оценкой
3	Описание структурно-функциональных характеристик информационной системы.	ПК-4 (ПК-4.2, ПК-4.3, ПК-5.1, ПК-5.2)	зачет с оценкой
4	Описание технологии обработки информации.	ПК-4 (ПК-4.2, ПК-4.3, ПК-5.1, ПК-5.2)	зачет с оценкой
5	Возможности нарушителей(модель нарушителя).	ПК-4 (ПК-4.2, ПК-4.3, ПК-5.1, ПК-5.2)	зачет с оценкой
6	Типы и виды нарушителей.	ПК-4 (ПК-4.2, ПК-4.3, ПК-5.1, ПК-5.2)	зачет с оценкой
7	Возможные цели и потенциал нарушителей.	ПК-4 (ПК-4.2, ПК-4.3, ПК-5.1, ПК-5.2)	зачет с оценкой
8	Классификация угроз информационной безопасности объектов информатизации.	ПК-4 (ПК-4.2, ПК-4.3, ПК-5.1, ПК-5.2)	зачет с оценкой
9	Возможные способы реализации угроз безопасности информации.	ПК-4 (ПК-4.2, ПК-4.3, ПК-5.1, ПК-5.2)	зачет с оценкой
10	Актуальные угрозы безопасности информации.	ПК-4 (ПК-4.2, ПК-4.3, ПК-5.1, ПК-5.2)	зачет с оценкой
11	Модели угроз и способы оценки рисков реализации угроз информационной безопасности.	ПК-4 (ПК-4.2, ПК-4.3, ПК-5.1, ПК-5.2)	Зачет с оценкой

4 ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ

4.1. Промежуточная аттестация в форме зачета с оценкой

Код компетенции/ индикаторов	Результаты освоения ОПОП Содержание компетенций/индикаторов
ПК-4 (ПК-4.2, ПК-4.3)	Способен разрабатывать системы защиты информации автоматизированных систем. ПК-4.2 Разрабатывает требования по защите, формирует политики безопасности компьютерных систем и сетей ПК-4.3 Проводит анализ безопасности компьютерных систем

Типовые тестовые вопросы:

1. В настоящее время наиболее широко распространены системы управления базами данных
а) иерархические
+ б) реляционные
в) сетевые
г) объектно-ориентированные

2. СУБД Oracle, Informix, Subase, DB 2, MS SQL Server относятся к
а) сетевым
б) иерархическим
+ г) реляционным
д) объектно-ориентированным

3. Традиционным методом организации информационных систем является
+ а) архитектура клиент-сервер
б) архитектура клиент-клиент
в) архитектура сервер-сервер
г) размещение всей информации на одном компьютере

4. Жизненный цикл ИС регламентирует стандарт ISO/IEC 12207. IEC – это
а) международная организация по стандартизации
+ б) международная комиссия по электротехнике
в) международная организация по информационным системам
г) международная организация по программному обеспечению

5. Согласно ISO 12207, объединение одного или нескольких процессов, аппаратных средств, программного обеспечения, оборудования и людей для удовлетворения определённым потребностям или целям это
а) полнофункциональный программно-аппаратный комплекс
б) информационная система
+ в) система
г) вычислительный центр

6. Какое определение информационных ресурсов общества соответствует Федеральному закону " Об информации, информатизации и защите информации"
+ а) Информационные ресурсы общества – это отдельные документы и отдельные массивы документов, документы и массивы в информационных системах (библиотеках, архивах, фондах, банках данных и других системах), созданные, приобретенные за счет средств федерального бюджета, бюджетов субъектов РФ.
б) Информационные ресурсы общества – это сведения различного характера, материализованные в виде документов, баз данных и баз знаний.
в) Информационные ресурсы общества – это множество web-сайтов, доступных в Интернете.

7. Какой информационной системе соответствует следующее определение: программно-аппаратный комплекс, способный объединять в одно целое предприятия с различной функциональной направленностью (производственные, торговые, кредитные и др. организации)
а) Информационная система промышленного предприятия.
б) Информационная система торгового предприятия.
+ в) Корпоративная информационная система.
г) Информационная система кредитного учреждения.

