МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

"БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

УТВЕРЖДАЮ

Проректор по учебной работе

_____Е.И.Луковникова

26 февраля 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.24 Информационная безопасность

Закреплена за кафедрой **Информатики и прикладной математики**

Учебный план bz090302_20_ИСиТ.plx
Направление: 09.03.02 Информационные системы и технологии

Квалификация **Бакалавр**

Форма обучения **заочная**

Общая трудоемкость **4 ЗЕТ**

Виды контроля на курсах:
Контрольная работа 5, Экзамен 5

Распределение часов дисциплины по курсам

Курс	5		Итого	
Вид занятий	УП	РП		
Лекции	12	12	12	12
Лабораторные	12	12	12	12
В том числе инт.	4	4	4	4
Итого ауд.	24	24	24	24
Контактная работа	24	24	24	24
Сам. работа	111	111	111	111
Часы на контроль	9	9	9	9
Итого	144	144	144	144

Программу составил(и):
к.т.н., доц., Сташок Ольга Владимировна Сташок
Рабочая программа дисциплины

Имитационное моделирование

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 09.03.02 Информационные системы и технологии (уровень бакалавриата) (приказ Минобрнауки России от 19.09.2017 г. № 926)
составлена на основании учебного плана:

Направление: 09.03.02 Информационные системы и технологии
утвержденного приказом ректора от 31.01.2020 протокол № 7.

Рабочая программа одобрена на заседании кафедры

Информатики и прикладной математики

Протокол от 21 февраля 2020 г. № 6

Срок действия программы: 2020 – 2021 уч.г.

Зав. кафедрой Горохов Денис Борисович

Председатель МКФ

доцент, к.т.н. Варданян М.А. 25 февраля 2020 г.

Ответственный за реализацию ОПОП _____ Горохов Д.Б.
(подпись) (ФИО)

Директор библиотеки _____ Сотник Т.Ю.
(подпись) (ФИО)

№ регистрации 214
(методический отдел)

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Обеспечение бакалавров опорными знаниями для выполнения научно-исследовательских работ и практических работ, связанных с широким набором вопросов защиты информации и организации систем информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.О.24
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Дисциплина Б1.В.ДВ.09.01 Теоретические основы информационной безопасности относится к элективной части и является дисциплиной по выбору.
2.1.2	Теория вероятностей и математическая статистика
2.1.3	Методы анализа предметной области
2.1.4	Операционные системы
2.1.5	Правоведение
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Выполнение и защита выпускной квалификационной работы
2.2.2	Основы процессов внедрения информационных систем
2.2.3	Проектирование информационных систем
2.2.4	Производственная (преддипломная) практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-2: Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности;	
Индикатор 1	ОПК - 2.1. Знает современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности.
Индикатор 2	ОПК - 2.2. Умеет выбирать современные информационные технологии и про-граммные средства, в том числе отечественного производства, при решении задач профессиональной деятельности.
Индикатор 3	ОПК - 2.3. Имеет навыки применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	
Индикатор 1	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профес-сиональной деятельности на основе информационной и библиографической культу-ры с применением информационно-коммуникационных технологий и с учетом ос-новных требований информационной безопасности.
Индикатор 2	ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информаци-онно-коммуникационных технологий и с учетом основных требований информаци-онной безопасности.
Индикатор 3	ОПК-3.3. Имеет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	- базовые направления обеспечения информационной безопасности предприятия; современные программные средства, в том числе отечественного производства, при решении задач обеспечения необходимого уровня информационной безопасности;
3.1.2	- технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;
3.1.3	- место и роль информационной безопасности в системе национальной без-опасности Российской Федерации;
3.1.4	- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области;
3.1.5	- базисные положения информационной безопасности, как отдельной области информационных технологий (ИТ); роль информационной безопасности, основные концептуальные положения систем защиты информации.
3.2	**Уметь:**

