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.08 Разработка безопасного программного обеспечения компьютерных систем

Специальность – 10.05.01 «Компьютерная безопасность»
Специализация №5 «"Разработка систем защиты информации компьютерных систем объектов информатизации" (по отрасли или в сфере профессиональной деятельности)»

Квалификация выпускника - специалист по защите информации

Форма обучения - очная

Рязань 2023 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.

В качестве оценочных средств на протяжении семестра используется устные и письменные ответы студентов на индивидуальные вопросы, письменное тестирование по теоретическим разделам курса. Дополнительным средством оценки знаний и умений студентов является отчет о выполнении практических заданий и их защита. Результат выполнения каждого индивидуального задания должен соответствовать всем критериям оценки в соответствии с компетенциями, установленными для заданного раздела дисциплины.

По итогам курса обучающиеся сдают зачет с оценкой и выполняют курсовую работу. Форма проведения зачета – устный ответ с письменным подкреплением по утвержденным билетам, сформулированным с учетом содержания дисциплины. В билет для зачета включается два теоретических вопроса и задача. В процессе подготовки к устному ответу студент должен составить в письменном виде план ответа.

2 ПАСПОРТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО ДИСЦИПЛИНЕ

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или её части)	Вид, метод, форма оценочного мероприятия
1	1. Введение в дисциплину.	ПК 3.2	зачет с оценкой
2	2. Базовая терминология безопасной разработки ПО. Дефекты ПО, уязвимости ПО и НДВ ПО.	ПК 3.2	зачет с оценкой
3	3. Угрозы безопасности информации при разработке ПО	ПК 3.2	зачет с оценкой
4	4. Организационные и технические меры по разработке безопасного ПО, реализуемых на различных стадиях жизненного цикла разработки безопасного ПО	ПК 3.2	зачет с оценкой
5	5. Выявление уязвимостей и НДВ в ПО	ПК 3.2	зачет с оценкой
6	6. Методы анализа ПО	ПК 3.2	зачет с оценкой
7	7. Управление рисками информационной безопасности при разработке ПО	ПК 3.2	зачет с оценкой

3 ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ С УКАЗАНИЕМ ЭТАПРВ ИХ ФОРМИРОВАНИЯ

При освоении дисциплины формируются следующие компетенции: ПК 3.2.

Указанные компетенции формируются в соответствии со следующими этапами:

– формирование и развитие теоретических знаний, предусмотренных указанными компетенциями (лекционные занятия, самостоятельная работа студентов);

– приобретение и развитие практических умений предусмотренных компетенциями (практические занятия, самостоятельная работа студентов);

– закрепление теоретических знаний, умений и практических навыков, предусмотренных компетенциями, в ходе решения конкретных задач на занятиях, выполнения индивидуальных заданий на практических занятиях и их защиты, а так же в процессе сдачи зачета.

4 ПОКАЗАТЕЛИ И КРИТЕРИИ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ (РЕЗУЛЬТАТОВ) НА НАЗЛИЧНЫХ ЭТАПАХ ИХ ФОРМИРОВАНИЯ, ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

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

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

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

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

Принимается во внимание наличие и степень сформированности у обучающихся знаний, умений и обладание навыками, которые должны были формироваться в процессе изучения дисциплины.

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), теоретический вопрос и практическое задание. Максимально студент может набрать 9 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 9 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 6 до 8 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 3 до 4 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 3 баллов или не выполнил всех предусмотренных в течение семестра практических заданий.

5 ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ

5.1. Промежуточная аттестация в форме зачета с оценкой

Код компетенции	Результаты освоения ОПОП Содержание компетенций
ПК 3.2	Проводит анализ безопасности компьютерных систем

Типовые тестовые вопросы:

1. Безопасное программное обеспечение это:
+а) программное обеспечение, разработанное с использованием совокупности мер, направленных на предотвращение появления и устранение уязвимостей;
б) программное обеспечение, прошедшее функциональное тестирование;
в) объектно-ориентированное программное обеспечение;
г) программное обеспечение на языках Java и C#.

