Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)

Институт информационных технологий и радиоэлектроники

Кафедра информатики и защиты информации

Основание: решение кафедры ИЗИ
от «28» 12 2016 года.

Зав. кафедрой ИЗИ _____ М.Ю. Монахов

# Фонд оценочных средств
для текущего контроля и промежуточной аттестации
при изучении учебной дисциплины
«Управление информационной безопасностью»

Направление подготовки: 10.04.01 «информационная безопасность»

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Владимир, 2016

## 1. Паспорт фонда оценочных средств

Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации при изучении учебной дисциплины «Управление информационной безопасностью» разработан в соответствие с рабочей программой, входящей в ОПОП направления подготовки 10.04.01 «информационная безопасность».

| № п/п | Контролируемые разделы (темы) дисциплины | Семестр | Код контролируемой компетенции (или ее части) | Наименование оценочного средства |
|---|---|---|---|---|
| 1 | Введение. Основные понятия | 3 | ПК-12, ПК-13 | Контрольные вопросы и задания |
| 2 | Основные определения и критерии классификации угроз | 3 | ПК-12, ПК-13 | Контрольные вопросы и задания |
| 3 | Общие положения управления рисками | 3 | ПК-12, ПК-13 | Контрольные вопросы и задания |
| 4 | Подготовительные этапы управления рисками | 3 | ПК-12, ПК-13 | Контрольные вопросы и задания |
| 5 | Анализ угроз и оценка рисков | 3 | ПК-12, ПК-13 | Контрольные вопросы и задания |
| 6 | Выбор защитных мер и последующие этапы управления рисками | 3 | ПК-12, ПК-13 | Контрольные вопросы и задания |
| 7 | Ключевые роли в процессе управления рисками | 3 | ПК-12, ПК-13 | Контрольные вопросы и задания |
| 8 | Детальное рассмотрение процесса оценки рисков | 3 | ПК-12, ПК-13 | Контрольные вопросы и задания |
| 9 | Результирующая документация | 3 | ПК-12, ПК-13 | Контрольные вопросы и задания |

Комплект оценочных средств по дисциплине «Управление информационной безопасностью» предназначен для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям образовательной программы, в том числе рабочей программы дисциплины «Управление информационной безопасностью», для оценивания результатов обучения: знаний, умений, навыков и уровня приобретенных компетенций.

Комплект оценочных средств по дисциплине «Управление информационной безопасностью» включает:

*3 семестр*

1. Оценочные средства для проведения текущего контроля успеваемости:

- комплект вопросов рейтинг-контроля, позволяющих оценивать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, распознавание объектов изучения в рамках определенного раздела дисциплины;

- комплект вопросов для контроля самостоятельной работы обучающихся при выполнении лабораторных работ, позволяющих оценивать знание фактического материала и умение использовать теоретические знания при решении практических задач.

- комплект вопросов для контроля самостоятельной работы обучающихся при выполнении заданий по СРС, позволяющих оценивать знание фактического материала и умение использовать теоретические знания при решении практических задач.

2. Оценочные средства для проведения промежуточной аттестации в форме: контрольные вопросы для проведения экзамена, позволяющие провести процедуру измерения уровня знаний и умений обучающихся.

**2. Перечень компетенций, формируемых в процессе изучения дисциплины «Управление информационной безопасностью» при освоении образовательной программы по направлению подготовки 10.04.01 «информационная безопасность»**

Перечень компетенций содержится в разделе 3 Рабочей программы дисциплины «Компетенции обучающегося, формируемые в результате освоения дисциплины»:

| ПК-12 – способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения; | | |
|---|---|---|
| Знать | Уметь | Владеть |
| - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; - основные механизмы информационной безопасности и типовые процессы управления этими механизмами в информационной системе; - основные угрозы безопасности информации и модели нарушителя в информационных системах; - принципы формирования политики информационной безопасности в информационных системах; - методы аттестации уровня защищенности информационных систем; - основные методы управления информационной безопасностью; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем | - строить системы обеспечения информационной безопасности в различных условиях функционирования защищаемых информационных систем;- разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; - разрабатывать частные политики информационной безопасности информационных систем; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; - оценивать информационные риски в информационных системах; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; - составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности | - методами и средствами выявления угроз безопасности информационным системам; - навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; - навыками участия в экспертизе состояния защищенности информации на объекте защиты; - методами управления информационной безопасностью информационных систем; - методами оценки информационных рисков; - методами организации и управления деятельностью служб защиты информации на предприятии; - навыками управления информационной безопасностью простых объектов |