3.2.1	- разрабатывать способы защиты информации, и меры противодействия не-санкционированному доступу к источникам конфиденциальной информации;
3.2.2	- использовать современные ИТ и программные средства, при анализе защищенности ИС предприятия;
3.2.3	- самостоятельно анализировать и оценивать угрозы информационной безопасности; выделять основания и объекты защиты информации;
3.2.4	- анализировать и оценивать угрозы информационной безопасности объекта;
3.2.5	- правильно применять современные средства информационной безопасности отечественных и зарубежных производителей.
3.2.6	- определять основания и процедуру осуществления защиты информации;
3.2.7	- использовать меры административного, законодательного, процедурного, инженерно-технического уровней безопасности информации, применять в системах защиты информации.
3.3	**Владеть:**
3.3.1	- построения средств противодействия угрозам;
3.3.2	- применения приемов разработки концептуальных моделей информационной безопасности предприятия;
3.3.3	- организации работы с программными средствами безопасности, навыками управления сервисами безопасности в составе ИС;
3.3.4	- формирования требований по защите информации;
3.3.5	- выявления угроз безопасности автоматизированным системам.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Вид занятия	Наименование разделов и тем	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел	**Раздел 1. Структура теории компьютерной безопасности.**						
1.1	Лек	Основные понятия теории компьютерной безопасности.	5	1	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	0	ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК 3.3
1.2	Лаб	Основные понятия теории компьютерной безопасности.	5	1	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	0	ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК 3.3
1.3	Ср	Основные понятия теории компьютерной безопасности.	5	1	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	0	ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК 3.3
1.4	Лек	Методология построения защищенных автоматизированных систем.	5	5	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	0	ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК 3.3
1.5	Лаб	Методология построения защищенных автоматизированных систем.	5	2	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	2	работа в малых группах ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК 3.3

1.6	Ср	Методология построения защищенных автоматизированных систем.	5	30	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	0	ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК 3.3
1.7	Экзамен	Методология построения защищенных автоматизированных систем.	5	3	ОПК-2 ОПК-3	Л1.2Л2.1Л3.1	0	ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК 3.3
1.8	Контр.раб.	Методология построения защищенных автоматизированных систем.	5	2	ОПК-2 ОПК-3	Л1.2Л2.1Л3.1	0	ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК 3.3
	Раздел	**Раздел 2. Основные критерии защищенности автоматизированных систем. Классы защищенности автоматизированных систем.**						
2.1	Лек	Политика безопасности.	5	5	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	0	ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК 3.3
2.2	Лаб	Политика безопасности.	5	4	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	0	ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК 3.3
2.3	Ср	Политика безопасности.	5	40	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	0	ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК 3.3
2.4	Лек	Стандарты в области информационной безопасности.	5	1	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	2	лекция - беседа ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК 3.3
2.5	Лаб	Стандарты в области информационной безопасности.	5	5	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	0	ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК 3.3
2.6	Ср	Стандарты в области информационной безопасности.	5	40	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2	0	ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК 3.3

2.7	Контр.раб.	Политика безопасности.	5	1	ОПК-2 ОПК-3	Л1.2Л2.1Л3.1	0	ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК 3.3
2.8	Экзамен	Политика безопасности.	5	3	ОПК-2 ОПК-3	Л1.2Л2.1Л3.1	0	ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК 3.3

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии с использованием активных методов обучения (лекция – беседа, лекция – дискуссия, проблемная лекция, лекция-визуализация, лекция с заранее запланированными ошибками, лекция – пресс-конференция, лекция с разбором конкретных ситуаций, лекция-консультация, занятия с применением затрудняющих условий, методы группового решения творческих задач, метод развивающейся кооперации)

Технология коллективного взаимодействия (работа в малых группах) (самостоятельное изучение обучающимися нового материала посредством сотрудничества в малых группах, дает возможность всем участникам участвовать в работе, практиковать навыки сотрудничества, межличностного общения)

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Контрольные вопросы и задания

ВОПРОСЫ К ЭКЗАМЕНУ
1.Анализ угроз информационной безопасности.
2.Модели ценности информации.
3.Построение систем защиты от угрозы нарушения конфиденциальности информации.
4.Построение систем защиты от угрозы нарушения целостности информации.
5.Модель безопасности Харрисона-Руззо-Ульмана, распространение прав доступа.
6.Модель безопасности Белла-Лападулы, распространение прав доступа.
7.Стандарт оценки безопасности компьютерных систем TCSEC.
8.Стандарт оценки безопасности компьютерных систем Гостехкомиссии РФ.
9.Основные понятия теории компьютерной безопасности.
10.Реализация парольной защиты.
11.Политика безопасности.
12.Мандатная политика разграничения доступа.
13.Единые критерии безопасности информационных технологий.
14.Ценность информации.
15.Построение системы защиты от угрозы раскрытия параметров информационной системы.
16.Классификация защищенности ОС семейства *Nix.