2. Методология SDL нацелена на:
Ответ:

(1) упрощение процесса нейтрализации выявляемых уязвимостей
(2) (+) повышение уровня безопасности разрабатываемого ПО
(3) ускорение сбора информации о вновь выявляемых уязвимостях

3. Д**инамический анализ кода программы это:**
+а) анализ кода программы в режиме непосредственного исполнения;
б) анализ условных переходов в программе;
в) анализ быстродействия программы;
г) анализ потоков программы.
4. И**нструментальное средство это:**
+а) компьютерная программа, используемая как средство разработки;
б) средство защиты информации;
в) описание процедур настройки и инсталляции;
г) средство анализа параметров сетевого трафика.

5. Т**естирование на проникновение это:**
+а) вид работ по выявлению уязвимостей программы, основанный на моделировании действий потенциального нарушителя;
б) тестирование программы на различных наборах входных данных;
в) вид нагрузочного тестирования;
г) сканирование уязвимостей.

6. У**гроза безопасности информации это:**
+а) совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;
б) использование несертифицированных средств защиты информации;
в) использование устаревших версий программного обеспечения;

7. Уязвимость программы это:
+а) недостаток программы, который может быть использован для реализации угроз безопасности информации;
б) недостаточное быстродействие программы;
в) динамическое выделение программой оперативной памяти;
г) большое количество входных параметров.

8. К**омпьютерная атака это:**
+а) целенаправленное несанкционированное воздействие на ресурс АСЗИ;
б) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств АСЗИ;
в) **с**овокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации АСЗИ.

9. С**етевая атака это:**
+а) компьютерная атака с использованием протоколов межсетевого взаимодействия;
б) попытка воздействия на веб-приложение;
в) попытка воздействия на клиент-серверное приложение;
г)попытка воздействия на серверную операционную систему.

10. С**татический анализ исходного кода программы это:**
+а) вид работ по инструментальному исследованию программы в режиме, не предусматривающем реального выполнения кода;
б) этап компиляции программы;
в) оптимизация исходного кода программы с целью повышения быстродействия;

11. Фаззинг-тестирование программы это:
+а) вид работ по исследованию программы, основанный на передаче программе случайных или специально сформированных входных данных, отличных от данных, предусмотренных алгоритмом работы программы;
б) выявление недекларированных возможностей;
в) проверка функций программы на соответствие техническому заданию;
г) вид нагрузочного тестирования.

12. Информационная система это:
+а) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
б) программная система, имеющая средства визуализации результатов;
в) программная система клиент-серверной архитектуры.

13. Б**езопасность информации это:**
+а) состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность;
б) обработка информации только сертифицированным программным обеспечением;
в) состояние информации при котором исключен несанкционированный доступ.

14. Защита информации это:
а) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
б) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
в) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
+ г) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

16. Естественные угрозы безопасности информации вызваны:
а) деятельностью человека;
б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
+ в) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
г) корыстными устремлениями злоумышленников;

17. Искусственные угрозы безопасности информации вызваны:
+ а) деятельностью человека;
б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
в) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
г) корыстными устремлениями злоумышленников;

18. Конфиденциальность - это:
а) защита от несанкционированного использования ресурсов сети.
+ б) предотвращение пассивных атак для передаваемых или хранимых данных;
в) защита от возможных отказов от фактов отправки, приема или содержания отправленных или принятых данных;
г) подтверждении подлинности взаимодействующих объектов;

19 Активные угрозы становятся видимыми на уровне (модели OSI):
а) физическом
б) канальном
в) сетевом
+ г) транспортном

20. Обозначение, семейства протоколов, охватывающих проблемы безопасности на IP-уровне:
а) FTP
+ б) Ipsec
в) TCP/IP
г) UDP

21. Информирование персонала предприятия об основных целях в сфере информационной безопасности осуществляется с помощью:
а) положения о департаменте информационной безопасности
+ б) политики безопасности
в) аудита безопасности

22. Все известные на настоящий момент меры защиты информации можно разделить на:
а) правовые
б) организационные и технические
в) правовые и технические
+ г) правовые, технические и организационные

