ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Утверждено:
на заседании кафедры
протокол№ 8 от « 24 » февраля 2021 г.
Зав. кафедрой _____ /Исмагилова А.С.

Согласовано:
Председатель УМК института
_____ / Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина
Расследование инцидентов информационной безопасности
Б1.В.ДВ.02.01
программа специалитета

Специальность
10.05.05 Безопасность информационных технологий в правоохранительной сфере

Профиль подготовки
Организация и технологии защиты информации

Квалификация
специалист

Разработчик (составитель)
к.ф.-м.н., доцент _____ /И.А. Шагапов

Для приема: 2021 г.

Уфа – 2021

Составитель: доцент Шагапов Илдар Ахняфович

Рабочая программа дисциплины утверждена на заседании кафедры, протокол № 8 от «24» февраля 2021 г.

Дополнения и изменения, внесенные в программу практики, утверждены на заседании ученого совета института истории и государственного управления:
_____
_____
_____

Директор _____ А.И. Уразова

Дополнения и изменения, внесенные в программу практики, утверждены на заседании ученого совета института истории и государственного управления:
_____
_____
_____

Директор _____ А.И. Уразова

Дополнения и изменения, внесенные в программу практики, утверждены на заседании ученого совета института истории и государственного управления:
_____
_____
_____

Директор _____ А.И. Уразова

Дополнения и изменения, внесенные в программу практики, утверждены на заседании ученого совета института истории и государственного управления:
_____
_____
_____

Директор _____ А.И. Уразова

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

В результате освоения образовательной программы обучающийся должен овладеть следующими результатами обучения по дисциплине:

Категория (группа) компетенций (при наличии ОПК)	Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
	УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.1 Знать методы организации работы команды для достижения поставленной цели	Знает методы организации работы команды для достижения поставленной цели
		УК-3.2 Уметь организовать работу команды и выработать стратегию для достижения поставленной цели	Умеет организовать работу команды и выработать стратегию для достижения поставленной цели
		УК-3.3 Владеть основными методами организации и руководства работы команды, вырабатывая командную стратегию для достижения поставленной цели	Владеет основными методами организации и руководства работы команды, вырабатывая командную стратегию для достижения поставленной цели
	ПК-2 Способен проводить мероприятия по оценке защищенности компьютерных систем и сетей	ПК-2.1 Знать основные мероприятия по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности	Знает основные мероприятия по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности
		ПК-2.2 Уметь проводить основные мероприятия по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности	Умеет проводить основные мероприятия по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности
		ПК-2.3 Владеть технологией проведения мероприятий по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности	Владеет технологией проведения мероприятий по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Расследование инцидентов информационной безопасности» относится к группе дисциплин вариативной части образовательной программы.

Дисциплина изучается на 4 курсе в 7 семестре.

Целью учебной дисциплины «Расследование инцидентов информационной безопасности» является выработать навыки предотвращения и своевременного реагирования на инциденты

информационной безопасности.

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении 1.

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине

УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Критерии оценивания результатов обучения (зачет)**	
		«Незачтено»	«Зачтено»
УК-3.1 Знать методы организации работы команды для достижения поставленной цели	Знает методы организации работы команды для достижения поставленной цели	Не знает методы организации работы команды для достижения поставленной цели	Знает методы организации работы команды для достижения поставленной цели
УК-3.2 Уметь организовать работу команды и выработать стратегию для достижения поставленной цели	Умеет организовать работу команды и выработать стратегию для достижения поставленной цели	Не умеет организовать работу команды и выработать стратегию для достижения поставленной цели	Умеет организовать работу команды и выработать стратегию для достижения поставленной цели
УК-3.3 Владеть основными методами организации и руководства работы команды, вырабатывая командную стратегию для достижения поставленной цели	Владеет основными методами организации и руководства работы команды, вырабатывая командную стратегию для достижения поставленной цели	Не владеет основными методами организации и руководства работы команды, вырабатывая командную стратегию для достижения поставленной цели	Владеет основными методами организации и руководства работы команды, вырабатывая командную стратегию для достижения поставленной цели

ПК-2 Способен проводить мероприятия по оценке защищенности компьютерных систем и сетей

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Критерии оценивания результатов обучения (зачет)**	
		«Незачтено»	«Зачтено»
ПК-2.1 Знать основные мероприятия по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности	Знает основные мероприятия по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности	Не знает основные мероприятия по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности	Знает основные мероприятия по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности

ПК-2.2 Уметь проводить основные мероприятия по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности	Умеет проводить основные мероприятия по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности	Не умеет проводить основные мероприятия по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности	Умеет проводить основные мероприятия по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности
ПК-2.3 Владеть технологией проведения мероприятий по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности	Владеет технологией проведения мероприятий по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности	Не владеет технологией проведения мероприятий по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности	Владеет технологией проведения мероприятий по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности

4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**
УК-3.1 Знать методы организации работы команды для достижения поставленной цели	Знает методы организации работы команды для достижения поставленной цели	Письменная контрольная работа 1,2,3,4
УК-3.2 Уметь организовать работу команды и выработать стратегию для достижения поставленной цели	Умеет организовать работу команды и выработать стратегию для достижения поставленной цели	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4
УК-3.3 Владеть основными методами организации и руководства работы команды, вырабатывая командную стратегию для достижения поставленной цели	Владеет основными методами организации и руководства работы команды, вырабатывая командную стратегию для достижения поставленной цели	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**
ПК-2.1 Знать основные мероприятия по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности	Знает основные мероприятия по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4
ПК-2.2 Уметь проводить основные мероприятия по оценке защищенности компьютерных систем и сетей в	Умеет проводить основные мероприятия по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4

рамках расследования инцидентов информационной безопасности ПК-2.3 Владеть технологией проведения мероприятий по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности	Владеет технологией проведения мероприятий по оценке защищенности компьютерных систем и сетей в рамках расследования инцидентов информационной безопасности	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4

Критериями оценивания при *модульно-рейтинговой системе* являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (*для экзамена:* текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10; *для зачета:* текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
не зачтено – от 0 до 59 рейтинговых баллов)

Рейтинг – план дисциплины

Расследование инцидентов информационной безопасности

Направление подготовки 10.05.05 БИТвПС

Курс 4, семестр 7

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1.				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №1	10	1	0	10
2. Практическая работа №2	10	1	0	10
Рубежный контроль				
1. Письменная контрольная работа №1	10	1	0	10
1. Письменная контрольная работа №2	10	1	0	10
Всего				50
Модуль 2.				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №3	10	1	0	10
2. Практическая работа №4	10	1	0	10
Рубежный контроль				
1. Письменная контрольная работа №3	10	1	0	10
1. Письменная контрольная работа №4	10	1	0	10
Всего				50

Поощрительные баллы				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
Итоговый контроль				
Зачет				

Практическая работа №1

Проектирование структуры службы защиты информации

Цель - спроектировать структуру службы защиты информации

Задание.

1. Спроектировать службу информационной безопасности предприятия информационного объекта и коротко описать функциональные обязанности по 4 (на выбор) из представленных должностей.

Функциональные подразделения и должностные лица
1. Директор
2. Начальник службы защиты информации
3. Аналитик
4. Юрист
5. Сотрудники сектора обеспечения безопасности, экономической разведки, промышленной контрразведки
6. Сотрудники сектора технической защиты
7 Сотрудники сектора охраны и режима
8. Администратор безопасности системы
9. Сотрудник группы безопасности.

2. Начертить структуру службы защиты информации.
3. Оформленный отчет о проделанной работе в электронном виде. Приветствуется использование фото, схем, таблиц и т.д.
4. Защитить работу.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены 50%	5
Выполнены 100%	10
Максимальный балл	10

Практическая работа №2

Организационные основы и принципы деятельности службы защиты информации

Задачи.

Цель – для конкретного информационного объекта определить задачи, функции

службы информационной безопасности

1. Перечислить:

– принципы службы информационной безопасности;

– функции деятельности службы;

– организационно-правовой статус службы безопасности;

– Разработать перечень задач для службы информационной безопасности для конкретного предприятия (см. Приложение), сформировать список защищаемой информации, угроз безопасности информации ;

– Определить функции отдела информационной безопасности для вашей организации;

– Перечислить общие принципы деятельности службы;

– Перечислить общие виды гарантий безопасности объектов защиты;

Приложение:

Транспортно экспедиционная компания Сфера деятельности:

- Международные грузоперевозки
- Железнодорожные грузоперевозки
- Таможенное оформление

Транспортно экспедиционная компания должна удовлетворять следующим требованием:

- Быстрая и четкая обработка поступающих заказов.
- Поиск и предоставления автотранспорта в заданные сроки.
- Неукоснительное соблюдение всех правил и условий транспортировки груза. Контроль за исполнение и информирование клиента о статусе перевозки груза.
- Формирование отчетности и прочих финансовых, сопроводительных документов.
- Строгое соблюдение законодательства.