| ПК-13 – способностью организовать управление информационной безопасностью. | | |
|---|---|---|
| Знать | Уметь | Владеть |
| - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; - основные механизмы информационной безопасности и типовые процессы управления этими механизмами в информационной системе; - основные угрозы безопасности информации и модели нарушителя в информационных системах; - принципы формирования политики | - строить системы обеспечения информационной безопасности в различных условиях функционирования защищаемых информационных систем;- разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; - разрабатывать частные политики информационной безопасности информационных систем; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; - оценивать информационные риски в информационных системах; - | - методами и средствами выявления угроз безопасности информационным системам; - навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; - навыками участия в экспертизе состояния защищенности информации на объекте защиты; - методами управления |

| | | |
|---|---|---|
| информационной безопасности в информационных системах; - методы аттестации уровня защищенности информационных систем; - основные методы управления информационной безопасностью; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем | разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; - составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности | информационной безопасностью информационных систем; - методами оценки информационных рисков; - методами организации и управления деятельностью служб защиты информации на предприятии; - навыками управления информационной безопасностью простых объектов |

Оценка по дисциплине выставляется с учетом среднего балла освоения компетенций, формируемых дисциплиной, при условии сформированности каждой компетенции не ниже порогового уровня.

## 3. Показатели, критерии и шкала оценивания компетенций текущего контроля знаний по учебной дисциплине «Управление информационной безопасностью»

Текущий контроль знаний, согласно «Положению о рейтинговой системе комплексной оценки знаний студентов в ВлГУ» (далее Положение) в рамках изучения дисциплины «Управление информационной безопасностью» предполагает письменный рейтинг-контроль, выполнение и защиту лабораторных, а также выполнение самостоятельных работ. В случае использования при изучении дисциплины дистанционных образовательных технологий проводится компьютерное тестирование.

**Регламент проведения письменного рейтинг-контроля**

| № | Вид работы | Продолжительность |
|---|---|---|
| 1 | Предел длительности рейтинг-контроля | 35-40 мин. |
| 2 | Внесение исправлений | до 5 мин. |
| | Итого | до 45 мин. |

**Критерии оценки письменного рейтинг-контроля**

Результаты каждого письменного рейтинга оцениваются в баллах. Максимальная сумма, набираемая студентом на каждом письменном рейтинге, составляет 10 баллов.

Критерии оценки для письменного рейтинга:

- 9-10 баллов выставляется обучающемуся, если соблюдаются критерии: полное раскрытие темы, вопроса, указание точных названий и определений, правильная формулировка понятий и категорий, приведение формул и (в необходимых случаях) их вывода, приведение статистики, самостоятельность ответа, использование дополнительной литературы;

- 7-8 баллов выставляется обучающемуся, если соблюдаются критерии: недостаточно полное раскрытие темы, несущественные ошибки в определении понятий и категорий, формулах, выводе формул, статистических данных, кардинально не меняющих суть изложения, наличие грамматических и стилистических ошибок, использование устаревшей учебной литературы;

- 5-6 баллов выставляется обучающемуся, если соблюдаются критерии: отражение лишь общего направления изложения лекционного материала и материала современных учебников, наличие достаточно количества несущественных или одной-двух существенных

ошибок в определении понятий и категорий, формулах, их выводе, статистических данных, наличие грамматических и стилистических ошибок, использование устаревшей учебной литературы, неспособность осветить проблематику дисциплины;

- 1-4 балла выставляется обучающемуся, если соблюдаются критерии: нераскрытые темы; большое количество существенных ошибок, наличие грамматических и стилистических ошибок, отсутствие необходимых умений и навыков.

**Оценочные средства для текущего контроля знаний по учебной дисциплине «Управление информационной безопасностью» (письменный рейтинг-контроль)**

***3 семестр:***

*Перечень вопросов для текущего контроля (письменный рейтинг №1):*

1. Что понимается под адекватной безопасностью?
2. Что такое компрометация в информационной безопасности?
3. Что понимается под нарушением информационной безопасности?
4. Что понимается под уровнем (степенью) критичности ИС?
5. Определите окружение (среду) ИС .
6. Охарактеризуйте процесс воздействия на производственную деятельность.
7. Дайте определение понятию «риск».
8. В чем особенности рисков, связанных с информационными технологиями.
9. Что такое остаточный риск?
10. Что такое совокупный (суммарный, полный) риск.
11. Определите понятие «Анализ рисков».
12. В чем состоит управление рисками в информационной безопасности?
13. Что такое нейтрализация (уменьшение, ослабление) рисков?
14. Что такое терпимость по отношению к риску?
15. Определите основные категория безопасности.
16. Что понимают под уровнем защищенности.
17. Дайте определение угроз конфиденциальной информации.
18. Что такое атака?
19. Что такое окно опасности?
20. Какие события происходят во время существования окна опасности?
21. Что такое угрозы воздействия на источник информации?
22. Что такое угрозы утечки информации?
23. Какие угрозы называются преднамеренными?
24. Какие угрозы называются случайными?
25. Что такое канал несанкционированного доступа?
26. Что такое утечка информации?
27. Что такое перехват в теории информационной безопасности?
28. Что такое канал утечки информации?
29. Что такое технический канал утечки информации?
30. Охарактеризуйте случайный и организованный канал утечки информации.
31. Что такое источник угроз безопасности информации?
32. Назовите основные источники преднамеренных угроз.
33. Назовите основные источники случайных угроз.
34. Прокомментируйте наиболее распространенные угрозы доступности.
35. Охарактеризуйте непреднамеренные ошибки в качестве угрозы доступности.
36. Что такое отказ пользователей?
37. Прокомментируйте внутренний отказ ИС в качестве угрозы.
38. Прокомментируйте отказ поддерживающей инфраструктуры в качестве угрозы.
39. Каким образом происходит повреждение или даже разрушение оборудования?
40. Что такое вредоносное программное обеспечение?