6.2. Темы письменных работ

6.3. Фонд оценочных средств

Задания для контрольной работы
Задание № 1
Вопрос:
Информационная безопасность - это комплекс мероприятий, обеспечивающий для охватываемой им информации следующие факторы:
Выберите несколько из 6 вариантов ответа:
1) конфиденциальность
2) целостность
3) доступность
4) учет
5) неотрекаемость
6) мобильность
Задание № 2
Вопрос:
Сопоставьте понятия и их определения.
Укажите соответствие для всех 5 вариантов ответа:
1) возможность ознакомиться с информацией имеют в своем распоряжении только те лица, кто владеет соответствующими полномочиями.
2) возможность внести изменение в информацию должны иметь только те лица, кто на это уполномочен.
3) возможность получения авторизованного доступа к информации со стороны уполномоченных лиц в соответствующий

санкцианированный для работы период времени.
4) все значимые действия лица, выполняемые им в рамках, контролирумых системой безопасности, должны быть зафиксированы и проанализированы.
5) лицо, направившее информацию другому лицу, не может отречься от факта направления информации, а лицо, получившее информацию, не может отречься от факта ее получения.
__ конфиденциальность
__ целостность
__ доступность
__ учет
__ неотрекаемость

Задание № 3
Вопрос:
... - это набор формальных правил, которые регламентируют функционирование механизма информационной безопасности.
Выберите один из 5 вариантов ответа:
1) Политика
2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация

Задание № 4
Вопрос:
... - распознавание каждого участника процесса информационного взаимодействия перед тем, как к нему будут применены какие бы то ни было понятия информационной безопасности.
Выберите один из 5 вариантов ответа:
1) Политика
2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация

Задание № 5
Вопрос:
... - обеспечение уверенности в том, что участник процесса обмена информацией определен верно, т.е. действительно является тем, чей идентификатор он предъявил.
Выберите один из 5 вариантов ответа:
1) Политика
2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация

Задание № 6
Вопрос:
... - создание и поддержание набора правил, определяющих каждому участнику процесса информационного обмена разрешение на доступ к ресурсам и уровень этого доступа.
Выберите один из 5 вариантов ответа:
1) Политика
2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация

Задание № 7
Вопрос:
... - формирование профиля прав для конкретного участника процесса информационного обмена из набора правил контроля доступа.
Выберите один из 5 вариантов ответа:
1) Политика
2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация

Задание № 8
Вопрос:

... - обеспечение соответствия возможных потерь от нарушения информационной безопасности затратам на их построение.
Выберите один из 5 вариантов ответа:
1) Реагирование на инциденты
2) Управление конфигурацией
3) Управление пользователями
4) Управление рисками
5) Обеспечение устойчивости

Задание № 9
Вопрос:
... - поддержание среды информационого обмена в минимально допустимом работоспособном состоянии и сооответствии требованиям информационной безопасности в услових деструктивны внешних или внутренних воздействий.
Выберите один из 5 вариантов ответа:
1) Реагирование на инциденты
2) Управление конфигурацией
3) Управление пользователями
4) Управление рисками
5) Обеспечение устойчивости

Задание № 10
Вопрос:
... - совокупность процедур или мероприятий, которые производятся при нарушении или подозрении на нарушение информационой безопасности.
Выберите один из 5 вариантов ответа:
1) Реагирование на инциденты
2) Управление конфигурацией
3) Управление пользователями
4) Управление рисками
5) Обеспечение устойчивости

Задание № 11
Вопрос:
Перечислите основные направления информационной безопасности.
Выберите несколько из 4 вариантов ответа:
1) Физическая безопасность
2) Компьютерная безопасность
3) Визуальная безопасность
4) Сензитивная безопасность

Задание № 12
Вопрос:
Перечислите состав службы информационной безопасности.
Выберите несколько из 6 вариантов ответа:
1) Руководитель службы
2) Операционный отдел
3) Исследовательский отдел
4) Методический отдел
5) Отдел общения с прессой
6) Отдел бухгалтерии

Задание № 13
Вопрос:
Составление списка объектов, которые будут подлежать защите, и субъектов, которые задействованы в данном информационном пространстве, и будут влиять на информационную защиту системы, - это ...

Запишите ответ:
_____

Задание № 14
Вопрос:
Критериями определения уровня безопасности систем являются:
Выберите несколько из 5 вариантов ответа:
1) Оранжевая книга
2) Красная книга
3) Зеленая книга
4) Серо-буромалиновая книга
5) Белая книга

Задание № 15
Вопрос:
... - выпущенные Министерством обороны США критерии оценки уровня безопасности компьютерных систем.
Выберите один из 5 вариантов ответа:
1) Оранжевая книга
2) Красная книга
3) Белая книга
4) Зеленая книга
5) Открытая книга

Задание № 16
Вопрос:
... - выпущенные Министерством обороны США расширение критериев оценки уровня безопасности компьютерных систем для случаев использования компьютерных систем в информационной сети.
Выберите один из 5 вариантов ответа:
1) Оранжевая книга
2) Красная книга
3) Белая книга
4) Зеленая книга
5) Открытая книга