2. Оформленный отчет о проделанной работе в электронном виде. Приветствуется использование фото, схем, таблиц и т.д.

3. Защитить работу.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены 50%	5
Выполнены 100%	10
Максимальный балл	10

Практическая работа №3

Организационные основы и принципы деятельности службы защиты информации. Пакет документов

Цель – разработать пакет нормативных документов, необходимых для работы службы защиты информации вашей организации

Задание

1. Перечислите документы, необходимые для обеспечения полноценной организационной и правовой защиты информации;
2. Приведите примеры дополнений необходимых документов, затрагивающих вопросы, связные с защитой информации;
3. Разработайте документы, необходимые для работы службы безопасности, ва-

шей организации.

- Оформленный отчет о проделанной работе в электронном виде. Приветствуется использование фото, схем, таблиц и т.д.

- Защитить работу.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены 50%	5
Выполнены 100%	10
Максимальный балл	10

Практическая работа №4

Организация информационно-аналитической работы

Цель – проанализировать организацию информационно-аналитической работы.

Задание.

1. Определить цели и задачи информационно-аналитической работы;
2. Определить направления аналитической работы;
3. Перечислить этапы выполнения информационно-аналитических исследований производственных ситуаций;
4. Определить методы выполнения аналитических исследований

- Оформить отчѐт.
- Защитить работу

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены 50%	5
Выполнены 100%	10
Максимальный балл	10

Письменная контрольная работа №1

Построить возможные сценарии инцидента неавторизованного доступа.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены 50%	5
Выполнены 100%	10
Максимальный балл	10

Письменная контрольная работа №2

Построить возможные сценарии инцидента отказа в обслуживании.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены 50%	5
Выполнены 100%	10

Максимальный балл	10

Письменная контрольная работа №3

Организация информационно-аналитической работы

Цель – проанализировать организацию информационно-аналитической работы.

Задание.

1. Определить цели и задачи информационно-аналитической работы;
2. Определить направления аналитической работы;
3. Перечислить этапы выполнения информационно-аналитических исследований производственных ситуаций;
4. Определить методы выполнения аналитических исследований

- Оформить отчѐт.
- Защитить работу

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены 50%	5
Выполнены 100%	10
Максимальный балл	10

Письменная контрольная работа №4

Разработка технического задания (ТЗ) на создание системы защиты информации предприятия

1. Изучить деятельность выбранного (гипотетически придуманного) предприятия.
2. Собрать необходимую информацию по предприятию.
3. Составить техническое задание на создание системы защиты информации предприятия.

Методические указания

а. Изучить ГОСТ по написанию ТЗ и образцы готовых вариантов.

б. Помнить, для чего и для кого разрабатывается ТЗ.

Теоретическая часть

Разработка программы: пример технического задания

1. Введение

1.1. Наименование программы

Наименование программы: "Тестовая программа"

1.2. Назначение и область применения

Программа предназначена для ...

2. Требования к программе

2.1. Требования к функциональным характеристикам

Программа должна обеспечивать возможность выполнения перечисленных ниже функций:

2.2. Требования к надежности

2.2.1 Требования к обеспечению надежного функционирования программы

Надежное (устойчивое) функционирование программы должно быть обеспечено выполнением Заказчиком совокупности организационно-технических мероприятий, перечень которых приведен ниже:

а) организацией бесперебойного питания технических средств;

б) использованием лицензионного программного обеспечения;

в) регулярным выполнением рекомендаций Министерства труда и социального развития

РФ, изложенных в Постановлении от 23 июля 1998 г.

Об утверждении межотраслевых типовых норм времени на работы по сервисному обслуживанию ПЭВМ и оргтехники и сопровождению программных средств»;

г) регулярным выполнением требований ГОСТ 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов

2.2.2. Время восстановления после отказа

Время восстановления после отказа, вызванного сбоем электропитания технических средств (иными внешними факторами), не фатальным сбоем (не крахом) операционной системы,

не должно превышать 30-ти минут при условии соблюдения условий эксплуатации технических и программных средств.

Время восстановления после отказа, вызванного неисправностью технических средств, фатальным сбоем (крахом) операционной системы, не должно превышать времени, требуемого на устранение неисправностей технических средств и переустановки программных средств.

2.2.3. Отказы из-за некорректных действий оператора

Отказы программы возможны вследствие некорректных действий оператора (пользователя) при взаимодействии с операционной системой.