41. Какие негативные последствия в функционировании ИС вызывает вредоносное ПО?
42. Охарактеризуйте основные угрозы целостности конфиденциальной информации.
43. Перечислите основные угрозы конфиденциальности информацию
44. Что понимают под перехватом данных и в чем заключается угроза конфиденциальности?
45. Охарактеризуйте этап выбора эффективных и экономичных защитных средств (нейтрализация рисков).
46. В чем заключается суть мероприятий по управлению рисками?
47. Какие возможны действия по отношению к выявленным рискам?
48. Какие этапы управления рисками относятся к вспомогательным и почему?
49. Почему карта информационной системы способствует управлению рисками?
50. Какие этапы управления рисками относятся к основным и почему?
51. Почему важен процесс интегрирования управления рисками в жизненный цикл ИС?

*Перечень вопросов для текущего контроля (письменный рейтинг №2):*

1. Каким образом производится выбор анализируемых объектов
2. Почему важен уровень детализации при рассмотрении анализируемых объектов?
3. Что такое инфологическая модель ИС?
4. Приведите основные объекты инфологической модели объекта
5. Как сформировать карту информационной системы организации?
6. Что такое идентификация активов в управлении рисками информационной безопасности?
7. Какие средства автоматизации идентификация активов ИС организации Вы знаете?
8. Приведите перечень наиболее распространенных угроз.
9. Что такое модель угроз организации?
10. Приведите основные компоненты модели угроз организации.
11. Охарактеризуйте процедуры идентификации угроз.
12. Приведите основные источники возникновения угроз.
13. Что включает в себя понятие «модель (облик) нарушителя»?
14. Приведите возможную классификацию нарушителей.
15. Прокомментируйте возможности конкурентов, клиентов, посетителей и хакеров в качестве потенциальных злоумышленников
16. Определите цели администраторов, программистов, операторов, руководителей, технического персонала, сотрудников, уволенных с работы в качестве потенциальных нарушителей ИБ
17. Что такое матрица нарушений ИБ? Приведите ее возможную структуру.
18. Зачем необходим сценарий нарушения ИБ?
19. Приведите модели оценки вероятности осуществления угрозы.
20. Охарактеризуйте основные метрики, используемые для оценки вероятности осуществления угрозы.
21. Дайте определение способа защиты информации.
22. Охарактеризуйте способ предупреждения возможных угроз.
23. Прокомментируйте основные действия способа выявления угроз
24. Охарактеризуйте способ обнаружения угроз.
25. Охарактеризуйте способ пресечения или локализации угроз.
26. Прокомментируйте основные действия способа ликвидации последствий.
27. Перечислите основные защитные действия при реализации способов ЗИ,
28. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации
29. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации
30. Назовите три группы мероприятий по технической защите информации.
31. Прокомментируйте основные организационные мероприятия по технической защите информации.

32. В каких ограничительных мерах выражаются организационные мероприятия по ЗИ.
33. Прокомментируйте основные организационно-технические мероприятия по ЗИ.
34. Прокомментируйте основные технические мероприятия по технической защите информации.
35. Как оценить стоимости защитных мер.
36. В чем заключается проблема совместимости нового средства защитных мер со сложившейся организационной и аппаратно-программной структурой, с традициями организации?
37. Планирование реализации и проверки новых регуляторов безопасности.
38. План тестирования (автономного и комплексного) программно-технических механизмов защиты.

