Федеральное государственное бюджетное образовательное учреждение высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

—УТВЕРЖДАЮ‖
ДЕКАН
АВТФ к.т.н., доцент
И.Л. Рева
—__‖_____г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ДИСЦИПЛИНЫ

Аудит информационной безопасности

Образовательная программа: 10.04.01 Информационная безопасность, профиль: Методы и средства обеспечения технической защиты информации

Новосибирск - 2023

1. Методика оценки этапов формирования компетенций по дисциплине

Результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций проверяются при проведении мероприятий текущей аттестации (контроля) в процессе изучения дисциплины.

Промежуточная аттестация по **дисциплине** проводится во 2 семестре - в форме зачета, который направлен на оценку сформированности результатов обучения по дисциплине, соотнесенных с установленными в программе индикаторами достижения компетенций ОПК-1 и соотнесенных с ними индикаторов.

Зачет проводится в форме письменного тестирования с использованием электронной информационно-образовательной среды НГТУ (http:// www.nstu.ru/sveden/eos).

Общие правила выставления оценок текущей и промежуточной аттестации по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе дисциплины.

На основании критериев, приведенных в п. 2, осуществляется оценка уровней достигнутых результатов обучения по дисциплине, соотнесенных с установленными в программе индикаторами достижения компетенции ОПК-1, закрепленных за дисциплиной.

2. Общая характеристика уровней результатов обучения, соотнесенных с индикаторами достижения компетенций

Продвинутый. Теоретическое содержание курса освоено полностью. Студент демонстрирует систематическое и глубокое понимание учебного материала и способность к самостоятельному пополнению и обновлению знаний в ходе дальнейшей учебной работы и профессиональной деятельности. Сформированы необходимые навыки практической работы. Все учебные задания, предусмотренные программой обучения, выполнены качественно, без замечаний. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов, входящим в диапазон продвинутого уровня.

Базовый. Теоретическое содержание курса освоено в объеме, необходимом для дальнейшей учебы и профессиональной деятельности. Навыки практической работы сформированы на базовом уровне. Все предусмотренные программой обучения учебные задания выполнены с небольшими погрешностями. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов в пределах базового уровня.

Пороговый. Теоретическое содержание курса освоено в объеме, необходимом для дальнейшей учебы и профессиональной деятельности.Некоторые практические навыки работы с сформированы с пробелами. Учебные задания, предусмотренные программой обучения, выполнялись с ошибками, исправленными под руководством преподавателя. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов в пределах порогового уровня.

Ниже порогового. Теоретическое содержание курса освоено фрагментарно. Необходимые навыки практической работы сформированы минимально. Большинство учебных заданий, предусмотренных программой обучения, не выполнены. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов, входящих в диапазон ниже порогового уровня.

Паспорт зачета

по дисциплине «Аудит информационной безопасности», 2 семестр

1. Методика оценки

Зачет проводится в форме письменного тестирования с использованием электронной информационно-образовательной среды НГТУ (http:// www.nstu.ru/sveden/eos).

Тестовые задания охватывают все содержание дисциплины «Аудит информационной безопасности».

Тест состоит из вопросов различного вида, и позволяет проверить результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций.

2. Критерии оценки результатов обучения, соотнесенных с уровнями освоения индикаторов достижения компетенций

Выполнение теста засчитывается на **продвинутом** уровне, если студент правильно ответил на 5/6 вопросов теста, знает определения всех понятий, продемонстрировал способность безошибочно устанавливать последовательность и соответствие между процессами и явлениями, выявлять проблемы, предлагать механизмы их решения, представляет количественные и качественные характеристики определенных процессов и не допускает ошибок при решении задач. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций не содержит пробелов. Установленные в программе компетенции сформированы в полном объеме. Оценка составляет *от 18 до 20 баллов.*

Выполнение теста засчитывается на **базовом** уровне, если студент правильно ответил на 2/3 вопросов теста, знает определения основных понятий, продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, правильно характеризует процессы, явления, не допускает существенных ошибок при решении задач. Совокупность результатов обучения по дисциплине (модулю) и соотнесенных с ними индикаторов достижения компетенций содержит несущественные пробелы. Установленные в программе компетенции сформированы на базовом уровне. Оценка составляет *от 14 до 17 баллов.*

Выполнение теста засчитывается на **пороговом** уровне, если студент правильно ответил от 1/2 до 2/3 вопросов теста, знает определения основных понятий, продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, при решении задач допускает непринципиальные ошибки, например, вычислительные. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит пробелы. Установленные в программе компетенции сформированы на пороговом уровне. Оценка составляет *от 10 до 13 баллов.*

Выполнение теста считается **неудовлетворительным**, если студент правильно ответил менее чем на половину вопросов теста, не знает определений понятий, не продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, при решении задач допускает принципиальные ошибки. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит существенные пробелы. Установленные в программе компетенции не сформированы. Оценка составляет *менее 10 баллов.*

3. Шкала оценки

Зачет считается сданным, если сумма баллов по всем заданиям билета составляет от 10 до 20 баллов включительно. Сумма менее 10 баллов признается неудовлетворительным результатом промежуточной аттестации по дисциплине.