Задание № 17
Вопрос:
Перечислите модели классификации информационных объектов.
Выберите несколько из 5 вариантов ответа:
1) По наличию
2) По несанкционированной модификации (целостность)
3) По разглашению
4) По принадлежности
5) По аппелируемости

Задание № 18
Вопрос:
Какой считается информация, по классификации информационных объектов, если без нее можно работать, но очень короткое время.
Выберите один из 6 вариантов ответа:
1) критической
2) очень важной
3) важной
4) полезной
5) несущественной
6) вредной

Задание № 19
Вопрос:
Какой считается информация, по классификации информационных объектов, если без нее можно работать, но ее использование экономит ресурсы.
Выберите один из 6 вариантов ответа:
1) критической
2) очень важной
3) важной
4) полезной
5) несущественной
6) вредной

Задание № 20
Вопрос:
Какой считается по классификации информационных объектов устаревшая или неиспользуемая информация, не влияющая на работу субъекта.
Выберите один из 6 вариантов ответа:
1) критической
2) очень важной
3) важной
4) полезной
5) несущественной
6) вредной

Задание № 21

Вопрос:
Какой считается информация, по классификации информационных объектов, разглашение которой может принести моральный ущерб в очень редких случаях.
Выберите один из 6 вариантов ответа:
1) критической
2) очень важной
3) важной
4) значимой
5) малозначимой
6) незначимой

Задание № 22
Вопрос:
Какой считается информация, по классификации информационных объектов, если ее несанкционированное изменение скажется через некоторое время, но не приведет к сбою в работе субъекта, последствия модификации необратимы.
Выберите один из 6 вариантов ответа:
1) критической
2) очень важной
3) важной
4) значимой
5) малозначимой
6) незначимой

Задание № 23
Вопрос:
Жизненный цикл информации состоит из следующих стадий:
Выберите несколько из 4 вариантов ответа:
1) Информация используется в операционном режиме
2) Информация используется в архивном режиме
3) Информация хранится в архивном режиме
4) Информация хранится в операционном режиме

Задание № 24
Вопрос:
Какие существуют основные классы атак?
Выберите несколько из 5 вариантов ответа:
1) Локальная атака
2) Удаленная атака
3) Атака на поток данных
4) Атака фрикера
5) Распределенная атака

Задание № 25
Вопрос:
... - это случай, когда злоумышленник оказался непосредственно перед клавиатурой данного компьютера
Выберите один из 5 вариантов ответа:
1) Локальная атака
2) Удаленная атака
3) Атака на поток данных
4) Распределенная атака
5) Атака фрикера

Задание № 26
Вопрос:
... - это вариант атаки, когда злоумышленник не видит ту рабочую станцию, с которой он работает.
Выберите один из 5 вариантов ответа:
1) Локальная атака
2) Удаленная атака
3) Атака на поток данных
4) Рейдерская атака
5) Социальная инженерия

Задание № 27
Вопрос:
... - это вариант атаки, когда атакуемый компьютер активно отправляет, принимает или обменивается с данными с другими компьютерами сети, локальной или глобальной, а местом приложения атакующего воздействия является сегмент сети или сетевой узел между этими системами.
Выберите один из 5 вариантов ответа:

1) Локальная атака
2) Удаленная атака
3) Атака на поток данных
4) Рейдерская атака
5) Социальная инженерия

Задание № 28
Вопрос:
... - идейный борец за свободу информации, вторгающийся в чужие системы в основном из интереса, без прямой материальной заинтересованности.
Выберите один из 5 вариантов ответа:
1) Хакер
2) Кракер
3) Фрикер
4) Джокер
5) Анонимайзер

Задание № 29
Вопрос:
... - тот, кто взламывает чужие системы, преследуя собственный финансовый интерес.
Выберите один из 5 вариантов ответа:
1) Хакер
2) Кракер
3) Фрикер
4) Джокер
5) Анонимайзер

Задание № 30
Вопрос:
... - злоумышленник, использующий в собственных интересах уязвимости в телефонных системах.
Выберите один из 5 вариантов ответа:
1) Хакер
2) Кракер
3) Фрикер
4) Джокер
5) Анонимайзер

Задание № 31
Вопрос:
... - это набор мероприятий по сбору сведений об информационной системе, напрямую не связанный с техническими подробностями реализации системы, основанный на человеческом факторе.
Запишите ответ:
_____

Задание № 32
Вопрос:
... в аппаратном обеспечении -это устройство, которое выполняет некоторые недокументированные функции, обычно в ущерб пользователю данной информационной системы.
Запишите ответ:
_____