*Перечень вопросов для текущего контроля (письменный рейтинг №3):*

1. Почему управление рисками рассматривается на административном уровне ИБ?
2. Охарактеризуйте роль руководителя организации в процессе управления рисками информационной безопасности.
3. Охарактеризуйте роль начальника управления (отдела) информатизации в процессе управления рисками информационной безопасности.
4. Охарактеризуйте роль владельцев систем и информации в процессе управления рисками информационной безопасности.
5. Охарактеризуйте роль руководителей производственных отделов и отдела закупок в процессе управления рисками информационной безопасности.
6. Охарактеризуйте роль начальника отдела (управления) информационной безопасности в процессе управления рисками информационной безопасности.
7. Охарактеризуйте роль администраторов безопасности в процессе управления рисками информационной безопасности.
8. Охарактеризуйте роль специалистов по обучению персонала в процессе управления рисками информационной безопасности.
9. Почему управление рисками рассматривается на административном уровне ИБ?
10. Охарактеризуйте роль руководителя организации в процессе управления рисками информационной безопасности.
11. Охарактеризуйте роль начальника управления (отдела) информатизации в процессе управления рисками информационной безопасности.
12. Охарактеризуйте роль владельцев систем и информации в процессе управления рисками информационной безопасности.
13. Охарактеризуйте роль руководителей производственных отделов и отдела закупок в процессе управления рисками информационной безопасности.
14. Охарактеризуйте роль начальника отдела (управления) информационной безопасности в процессе управления рисками информационной безопасности.
15. Охарактеризуйте роль администраторов безопасности в процессе управления рисками информационной безопасности.
16. Охарактеризуйте роль специалистов по обучению персонала в процессе управления рисками информационной безопасности.
17. Назовите и охарактеризуйте этапы процесса управления рисками.
18. Какие этапы управления рисками относятся к вспомогательным и почему?
19. Опишите этап выбора анализируемых объектов и уровня детализации их рассмотрения процесса управления рисками.
20. Какие этапы управления рисками относятся к основным и почему?
21. Охарактеризуйте основные шаги анализа угроз в процедуре управления рисками.
22. Охарактеризуйте этап оценки рисков в процедуре управления рисками.
23. Охарактеризуйте этап выбора защитных мер в процедуре управления рисками.
24. Охарактеризуйте этап реализации и проверки выбранных мер защиты в процедуре управления рисками.

25. Что такое оценка остаточного риска?
26. Определение приоритетов, оценка и реализация контрмер, уменьшающих риски и рекомендованных по результатам оценки рисков.
27. Назовите различные возможности в процессе принятия риска
28. Назовите различные возможности в процессе уклонения от риска
29. Назовите различные возможности в процессе ограничения (нейтрализации) риска
30. Назовите различные возможности в процессе переадресации риска.
31. В чем состоит оценка экономической эффективности.
32. Приведите возможный формат отчета об оценке рисков.
33. Приведите возможный формат плана реализации контрмер.
34. Приведите возможные трактовки и способы вычисления рисков.
35. Каким образом осуществляется представление рисков в виде дерева уязвимостей, угроз и контрмер.

**Регламент проведения лабораторных работ**

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Управление информационной безопасностью» предполагается выполнение лабораторных работ, что позволяет углубить процесс познания, раскрыть понимание прикладной значимости осваиваемой дисциплины.

**Критерии оценки выполнения лабораторных работ**

Результаты выполнения каждой лабораторной работы оцениваются в баллах. Максимальная сумма, набираемая студентом за выполнение каждой лабораторной работы, составляет 3 балла.

Критерии оценки для выполнения лабораторной работы:

- 2,4-3 балла выставляется обучающемуся, если соблюдаются критерии: представлен полный письменный отчет по лабораторной работе, содержащий описание всех этапов ее выполнения и надлежащим образом оформленный (в печатном или электронном виде - в соответствие с требованием преподавателя), полностью выполнено задание на лабораторную работу, обучающийся верно и полно ответил на все контрольные вопросы преподавателя по теоретической и практической части лабораторной работы, лабораторная работа выполнена самостоятельно и в определенный преподавателем срок;

- 1,4-2,3 балла выставляется обучающемуся, если соблюдаются критерии: представлен недостаточно полный письменный отчет по лабораторной работе, содержащий описание всех этапов ее выполнения, имеющий, возможно, погрешности в оформлении (в печатном или электронном виде - в соответствие с требованием преподавателя), полностью выполнено задание на лабораторную работу, обучающийся преимущественно верно и полно ответил на контрольные вопросы преподавателя по теоретической и практической части лабораторной работы, лабораторная работа выполнена самостоятельно, возможно, с нарушением определенного преподавателем срока предоставления отчета, отчет содержит грамматические и стилистические ошибки;

- 0,7-1,3 балла выставляется обучающемуся, если соблюдаются критерии: представлен недостаточно полный письменный отчет по лабораторной работе, содержащий описание не всех этапов ее выполнения, имеющий, возможно, погрешности в оформлении (в печатном или электронном виде - в соответствие с требованием преподавателя), в основном выполнено задание на лабораторную работу, обучающийся ответил на контрольные вопросы преподавателя по теоретической и практической части лабораторной работы с отражением лишь общего направления изложения материала, с наличием достаточно количества

несущественных или одной-двух существенных ошибок, лабораторная работа выполнена самостоятельно, с нарушением определенного преподавателем срока предоставления отчета, отчет содержит грамматические и стилистические ошибки, при его составлении использована устаревшая учебная литература;