В общей оценке по дисциплине зачетные баллы учитываются в соответствии с правилами балльно-рейтинговой системы, установленными в НГТУ.

4. Фонд оценочных материалов (вопросы теста[1]) для оценки уровня сформированности компетенций и соотнесенных с ними индикаторов

Формируемая компетенции	Индикаторы компетенции
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	2. владеет навыками участия в разработке системы обеспечения информационной безопасности объекта 5. знает основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности

Вопросы теста для оценки сформированности компетенции ОПК-1

Вопрос 1. Какой тип аудита **не** определен стандартом ГОСТ Р ИСО/МЭК 27000 «Информационные технологии - Методы и средства обеспечения безопасности - Системы менеджмента информационной безопасности – Общие сведения и словарь»?

☐ внутренний

☐ **низкоуровневый** ✔

☐ внешний

(один вариант)

Вопрос 2. Дополните понятие «аудит», согласно ГОСТ Р ИСО/МЭК 27000 «Информационные технологии - Методы и средства обеспечения безопасности - Системы менеджмента информационной безопасности – Общие сведения и словарь». Аудит - систематический, независимый и ___ _____ получения свидетельства аудита.

Ответ:

Решение: документированный процесс

Вопрос 3. Кем проводятся, согласно национального стандарта Российской Федерации ГОСТ Р ИСО 19011-2021 «Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента», внутренние аудиты (аудиты первой стороны)?

Ответ:

Решение: Проводятся самой организацией.

Вопрос 4. Кем проводятся, согласно национального стандарта Российской Федерации ГОСТ Р ИСО 19011-2021 «Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента», внешние аудиты, называемые «аудиты второй стороны»?

Ответ:

Решение: Проводятся потребителями.

[1] Правильные ответы выделены галочкой

Вопрос 5. Какую организацию должен привлекать к проведению работ по аттестации объекта информатизации его владелец?

Ответ:

Решение: имеющую лицензию на осуществление деятельности по технической защите.

Вопрос 6. Каковы цели аудита СМИБ, согласно национального стандарта Российской Федерации ГОСТ Р ИСО 19011-2021 «Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента»?

☐ **оценка возможности системы менеджмента обеспечить соответствие законодательным, нормативно-правовым требованиям, договорным требованиям, а также другим требованиям, которые организация обязуется выполнять** ✔

☐ определение эффективности системы менеджмента при достижении намеченных результатов.

☐ оценка возможностей для потенциального улучшения системы менеджмента.

(один вариант)

Вопрос 7. Кем проводятся, согласно национального стандарта Российской Федерации ГОСТ Р ИСО 19011-2021 «Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента», внешние аудиты, называемые «аудиты третьей стороны»?

Ответ:

Решение: Проводятся внешними организациями.

Вопрос 8. В скольких проверяемых организациях проводится «комплексный аудит», согласно национального стандарта Российской Федерации ГОСТ Р ИСО 19011-2021 «Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента»?

Ответ:

Решение: в одной.

Вопрос 9. Дополните понятие «критерии аудита», согласно национального стандарта Российской Федерации ГОСТ Р ИСО 19011-2021 «Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента». Критерии аудита - это ____ _____, используемых как основа для сравнения с ними объективного свидетельства.

Ответ:

Решение:. совокупность требований

Вопрос 10. Дополните понятие сертификат соответствия, полученный в системе сертификации ФСТЭК. Сертификат соответствия ФСТЭК - это документ, подтверждающий, что представленный ИТ- продукт (инструмент защиты данных) прошел ___ ____ процедуры и соответствует действующим стандартам и требованиям.

Ответ:

Решение: необходимые проверочные

Вопрос 11. Что составляет свидетельства аудита СМИБ, согласно национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 27007—2014 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности»?