8. Открытая информационная система это
+ а) Система, созданная на основе международных стандартов.
б) Система, включающая в себя большое количество программных продуктов.
в) Система, ориентированная на оперативную обработку данных.
г) Система, включающая в себя различные информационные сети.

9. Информационные модели предназначены для
+ а) отражения информационных потоков между объектами и
отношений между ними
б) математического отражения структуры явлений;
в) отражения качественных характеристик процессов.
г) содержательного отражения отношений между объектами;

10. Укажите информационные модели, разработка которых регламентируется соглашениями, принятыми в практике создания информационных систем
а) Сетевые модели.
б) Иерархические модели.
+ в) Диаграммы потоков данных.
г) Реляционные модели.

11. При полномочной политике безопасности совокупность меток с одинаковыми значениями образует:
+а) уровень безопасности
б) область равного доступа
в) область равной критичности
г) уровень доступности

12. Конкретизацией модели Белла-ЛаПадула является модель политики безопасности
+ а) LWM
б) на основе угроз
в) Лендвера
г) с полным перекрытием

13. Недостатком модели конечных состояний политики безопасности является
а) изменение линий связи
б) статичность
+ в) сложность реализации
г) низкая степень надёжности

14. «При избирательной политике безопасности в матрице доступа на пересечении столбца и строки указывается
а) субъект системы
+ б) тип разрешенного доступа
в) факт доступа
г) объект системы

15. Основу политики безопасности составляет
+ а) способ управления доступом
б) управление риском
в) программное обеспечение
г) выбор каналов связи

16. Недостатком дискретных моделей политики безопасности является

а) изначальное допущение вскрываемости системы
б) необходимость дополнительного обучения персонала
в) сложный механизм реализации
+ г) статичность

17. Модели политики безопасности на основе анализа угроз системе исследуют вероятность преодоления системы защиты
а) ограничение компетенцией злоумышленника
+ б) за определенное время
в) фиксированными затратами
г) фиксированным ресурсом

18. Организационные требования к системе защиты
а) управленческие и идентификационные
б) административные и аппаратурные
+ в) административные и процедурные
г) аппаратурные и физические

19. Политика информационной безопасности - это
а) профиль защиты
б) итоговый документ анализа рисков
в) стандарт безопасности
+ г) совокупность законов, правил, определяющих управленческие и проектные решения в области защиты информации

20. Из перечисленного: 1) идентификация и аутентификация; 2) регистрация и учет; 3) непрерывность защиты; 4) политика безопасности — согласно «Оранжевой книге» требованиями в области аудита являются
+ а) 1,2
б) 3,4
в) 2,4
г) 1,3

Типовые практические задания:

Задание 1

Разработать описание заданной информационной системы и особенностей ее функционирования.

Критерий выполнения задания 1

Задание считается выполненным, если обучаемый выполнил описание системы в соответствии с методическими документами.

Задание 2

Разработать описание структурно-функциональных характеристик заданной информационной системы.

Критерий выполнения задания 2

Задание считается выполненным, если обучаемый выполнил описание структуры и функций системы системы в соответствии с методическими документами.

Задание 3

Разработать классификацию угроз безопасности информации заданной системы.

Критерий выполнения задания 3

Задание считается выполненным, если обучаемый выполнил классификацию угроз в соответствии с методическими документами.

Задание 4

Разработать описание типов и видов нарушителей заданной системы.

Критерий выполнения задания 4

Задание считается выполненным, если обучаемый выполнил описание типов и видов нарушителей в соответствии с методическими документами.

Код компетенции/ индикаторов	Результаты освоения ОПОП Содержание компетенций/индикаторов
ПК-5 (ПК-5.1, ПК-5.2)	Способен разрабатывать системы защиты информации автоматизированных систем ПК-5.1 Обосновывает необходимость защиты информации в автоматизированной системе ПК-5.2 Определяет угрозы безопасности информации, обрабатываемой автоматизированной системой

Типовые тестовые вопросы:

1. Что понимается под понятием «Контролируемая зона»?