- 0,2-0,6 балла выставляется обучающемуся, если соблюдаются критерии: письменный отчет по лабораторной работе (в печатном или электронном виде - в соответствие с требованием преподавателя) не представлен или представлен неполный, отчет содержит описание не всех этапов выполнения работы, имеет погрешности в оформлении, задание на лабораторную работу выполнено не полностью, обучающийся ответил на контрольные вопросы преподавателя по теоретической и практической части лабораторной работы с большим количеством существенных ошибок, продемонстрировал неспособность осветить проблематику лабораторной работы, лабораторная работа выполнена несамостоятельно, с существенным нарушением определенного преподавателем срока предоставления отчета, отчет содержит грамматические и стилистические ошибки, при его составлении использована устаревшая учебная литература, обучающийся при выполнении работы продемонстрировал отсутствие необходимых умений и практических навыков.

При оценке за лабораторную работу менее 0,2 балла, данная работа считается невыполненной и не зачитывается. При невыполнении лабораторной работы хотя бы по одной из изучаемых тем, обучающийся не получает положительную оценку при промежуточном контроле по дисциплине (экзамене).

**Оценочные средства для текущего контроля знаний по учебной дисциплине «Управление информационной безопасностью» (лабораторные работы)**

*Перечень вопросов для контроля самостоятельной работы обучающихся при выполнении лабораторных работ (3 семестр):*

ЛАБОРАТОРНАЯ РАБОТА 1. Сбор исходных данных для аудита информационной безопасности объекта

-Дайте определение «аудит информационной безопасности объекта»

-Перечислите виды аудита безопасности?

-Как происходит сбор исходных данных?

-Какие существуют методы для сбора исходных данных?

ЛАБОРАТОРНАЯ РАБОТА 2. Выявление уязвимостей информационной системы

-Что понимается под уязвимостью информационной системы?

-Идентификация уязвимостей на стадии проектирования ИС, на этапе реализации, на этапе эксплуатации

-Каким образом осуществляется представление рисков в виде дерева уязвимостей, угроз и контрмер.

ЛАБОРАТОРНАЯ РАБОТА 3. Идентификация защитных механизмов

-Что понимается под понятием «защитный механизм»?

-Перечислите первичные защитные механизмы

-Перечислите вторичные защитные механизмы

-Как происходит идентификация защитных механизмов?

ЛАБОРАТОРНАЯ РАБОТА 4. Идентификация нарушителей

-Дайте определение понятию «идентификация»

-Кто называется нарушителем?

-Опишите механизм идентификации нарушителей

**Регламент проведения самостоятельной работы**

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Управление информационной безопасностью» предполагается выполнение заданий СРС, что позволяет углубить процесс познания, раскрыть понимание прикладной значимости осваиваемой дисциплины.

**Критерии оценки выполнения самостоятельной работы**

Результаты выполнения самостоятельной работы оцениваются в баллах. Максимальная сумма, набираемая студентом за выполнение работы по каждой теме, составляет 1 балл.

Критерии оценки для выполнения работы:

- 0,9-1 балла выставляется обучающемуся, если соблюдаются критерии: обучающийся верно и полно ответил на все контрольные вопросы преподавателя по теме; полностью, самостоятельно и в определенный преподавателем срок выполнено задание;

- 0,7-0,8 балла выставляется обучающемуся, если соблюдаются критерии: обучающийся преимущественно верно и полно ответил на контрольные вопросы преподавателя по теме; задание выполнено самостоятельно, возможно, с нарушением определенного преподавателем срока;

- 0,5-0,6 балла выставляется обучающемуся, если соблюдаются критерии: обучающийся ответил на контрольные вопросы преподавателя по теме с отражением лишь общего направления изложения материала; задание выполнено самостоятельно, возможно, с нарушением определенного преподавателем срока, содержит незначительные ошибки;

- 0,1-0,4 балла выставляется обучающемуся, если соблюдаются критерии: обучающийся ответил на контрольные вопросы преподавателя по теме с большим количеством существенных ошибок, продемонстрировал неспособность осветить проблематику темы; задание выполнено не полностью, не самостоятельно, с существенным нарушением определенного преподавателем срока, при выполнении задания продемонстрировал отсутствие необходимых умений и практических навыков.