---

23. В системах автоматизированного интерактивного анализа политик безопасности заключения о состоянии политики безопасности формируются на основе:
а) семантического анализа текстов политик безопасности
б) результатов аудита информационной безопасности
+ в) ответов на вопросы, задаваемые программой

24. Автоматизированный анализ управления информационной безопасностью предполагает:
а) загрузку политик безопасности в виде электронных документов
+ б) внесение данных в соответствии с вопросами, задаваемыми программой
в) внесение данных из журналов систем контроля безопасности

25. Автоматизированные системы анализа рисков используют данные о:
а) результатах аудита информационной безопасности
б) составе и объеме политики информационной безопасности
+ в) составе информационных активов

26. Обеспечение безопасности информации, в том числе и в компьютерных системах, требует сохранения следующих ее свойств:
а) целостности и доступности;
б) доступности и конфиденциальности;
+ в) конфиденциальности, доступности и целостности
г) достоверности, целостности и конфиденциальности

---

27. Все известные на настоящий момент меры защиты информации можно разделить на следующие виды:
а) правовые
б) организационные
в) технические
+ г) все из вышеперечисленных

---

27. 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

28. 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.

29. 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;

30. 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

31. 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)

32. 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

33. 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;

34. 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.

Типовые практические задания:

Задание 1

Разработать описание структурно-функциональных характеристик автоматизированной системы библиотеки университета.

Критерий выполнения задания 1

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

Задание 2

Разработать состав математического обеспечения АСЗИ бухгалтерии малого предприятия.

Критерии выполнения задания 2

Задание считается выполненным, если обучающийся в результате показал совокупность математических методов, моделей и алгоритмов, примененных в АСЗИ.

Задание 3

Разработать состав программного обеспечения АСЗИ бухгалтерии малого предприятия.

Критерии выполнения задания 3

Задание считается выполненным, если обучающийся в результате показал совокупность программ на носителях данных, программных документов, предназначенных для отладки, функционирования и проверки работоспособности АСЗИ.

Задание 4

Разработать состав информационного обеспечения АСЗИ бухгалтерии малого предприятия.

Критерии выполнения задания 4

Задание считается выполненным, если обучающийся в результате показал совокупность форм документов, классификаторов, нормативной базы, применяемой в АСЗИ при ее функционировании.

Задание 5

Разработать состав лингвистического обеспечения АСЗИ бухгалтерии малого предприятия.

Критерии выполнения задания 5

Задание считается выполненным, если обучающийся в результате показал совокупность средств и правил для формализации естественного языка, используемых при общении пользователей и эксплуатационного персонала автоматизированной системы с комплексом средств автоматизации при функционировании АСЗИ.

Задание 6

Выполнить классификацию угроз безопасности информации АСЗИ бухгалтерии малого предприятия.

Критерий выполнения задания 6

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

Задание 7

Выполнить описание возможных способов реализации угроз безопасности информации для АСЗИ бухгалтерии малого предприятия.

Критерий выполнения задания 7

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

Задание 8

Выполнить описание основных нормативных документов по созданию безопасного ПО.

Критерий выполнения задания 8

Задание считается выполненным, если обучаемый указал основные нормативные документы по созданию безопасного ПО, их область применения и основные положения.

Задание 9

Выполнить описание мер по разработке безопасного ПО.

Критерий выполнения задания 9

Задание считается выполненным, если обучаемый указал основные меры по разработке безопасного ПО на основе нормативных документов.

Задание 10

Выполнить классификацию уязвимостей АСЗИ бухгалтерии малого предприятия.

Критерий выполнения задания 10

Задание считается выполненным, если обучаемый провел классификацию на основе ГОСТ Р 56546-2015 Классификация уязвимостей информационных систем.

Задание 11

Выполнить описание *о*бщих требований к инструментальным средствам разработки программного и информационного обеспечения.

Критерий выполнения задания 11

Задание считается выполненным, если обучаемый указал основные положения нормативных документов по использованию инструментальных средств в АСЗИ.

Типовые теоретические вопросы:

1. Основные термины и определения.

2. Порядок организации разработки видов АСЗИ.

3. Общие требования к технологической безопасности математического, программного, информационного, лингвистического обеспечения.