Задание № 33
Вопрос:
... - это устройство, хранящее некий уникальный параметр, на основе которого выдается корректный ответ на запрос системы об аутентификации.
Выберите один из 4 вариантов ответа:
1) Токен
2) Пароль
3) Биометрические параметры
4) Мастер-ключ

Задание № 34
Вопрос:
Выполнение пользователем, получившим доступ в систему, различных несанкционированных действий, называется атакой на ...
Запишите ответ:
_____

Задание № 35
Вопрос:
... - это программа, перехватывающая пакеты, поступающие к данной станции, в том числе и те, котрое станция при нормальной работе должна проигнорировать.
Запишите ответ:

_____

Задание № 36
Вопрос:
... позволяют провести анализ и пошаговое выполнение программного обеспечения с тем, чтобы понять его внутреннюю логику и уязвимость или вызвать в его работе сбой с предсказуемым результатом, либо изменить ход работы программы в свою пользу.
Выберите один из 4 вариантов ответа:
1) Дизассемблеры
2) Программы повышения прав
3) Атаки на переполнение буфера
4) Программы подбора паролей

6.4. Перечень видов оценочных средств

Индивидуальное задание
Экзаменационный билет

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л1.1	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014	0	
Л1.2	Нестеров С. А.	Основы информационной безопасности: учебное пособие	Санкт-Петербург: Издательство Политехнического университета, 2014	1	http://biblioclub.ru/index.php?page=book&id=363040

7.1.2. Дополнительная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л2.1	Виноградова С.М., Войтович Н.А, Вус М.А.	Информационное общество. Информационные войны. Информационное управление. Информационная безопасность: учебное пособие	Санкт-Петербург: Изд-во Санкт-Петербургского ун-та, 1999	2	
Л2.2	Артемов А.А.	Информационная безопасность	Орел: МАБИВ, 2014	0	

7.1.3. Методические разработки

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л3.1	Бабаш А.В., Баранова Е.К., Мельников Ю.Н.	Информационная безопасность. Лабораторный практикум: учебное пособие	Москва: Кнорус, 2012	10	
Л3.2	Сычев Ю.Н.	Основы информационной безопасности	Москва: Евразийский открытый институт, 2010	0	

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	«Университетская библиотека online»

7.3.1 Перечень программного обеспечения

7.3.1.1	Microsoft Windows Professional 7 Russian Upgrade Academic OPEN No Level

7.3.1.2	Microsoft Office 2007 Russian Academic OPEN No Level
7.3.1.3	Microsoft Office Professional Plus 2010 Russian Academic OPEN 1 license No Level

7.3.2 Перечень информационных справочных систем

7.3.2.1	Издательство "Лань" электронно-библиотечная система
7.3.2.2	«Университетская библиотека online»
7.3.2.3	Электронный каталог библиотеки БрГУ
7.3.2.4	Электронная библиотека БрГУ

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

А1207	Лаборатория технических средств защиты информации	Учебная мебель Персональный компьютер i5-2500/H67/4Gb/500Gb(Монитор TFT19 Samsung E1920NR), интерактивная доска SMART Board X885ix со встроенным проектором UX 60,комплекс учебно-лабораторного оборудования “Технические средства и методы защиты информации”,управляемый коммутатор 2 уровня D-Link DES-3028.
А1303	Лекционная аудитория	Учебная мебель
2201	читальный зал №1	Учебная мебель Оборудование 10- ПК i5-2500/H67/4Gb (монитор TFT19 Samsung); принтер HP Laser Jet P2055D

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина призвана обеспечить раскрытие сущности и значения информационной безопасности и защиты информации, их места в системе национальной безопасности; определения теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации; классификации и характеристики составляющих информационной безопасности и защиты информации; установления взаимосвязи и логической организации входящих в 15 них компонентов:

- ознакомление с понятийным аппаратом в области информационной безопасности и защиты информации;
- рассмотрение базовых содержательных положений в области информационной безопасности и защиты информации;
- изучение современной доктрины информационной безопасности;
- определение целей и принципов защиты информации; установление факторов, влияющих на защиту информации;
- ознакомление с составом защищаемой информации, ее классификацией по видам тайны, материальным носителям, собственникам и владельцам;
- установление структуры угроз защищаемой информации;
- рассмотрение направлений, видов, методов и особенностей деятельности разведывательных органов по добыванию конфиденциальной информации;
- определение сущности компонентов защиты информации;
- определение назначения, сущности и структуры систем защиты информации.

Программа раскрывает содержание курса, определяет последовательность усвоения знаний и структуру смысловых связей в рамках изучаемого предмета.