**Оценочные средства для текущего контроля знаний по учебной дисциплине «Управление информационной безопасностью» (самостоятельная работа)**

*3 семестр:*

| № пп | Раздел (тема) дисциплины | Виды СРС | Формы контроля СРС | Баллы по СРС |
|---|---|---|---|---|
| 1 | Введение. Основные понятия | Работа с учебниками (учебными пособиями). Работа с конспектом лекций. | Письменный или устный опрос, проверка конспектов | 1 |
| 2 | Основные определения и критерии классификации угроз | Работа с учебниками (учебными пособиями). Работа с конспектом лекций. | Письменный или устный опрос, проверка конспектов | 1 |
| 3 | Общие положения управления рисками | Работа с учебниками (учебными пособиями). Работа с конспектом лекций. | Письменный или устный опрос, проверка конспектов | 1 |
| 4 | Подготовительные этапы управления рисками | Работа с учебниками (учебными пособиями). Работа с конспектом лекций. | Письменный или устный опрос, проверка конспектов | 1 |
| 5 | Анализ угроз и оценка рисков | Работа с учебниками (учебными пособиями). Работа с конспектом лекций. | Письменный или устный опрос, проверка конспектов | 1 |
| 6 | Выбор защитных мер и последующие этапы управления рисками | Работа с учебниками (учебными пособиями). Работа с конспектом лекций. | Письменный или устный опрос, проверка конспектов | 1 |

| | | | | |
|---|---|---|---|---|
| 7 | Ключевые роли в процессе управления рисками | Работа с учебниками (учебными пособиями). Работа с конспектом лекций. | Письменный или устный опрос, проверка конспектов | 1 |
| 8 | Детальное рассмотрение процесса оценки рисков | Работа с учебниками (учебными пособиями). Работа с конспектом лекций. | Письменный или устный опрос, проверка конспектов | 1 |
| 9 | Результирующая документация | Работа с учебниками (учебными пособиями). Работа с конспектом лекций. | Письменный или устный опрос, проверка конспектов | 1 |
| | | | Итого за семестр: | 9 |

*Перечень вопросов для контроля самостоятельной работы обучающихся при выполнении СРС (3 семестр):*

**Раздел 1.**

1. Определите базовый уровень безопасности.
2. Определите окружение (среду) ИС .
3. Охарактеризуйте процесс воздействия на производственную деятельность.
4. В чем особенности рисков, связанных с информационными технологиями.
5. Что такое нейтрализация (уменьшение, ослабление) рисков?
6. Что такое терпимость по отношению к риску?
7. Определите основные категория безопасности.
8. Что понимают под уровнем защищенности.

**Раздел 2.**

1. Назовите типовые причины возникновения каналов несанкционированного доступа.
2. Какие действия пользователя информации и злоумышленника, создающие угрозы утечки информации, в случае попадания ее к злоумышленнику приводят к утечке?
3. Охарактеризуйте случайный и организованный канал утечки информации.
4. Приведите качественную зависимость вероятности возникновения угрозы воздействия от соотношения цены информации и затрат злоумышленника на ее добывание.
5. Назовите основные источники преднамеренных угроз.
6. Назовите основные источники случайных угроз.
7. Какие сигналы в теории информационной безопасности принято называть опасными?
8. Что такое опасный функциональный сигнал?
9. Назовите основные источники опасных функциональных сигналов.
10. Что такое вредоносное программное обеспечение?
11. Дайте определение «бомбы».
12. Дайте определение «червя».
13. Дайте определение «вируса».
14. Что в ИБ понимают под маскарадом?

**Раздел 3.**

1. В чем заключается суть мероприятий по управлению рисками?
2. Охарактеризуйте процесс интегрирования управления рисками на этапе закупки (разработки) жизненного цикла ИС.
3. Охарактеризуйте процесс интегрирования управления рисками на этапе установки жизненного цикла ИС.
4. Охарактеризуйте процесс интегрирования управления рисками на этапе эксплуатации жизненного цикла ИС.
5. Охарактеризуйте процесс интегрирования управления рисками на этапе выведении системы из эксплуатации жизненного цикла ИС.

**Раздел 4.**

1. Каким образом производится выбор анализируемых объектов
2. Приведите основные объекты инфологической модели объекта
3. Как сформировать карту информационной системы организации?
4. Какие средства автоматизации идентификация активов ИС организации Вы знаете?

**Раздел 5**.

1. Приведите перечень наиболее распространенных угроз.
2. Приведите основные компоненты модели угроз организации.
3. Приведите основные источники возникновения угроз.
4. Приведите возможную классификацию нарушителей.
5. Прокомментируйте возможности конкурентов, клиентов, посетителей и хакеров в качестве потенциальных злоумышленников
6. Определите цели администраторов, программистов, операторов, руководителей, технического персонала, сотрудников, уволенных с работы в качестве потенциальных нарушителей ИБ
7. Приведите модели оценки вероятности осуществления угрозы.
8. Охарактеризуйте основные метрики, используемые для оценки вероятности осуществления угрозы.