а) Пространство, в котором не исключается неконтролируемое пребывание сотрудников и посетителей оператора, но исключается неконтролируемое пребывание посторонних транспортных, технических и иных материальных средств

+ б) Пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств

в) Пространство, в котором не исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств

2. Кто является основным ответственным за определение уровня классификации информации?

а) руководитель среднего звена

б) высшее руководство

+ в) владелец

г) пользователь

3. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

а) хакеры

+ б) сотрудники

в) атакующие

г) контрагенты(лица, работающие по договору)

4. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования

+ б) Улучшить контроль за безопасностью этой информации

в) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

г) Снизить уровень классификации этой информации

5. Что самое главное должно продумать руководство при классификации данных?

+ а) Необходимый уровень доступности, целостности и конфиденциальности

б) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

в) Оценить уровень риска и отменить контрмеры
г) Управление доступом, которое должно защищать данные

6. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
+ б) Когда стоимость контрмер превышает ценность актива и потенциальные потери
в) Когда риски не могут быть приняты во внимание по политическим соображениям
г) Когда необходимые защитные меры слишком сложны

7. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?
а) Только военные имеют настоящую безопасность
б) Военным требуется больший уровень безопасности, т.к. их риски существенно выше
+ в) Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
г) Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

8. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
а) Чтобы убедиться, что проводится справедливая оценка
б) Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
в) Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку
+ г) Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа

9. Что представляет собой стандарт ISO/IEC 27799?
а) Новая версия BS 17799
+ б) Стандарт по защите персональных данных о здоровье
в) Определения для новой серии ISO 27000
г) Новая версия NIST 800-60

10. Защита информации от утечки это деятельность по предотвращению:
а) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
б) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
в) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
+ г) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

11 . Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это
а) уязвимость информации
б) надежность информации
г) защищенность информации
+ д) безопасность информации

12. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это

а) аудит
+ б) аутентификация
в) авторизация
г) идентификация

13. Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется
а) системой защиты
б) стандартом безопасности
в) профилем безопасности
+ г) профилем защиты

14. Получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля называется
+ а) мониторингом
б) аудитом
в) управлением ресурсами
г) администрированием

15. Преднамеренной угрозой безопасности информации является
+ а) несанкционированное копирование конфиденциальной информации
б) наводнение
в) повреждение кабеля, по которому идет передача, в связи с погодными условиями
г) ошибка администратора

16. Непреднамеренной угрозой безопасности информации является
+ а) повреждение кабеля, по которому идет передача, в связи с погодными условиями
б) кража
в) умышленная порча носителей информации
г) несанкционированное копирование конфиденциальной информации

17. Типовая архитектура системы обнаружения атак включает в себя
а) система специального реагирования на обнаруженные атаки
+б) модули-датчики, предназначенные для сбора необходимой информации о функционировании ИС
в) все модули, не выполняющие функции управления компонентами системы обнаружения атак.
г) база данных, содержащая информацию о пользователях системы

18. Согласно "Рекомендациям по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения" под технической защитой информации понимается:
+ а) деятельность, направленная на обеспечение некриптографическими методами безопасности информации (данных), подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств
б) состояние защищенности объекта информатизации, при котором обеспечивается безопасность информации и автоматизированных средств ее обработки
в) состояние защищенности информации [данных], при котором обеспечиваются ее [их] конфиденциальность, доступность и целостность
г) состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право

19. Что входит в содержание раздела «Защита информации ограниченного доступа» структуры документов по защите информации:
+ а) перечень мероприятий, направленных на защиту информации ограниченного доступа в организации;
б) краткий перечень защищаемых в организации видов информации ограниченного доступа (все имеющиеся виды информации конфиденциального характера)

в) перечень информации, которая не может быть отнесена в организации к информации ограниченного доступа
г) порядок отнесения в организации информации к информации ограниченного доступа

20. Дайте определение понятия «топология сети»
+а) Описание конфигурации сети, схема расположения и соединения сетевых устройств.
б) Схема расположения компьютеров в сети.
в) Схема взаимодействия коммутирующего оборудования.
г) Технология обеспечения безопасности сети.

