Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра вычислительной техники
Кафедра экономической информатики

Паспорт зачета

по дисциплине «Информационная безопасность», 3 семестр

1. Методика оценки

Зачет проводится в тестам. Тестовое задание во время зачета формируется по следующему правилу: проверочные вопросы открытого и закрытого типа предлагаются в случайном порядке(список вопросов приведен ниже). Для закрытых вопросов перечень вариантов ответов предлагается тоже в случайном порядке. В заключении зачета преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Пример теста для зачета

1. Принцип проектирования системы информационной безопасности, при котором в коллектив разработчиков включаются предполагаемые пользователи
   Правильный ответ: *Не секретность проектирования*

2. В качестве мер защиты в Интернет можно рекомендовать...(отметить пункты)
   Правильный ответ (несколько вариантов):
   Не открывать подозрительные вложения
   Сообщать свой пароль только друзьям
   Дублировать важные сведения
   Не отвечать на письма незнакомых адресатов
   Не пересылать непрошенные письма, даже , если они интересны
3. Метод защиты от несанкционированного доступа, при котором каждому пользователю присваивается шифр, вводится пароль, определяется перечень доступных для работы (полный доступ или просмотр) модулей, ведется протокол доступа
   Правильный ответ: *Авторизация доступа*
4. Группа методов закрытия (скрытия) информации, основанных на размещении данных внутри других, тривиальных данных: в звуке (AUDIO-файлы), в изображении (VIDEO-файлы) называется…
   Правильный ответ: *Стеганография*
5. Промежуток времени от момента, когда появляется возможность использовать уязвимость, и до того, когда она устраняется
   Правильный ответ: *Окно опасности*

2. Критерии оценки

- Ответ на тест считается **неудовлетворительным**, если студент при ответе на вопросы не выбрал правильный ответ для более, чем 49% вопросов
  оценка составляет 0 *баллов.*
- Ответ на тест засчитывается на **пороговом** уровне, если студент суммарно набрал не менее 50 % баллов. Оценка составляет 10-15 *баллов.*

- Ответ на тест засчитывается на **базовом** уровне, если студент суммарно набрал не менее 90 % баллов,
  оценка составляет 16-19 *баллов.*
- Ответ на тест билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы суммарно набрал 100 % баллов, ответил на дополнительные вопросы
  оценка составляет 20 *баллов.*

3. Шкала оценки

Итоговая оценка ECTS складывается из баллов за продуктивное посещение лекций (10 баллов), лабораторные работы (34 баллов), баллов за выполнение РГЗ (36 баллов), баллов за тест (20) .

В общей оценке по дисциплине баллы учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе (см. таблицу) дисциплины.

Таблица – Оценка ECTS

Сумма набранных баллов	Оценка по шкале ECTS	Итог
100-97	A+	Зачтено
96-93	A	
92-89	A-	
88-84	B+	
83-80	B	
79-76	B-	
75-72	C+	
71-70	C	
69-65	C-	
64-58	D+	
57-50	D	
49-40	D–	Не зачтено
39-35	E	
34-30	FX	
29-0	F	

4. Вопросы к зачету по дисциплине «Информационная безопасность»

1) Характеристика каналов утечки информации на объекте.
2) Основные принципы создания систем ИБ и цели их реализации.
3) Общая технология проведения инвентаризации информационной системы для анализа состояния информационной информации.
4) Классификация категорий объектов информационной системы по результатам инвентаризации: уровни доступности, целостности, конфиденциальности.
5) Поддержка информационной безопасности для различных классов объектов. Основные виды работ, исполняемые роли.
6) Классификация методов защиты.
7) Характеристика, область применения и технология применения организационных средств защиты.
8) Характеристика, область применения и технология применения законодательных средств защиты.
9) Характеристика, область применения и технология применения аппаратных средств защиты.
10) Характеристика, область применения и технология применения технических средств защиты.
11) Характеристика, область и технология применения методов регламентации.
12) Характеристика, область и технология применения программных средств защиты.
13) Типовая технология установления подлинности пользователя.
14) Технология установления подлинности пользователя методом паролей.

15) Классификация методов и технология установления подлинности пользователя с использованием биометрических параметров человека.
16) Технология антивирусной защиты.
17) Классификация вредоносных программ.
18) Технология обнаружения и идентификации вирусов на компьютере.
19) Типовая технология установления полномочий пользователя.
20) Классификация и характеристика локальных атак.
21) Классификация и характеристика удаленных атак.
22) Методика оценки рисков при создании системы ИБ.
23) Технология шифрации и дешифрации (криптоанализа) в методе моноалфавитной и многоалфавитной подстановок. Стеганография.
24) Электронная цифровая подпись, технология и проблемы применения.
25) Технология защиты информации при передаче по каналам связи.