**Раздел 6.**

1. Дайте определение способа защиты информации.
2. Охарактеризуйте способ предупреждения возможных угроз.
3. Прокомментируйте основные действия способа выявления угроз
4. Охарактеризуйте способ обнаружения угроз.
5. Охарактеризуйте способ пресечения или локализации угроз.
6. Прокомментируйте основные действия способа ликвидации последствий.
7. Перечислите основные защитные действия при реализации способов ЗИ,
8. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации
9. Назовите три группы мероприятий по технической защите информации.
10. Прокомментируйте основные организационные мероприятия по технической защите информации.
11. В каких ограничительных мерах выражаются организационные мероприятия по ЗИ.

**Раздел 7.**

1. Охарактеризуйте роль руководителя организации в процессе управления рисками информационной безопасности.
2. Охарактеризуйте роль начальника управления (отдела) информатизации в процессе управления рисками информационной безопасности.
3. Охарактеризуйте роль владельцев систем и информации в процессе управления рисками информационной безопасности.
4. Охарактеризуйте роль руководителей производственных отделов и отдела закупок в процессе управления рисками информационной безопасности.
5. Охарактеризуйте роль начальника отдела (управления) информационной безопасности в процессе управления рисками информационной безопасности.
6. Охарактеризуйте роль администраторов безопасности в процессе управления рисками информационной безопасности.
7. Охарактеризуйте роль специалистов по обучению персонала в процессе управления рисками информационной безопасности.
8. Почему управление рисками рассматривается на административном уровне ИБ?

**Раздел 8.**

1. Назовите и охарактеризуйте этапы процесса управления рисками.
2. Опишите этап выбора анализируемых объектов и уровня детализации их рассмотрения процесса управления рисками.
3. Охарактеризуйте основные шаги анализа угроз в процедуре управления рисками.
4. Охарактеризуйте этап оценки рисков в процедуре управления рисками.
5. Охарактеризуйте этап выбора защитных мер в процедуре управления рисками.
6. Охарактеризуйте этап реализации и проверки выбранных мер защиты в процедуре управления рисками.

**Раздел 9.**

1. Назовите различные возможности в процессе ограничения (нейтрализации) риска
2. Назовите различные возможности в процессе переадресации риска.
3. В чем состоит оценка экономической эффективности.
4. Приведите возможный формат отчета об оценке рисков.
5. Приведите возможный формат плана реализации контрмер.
6. Приведите возможные трактовки и способы вычисления рисков.
7. Каким образом осуществляется представление рисков в виде дерева уязвимостей, угроз и контрмер.

**Регламент проведения курсового проекта**

*Примерные темы заданий к курсовой работе*

1. Задачи аналитической работы в сфере защиты информации;
2. Источники, угрозы, каналы распространения и утраты конфиденциальной информации;
3. Задачи аналитической работы по выявлению угроз и каналов утраты конфиденциальной информации;
4. Критерии целесообразности защиты информации;
5. Направления использования результатов аналитической работы для формирования системы защиты информации.
6. Направления классификации информационных ресурсов в предпринимательской сфере;
7. Критерии ценности, полезности и конфиденциальности информации;
8. Содержание процедуры разработки перечня ценных и конфиденциальных сведений;
9. Содержание процедуры ведения перечня ценных и конфиденциальных сведений;
10. Назначение и содержание перечня конфиденциальных документов фирмы.

**Критерии оценки выполнения курсового проекта**

| №п/п | Расшифровка критериев | Количество баллов |
|---|---|---|
| 1 | Представление результатов курсовой работы (доклад, ответы на вопросы) | 20 |
| 2 | Качество оформления пояснительной записки и графического материала (в т.ч. презентации). Нормоконтроль в соответствии с требованиями ГОСТ. | 30 |
| 3 | Промежуточная аттестация (оцениваются результаты работы: степень выполнения, соответствие поставленной задаче, график работ, устранение замечаний и т.п.) | 25 |
| 4 | Финальная аттестация (оцениваются результаты работы: степень выполнения, соответствие поставленной задаче, разработанное ПО и т.п.) | 25 |
| | Общее количество баллов | 100 |

**Баллы округляются в большую строну. Результаты курсового проекта определяются следующими оценками: «зачтено» и «незачтено» по следующей шкале:**

**«Зачтено» - от 61 балла.**

**«Незачтено» - 60 и менее баллов.**

При неудовлетворительной оценке за курсовой проект обучающийся не получает положительную оценку при промежуточном контроле по дисциплине (экзамене).