Типовые практические задания:

Задание 5
Выполнить описание возможных целей и потенциала нарушителей для заданной системы.

Критерий выполнения задания 5
Задание считается выполненным, если обучаемый выполнил описание возможных целей и потенциала нарушителей с методическими документами.

Задание 6
Выполнить описание возможных способов реализации угроз безопасности информации для заданной системы.

Критерий выполнения задания 6
Задание считается выполненным, если обучаемый выполнил возможных способов реализации угроз безопасности информации в соответствии с методическими документами.

Задание 7
Определенить уровень исходной защищенности заданной автоматизированной системы.

Критерий выполнения задания 7
Задание считается выполненным, если обучаемый определил уровень исходной защищенности автоматизированной системы в соответствии с методическими документами.

Задание 8
Определить вероятность реализации угроз безопасности информации для заданной системы.

Критерий выполнения задания 8
Задание считается выполненным, если обучаемый определил вероятность реализации угроз безопасности информации в соответствии с методическими документами.

Типовые теоретические вопросы:

1. Какие средства защиты информации применяются на компьютерах в ИСПДн и ГИС любых уровней и классов, как подключенных, так и не подключенных к сетям общего пользования с целью идентификации и аутентификации субъектов и объектов доступа, разделения полномочий пользователей и администраторов, защиты информации о событиях безопасности и других функций?
2. В случае поступления запросов на получение информации из организаций, не обладающих соответствующими полномочиями что обязан сделать работодатель?

3. Сколько существует уровней защищенности, которые необходимо обеспечить персональным данным в соответствии с постановлением Правительства №1119? Назовите их.

4. Правовое регулирование отношений по защите информации в информационных и телекоммуникационных сетях, а также в сети Интернет.

5. Классификация объектов информатизации.

6. Правовой порядок установления соответствия параметров объектов информатизации и средств защиты информации требованиям нормативных документов.

7. Модели компьютерных систем. Доступ и монитор безопасности.

8. Классы безопасности.

9. Политики разграничения доступа.

10. Какова цель защиты корпоративной информационной системы?

11. Назовите защитные механизмы. Как их можно классифицировать?

12. Перечислите основные классификационные схемы уязвимостей. Каковы их основные достоинства и недостатки.

4.2. Задания курсовой работы

Для заданного варианта задания на курсовую работу необходимо разработать модель угроз информационной безопасности.

Темы курсовой работы

1. Разработка модели актуальных угроз автоматизированной системы компании по доставке почтовых отправлений.
2. Разработка модели актуальных угроз автоматизированной системы ломбарда бытовой и электронной техники.
3. Разработка модели актуальных угроз автоматизированной системы конторы по продаже недвижимости.
4. Разработка модели актуальных угроз безопасности информации автоматизированной системы информационно-образовательного центра.
5. Разработка модели актуальных угроз автоматизированной системы бухгалтерии предприятия.
6. Разработка модели актуальных угроз автоматизированной системы кредитного отдела коммерческого банка.
7. Разработка модели актуальных угроз автоматизированной системы отдела кадров предприятия.
8. Разработка модели актуальных угроз автоматизированной системы поликлиники.
9. Разработка модели актуальных угроз автоматизированной системы автосалона.
10. Разработка модели актуальных угроз автоматизированной системы Интернет магазина.
11. Разработка модели актуальных угроз автоматизированной системы мобильного оператора.
12. Разработка модели актуальных угроз автоматизированной системы охранного предприятия.
13. Разработка модели актуальных угроз автоматизированной системы управления производством предприятия.
14. Разработка модели актуальных угроз автоматизированной системы сети розничных магазинов.
15. Разработка модели актуальных угроз автоматизированной системы приема коммунальных платежей.
16. Разработка модели актуальных угроз автоматизированной системы архивных данных.

Критерии выполнения курсовой работы

Результаты курсового проектирования оцениваются с учетом:

1) качества и полноты выполнения пояснительной записки;
2) наличия работающей программы;
3) уровня ответов студента.

Программу составил
к.т.н., доцент кафедры
«Информационная безопасность» Ю.В. Конкин