4. Инструментальные среды и средства разработки и анализа ПО.

5. ГОСТ 34.000-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

6. ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения.

7. ГОСТ Р 56546-2015 Классификация уязвимостей информационных систем.

8. ГОСТ Р 58412-2019 Защита информации. Разработка безопасного ПО. Угрозы безопасности информации при разработке ПО.

9. ГОСТ Р ИСО/МЭК 18045-2013 Методология оценки безопасности информационных технологий.

10. ГОСТ Р ИСО-МЭК 27034-1 Информационные технологии. Безопасность приложений. Часть 1. Безопасность приложений.

11. ГОСТ Р ИСО-МЭК 27034-7-2020 Информационные технологии. Безопасность приложений. Часть 7. Основы прогнозирования доверия.

12. Угрозы безопасности информации при разработке ПО (по ГОСТ Р 58412-2019).

13. Классификация уязвимостей информационных систем (по ГОСТ Р 56546—2015).

14. Выявление угроз безопасности информации при разработке ПО.

15. Оценка уровня доверия безопасности ПО (степени соответствия выявленной безопасности ПО предъявленным требованиям) (по ГОСТ Р ИСО-МЭК 27034-7).

16. Методы и средства оценки рисков информационной безопасности при создании ПО.

17. Общие требования к разработке математического обеспечения АСЗИ.

18. Общие требования к разработке программного обеспечения АСЗИ.

19. Общие требования к разработке информационного обеспечения АСЗИ.

20. Общие требования к разработке лингвистического обеспечения АСЗИ.

21. Общие требования к инструментальным средствам разработки программного и информационного обеспечения.

22. Требования по обеспечению информационной безопасности стенда для разработки программного и информационного обеспечения.

23. Требования к программно-методической документации в части информационной безопасности.

24. Меры по разработке безопасного ПО, реализуемые при выполнении анализа требований к ПО.

25. Меры по разработке безопасного ПО, реализуемые при выполнении проектирования архитектуры ПО.

26. Меры по разработке безопасного ПО, реализуемые при выполнении конструирования и комплексирования ПО.

27. Меры по разработке безопасного ПО, реализуемые при выполнении квалификационного тестирования ПО.

28. Меры по разработке безопасного ПО, реализуемые при выполнении инсталляции ПО и поддержки приемки ПО.

29. Меры по разработке безопасного ПО, реализуемые при решении проблем в программном обеспечении в процессе эксплуатации.

30. Меры по разработке безопасного ПО, реализуемые в процессе менеджмента документацией и конфигурацией программы.

31. Меры по разработке безопасного ПО, реализуемые в процессе менеджмента инфраструктурой среды разработки ПО.

32. Меры по разработке безопасного ПО, реализуемые в процессе менеджмента людскими ресурсами.
33. Виды тестирования ПО.
34. Статический анализ ПО.
35. Динамический анализ ПО.
36. Защита ПО от взлома и несанкционированного использования.
37. Угрозы и уязвимости информационной безопасности при разработке ПО.
38. Безопасное ПО.
39. Фаззинг.
40. Инструментальные среды и средства разработки и анализа ПО.
41. Управление конфигурацией ПО.
42. Документация разработчика ПО.
43. Цели создание безопасного ПО и меры по их достижению.

5.2. Курсовая работа (ПК 3.2)

Тематика курсовой работы: «Проведения анализа безопасности информации приложения, разработанного при выполнении курсовой работы по дисциплинам «Языки программирования» и/или «Методы программирования».

В рамках курсовой работы (КР) обучающиеся должны выполнить:
- анализ безопасности на уровне задания на КР;
- анализ безопасности архитектуры разработанного приложения:
- анализ безопасности исходного кода приложения;
- анализ безопасности используемых в приложении компонент;
- анализ безопасности исполняемого кода приложения;
- разработать меры по безопасной поставке приложения потребителю;
- разработать отчет об использованных при исследовании методах и средствах анализа и о результатах проведенных исследований безопасности приложения;
- выработать меры по устранению выявленных ошибок, уязвимостей и недекларированных возможностей приложения.