☐ область распространения СМИБ

☐ схема функциональной структуры

☐ бизнес-план организации

☐ **формулировка политики бизнеса, бизнес-процессы и виды деятельности ✔**

(один вариант)

Вопрос 12. Дополните понятие «свидетельство аудита», согласно национального стандарта Российской Федерации ГОСТ Р ИСО 19011-2021 «Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента». Свидетельство аудита – это записи, изложение фактов или другая информация, связанные с ____ _____ .

Ответ:

Решение: критериями аудита

Вопрос 13. На что направлено проведение внутреннего аудита ИБ?

Ответ:

Решение: на выявление внутренних проблем

Вопрос 14. Зависят ли цели программы аудита от идентифицированных требований информационной безопасности?

Ответ:

Решение: да

Вопрос 15. Что такое аттестация объекта информатизации на соответствие требованиям по защите информации?

○ Оценка соответствия продукции нормативам и требованиям

○ **Комплекс организационно-технических мероприятий, в результате которых подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации ✔**

○ Подтверждение соответствия требованиям, которые необходимы для оказания определенного вида услуг

○ Разработка перечня требований в определенной области деятельности

(один вариант)

Вопрос 16. Чем следует обладать лицу, осуществляющему управление программой аудита?

Ответ:

Решение: необходимой компетентностью.

Вопрос 17. Сколько существует видов аудита информационной безопасности?

Ответ:

Решение: два.

Вопрос 18. В чем важно удостовериться при оценке рисков ИБ?

Ответ:

Решение: рассматриваются все важные активы

Вопрос 19. Что должно быть установлено и продемонстрировано в ходе аудита?

- ☐ **Что СМИБ подвергается мониторингу и проверкам ✔**
- ☐ Что СМИБ существует
- ☐ Что СМИБ обновляется

(один вариант)

Вопрос 20. Что должен осуществить аудитор при оценке остаточных рисков информационной безопасности?

Ответ:

Решение: оценить остаточные риски информационной безопасности.

Вопрос 21. Какие могут быть последствия отсутствия аудита информационной безопасности?

Ответ:

Решение: утечка конфиденциальной информации

Вопрос 22. Как определено понятие «средство управления», согласно ГОСТ Р ИСО/МЭК 27000 «Информационные технологии - Методы и средства обеспечения безопасности - Системы менеджмента информационной безопасности – Общие сведения и словарь»?

Ответ:

Решение: Мероприятие, которое изменяет риск

Вопрос 23. Что включается в документ «Положение о применимости» СМИБ организации?

- ☐ **Применяемые цели контроля, меры и средства контроля и управления ✔**
- ☐ Бизнес-цели организации
- ☐ Требования к компетенциям сотрудников подразделения
- ☐ Требования к компетенциям высшего руководства организации

(один вариант)

Вопрос 24. Дополните предложение: Основные этапы аудита информационной безопасности включают в себя: планирование, сбор информации, ___ ____, выявление уязвимостей, разработку рекомендаций и формирование отчета

Ответ:

Решение: анализ данных

Вопрос 25. Кто имеет право осуществлять аттестацию объектов информатизации, согласно приказу ФСТЭК от 29.04.2021 №77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»?

Ответ:

Решение:

- ☐ Федеральные органы государственной власти
- ☐ **Все варианты верны ✓**
- ☐ Органы местного самоуправления

(один вариант)

Вопрос 26. На какие объекты информатизации распространяется требование об обязательной аттестации, согласно приказу ФСТЭК от 29.04.2021 №77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»?

Ответ:

Решение:

- ☐ **На государственные и муниципальные информационные системы ✓**
- ☐ На федеральные информационные системы
- ☐ На системы органов местного самоуправления

(один вариант)

Вопрос 27. Что подлежит обязательной сертификации в системе сертификации ФСТЭК, согласно приказу ФСТЭК от 03.04.2018 №55 «Об утверждении положения о системе сертификации средств защиты информации»?

- ☐ **Средства технической защиты информации, включая средства, в которых они реализованы, а также средства контроля эффективности технической защиты информации ✔**
- ☐ Операционные системы
- ☐ Прикладное программное обеспечение

(один вариант)

Вопрос 28. Дополните понятие аттестат соответствия требованиям по защите информации. Аттестат соответствия – это документ, который подтверждает, что информационная система ___ ____ безопасности информации

Ответ:

Решение: соответствует требованиям

Вопрос 29. Кто может приостановить действие аттестата соответствия требованиям по защите информации?

Ответ:

Решение: ФСТЭК России.

Вопрос 30. На какой срок выдается аттестат соответствия требованиям по защите информации, согласно приказу ФСТЭК от 29.04.2021 №77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»?

Ответ:

Решение: на весь срок эксплуатации