**Общее распределение баллов текущего контроля по видам учебных работ для студентов (в соответствие с Положением)**

***3 семестр***

| № | Пункт | Максимальное число баллов |
|---|---|---|
| 1 | Письменный рейтинг-контроль 1 | 10 |
| 2 | Письменный рейтинг-контроль 2 | 10 |
| 3 | Письменный рейтинг-контроль 3 | 10 |
| 4 | Посещение занятий студентом | 5 |
| 5 | Дополнительные баллы (бонусы) | 4 |
| 6 | Лабораторные работы | 12 |
| 7 | Выполнение семестрового плана самостоятельной работы | 9 |
| 8 | Экзамен | 40 |
| | Всего | 100 |

## 4. Показатели, критерии и шкала оценивания компетенций промежуточной аттестации знаний по учебной дисциплине «Управление информационной безопасностью»

**Регламент проведения промежуточного контроля (экзамена)**

Промежуточная аттестация по итогам освоения дисциплины (экзамен) проводится в экзаменационную сессию. Экзамен проводится по билетам, содержащим три вопроса. Студент пишет ответы на вопросы экзаменационного билета на листах белой бумаги формата А4, на каждом из которых должны быть указаны: фамилия, имя отчество студента; шифр студенческой группы; дата проведения экзамена; номер экзаменационного билета. Листы должны быть подписаны и студентом и экзаменатором после получения студентом экзаменационного билета. Экзаменационные билеты должны быть оформлены в соответствие с утвержденным регламентом.

После подготовки студент устно отвечает на вопросы билета и уточняющие вопросы экзаменатора. Экзаменатор вправе задать студенту дополнительные вопросы и задания по материалам дисциплины для выявления степени усвоения студентом компетенций.

Максимальное количество баллов, которое студент может получить на экзамене, в соответствие с Положением составляет 40 баллов.

**Критерии оценивания компетенций на экзамене**

| **Оценка в баллах** | **Оценка за ответ на экзамене** | **Критерии оценивания компетенций** |
|---|---|---|
| 30 - 40 | «Отлично» | Студент глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, не затрудняется с ответом при видоизменении заданий, использует при ответе материалы из основной и дополнительной литературы по дисциплине, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических задач, подтверждает полное освоение |

| | | |
|---|---|---|
| | | компетенций, предусмотренных рабочей программой дисциплины. |
| 20 - 29 | «Хорошо» | Студент показывает твердое знание материала, грамотно и по существу излагает его, не допускает существенных неточностей при ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения, допуская некоторые неточности; демонстрирует хороший уровень освоения материала, информационной и коммуникативной культуры и в целом подтверждает освоение компетенций, предусмотренных рабочей программой дисциплины. |
| 10 - 19 | «Удовлетворительно» | Студент показывает знания только основного материала, но не усвоил его деталей; допускает неточности, недостаточно правильные формулировки, которые в целом не препятствуют усвоению последующего программного материала; допускает нарушения логической последовательности в изложении программного материала; испытывает затруднения при выполнении практических работ; подтверждает освоение компетенций, предусмотренных рабочей программой дисциплины, на минимально допустимом уровне. |
| 0 - 10 | «Неудовлетворительно» | Студент не знает значительной части программного материала, имеет менее 50% правильно выполненных заданий от общего объема работы, допускает существенные ошибки при изложении материала, неуверенно, с большими затруднениями выполняет практические работы, не подтверждает освоение компетенций, предусмотренных рабочей программой дисциплины. |

**Оценочные средства для промежуточной аттестации по учебной дисциплине «Управление информационной безопасностью» (экзамен)**

*Перечень вопросов для промежуточного контроля (экзамена)*

1. Бизнес-ориентированное управление ИТ на современном предприятии.
2. Виды программ технического обслуживания (стандартные программы).
3. Значение технического обслуживания.
4. Как обслуживаются высококритичные системы.
5. Концепция управления ИТ-подразделением — IT Service Management.
6. Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC
7. Гарантии безопасности компьютерных систем в системе общих критериев
8. Классификация защищенности компьютерной системы по требованиям безопасности информации в системе общих критериев
9. Основные угрозы безопасности информации в компьютерных системах
10. Государственная политика в области безопасности компьютерных систем
11. Порядок сертификации средств защиты информации для разработчика СЗИ.
12. Порядок сертификации защищенных информационных систем
13. Порядок лицензирования в области создания средств защиты информации и защищенных информационных систем
14. Разработка политик безопасности для защищенных компьютерных систем
15. Порядок аттестации защищенных компьютерных систем
16. Критерии эффективности работы ИС.
17. Оперативные мероприятия.
18. Организация технического обслуживания ИТ.

19. Плановые мероприятия.
20. Понятие гарантии.
21. Порядок внедрения SLM-системы.
22. Порядок осуществления гарантии.
23. Преимущества внедрения ITSM.
24. Причины отказа в гарантийном обслуживании.
25. Программы технического обслуживания.
26. Разовые мероприятия.
27. Расширенные программы технического обслуживания.
28. Регламентные мероприятия.
29. Содержание модели ITSM HP. Процессы взаимодействия и ИТ-служб.
30. Содержание модели ITSM HP. Процессы проектирования и управления услугами.
31. Содержание модели ITSM HP. Процессы разработки услуг.
32. Содержание модели ITSM HP. Процессы эксплуатации.
33. Схемы технического обслуживания.
34. Эталонная модель Hewlett-Packard управления ИТ-услугами.