Во избежание возникновения отказов программы по указанной выше причине следует обеспечить работу конечного пользователя без предоставления ему административных привилегий

3. Условия эксплуатации

3.1. Климатические условия эксплуатации

Климатические условия эксплуатации, при которых должны обеспечиваться заданные характеристики, должны удовлетворять требованиям,

предъявляемым к техническим средствам в части условий их эксплуатации

3.2. Требования к квалификации и численности персонала

Минимальное количество персонала, требуемого для работы программы, должно составлять не менее 2 штатных единиц — системный администратор и конечный пользователь программы — оператор.

Системный администратор должен иметь высшее профильное образование и сертификаты компании-производителя операционной системы. В перечень задач, выполняемых системным администратором, должны входить:

а) задача поддержания работоспособности технических средств;

б) задачи установки (инсталляции) и поддержания работоспособности системных программных средств — операционной системы;

в) задача установки (инсталляции) программы.

г) задача создания резервных копий базы данных.

3.3. Требования к составу и параметрам технических средств

3.3.1. В состав технических средств должен входить IBM-совместимый персональный компьютер (ПЭВМ), выполняющий роль сервера, включающий в себя:

3.3.1.1. процессор Pentium-2.0Hz, не менее;

3.3.1.2. оперативную память объемом, 1Гигабайт, не менее;

3.3.1.3. оперативную память объемом, 1Гигабайт, не менее;

3.3.1.4. операционную систему Windows 2000 Server или Windows 2003;

3.3.1.5. операционную систему Windows 2000 Server или Windows 2003;

3.3.1.6. Microsoft SQL Server 2000

3.4. Требования к информационной и программной совместимости

3.4.1. Требования к информационным структурам и методам решения

База данных работает под управлением Microsoft SQL Server. Используется много поточный доступ к базе данных. Необходимо обеспечить одновременную работу с программой с той же базой данной модулей экспорта внешних данных.

3.4.2. Требования к исходным кодам и языкам программирования

Дополнительные требования не предъявляются

3.4.3. Требования к программным средствам, используемым программой

Системные программные средства, используемые программой, должны быть представлены лицензионной локализованной версией операционной системы Windows 2000 Server или Windows 2003 и Microsoft SQL Server 2000

3.4.4. Требования к защите информации и программ

Требования к защите информации и программ не предъявляются

3.5. Специальные требования

Специальные требования к данной программе не предьявляются

4. Требования к программной документации

4.1. Предварительный состав программной документации

Состав программной документации должен включать в себя:

4.1.1. техническое задание;

4.1.2. программу и методики испытаний;

4.1.3. руководство оператора;

5. Технико-экономические показатели

5.1. Экономические преимущества разработки

Ориентировочная экономическая эффективность не рассчитываются. Аналогия не проводится ввиду уникальности предъявляемых требований к разработке.

6. Стадии и этапы разработки

6.1. Стадии разработки

Разработка должна быть проведена в три стадии:

1. разработка технического задания;

2. рабочее проектирование;

3. внедрение.

6.2. Этапы разработки

На стадии разработки технического задания должен быть выполнен этап разработки, согласования и утверждения настоящего технического задания.

На стадии рабочего проектирования должны быть выполнены перечисленные ниже этапы работ:

1. разработка программы;

2. разработка программной документации;

3. испытания программы.

На стадии внедрения должен быть выполнен этап разработки подготовка и передача программы

6.3. Содержание работ по этапам

На этапе разработки технического задания должны быть выполнены перечисленные ниже работы:

1. постановка задачи;

2. определение и уточнение требований к техническим средствам;

3. определение требований к программе;

4. определение стадий, этапов и сроков разработки программы и документации на неё;

5. согласование и утверждение технического задания.

На этапе разработки программы должна быть выполнена работа по программированию (кодированию) и отладке программы.

На этапе разработки программной документации должна быть выполнена разработка программных документов в соответствии с требованиями к составу документации.

На этапе испытаний программы должны быть выполнены перечисленные ниже виды работ:

1. разработка, согласование и утверждение и методики испытаний;

2. проведение приемо-сдаточных испытаний;

3. корректировка программы и программной документации по результатам испытаний.

На этапе подготовки и передачи программы должна быть выполнена работа по подготовке и передаче программы и программной документации в эксплуатацию на объектах Заказчика.

7. Порядок контроля и приемки

7.1. Виды испытаний

Приемо-сдаточные испытания должны проводиться на объекте Заказчика в оговоренные сроки.

Приемо-сдаточные испытания программы должны проводиться согласно разработанной Исполнителем и согласованной Заказчиком Программы и методик испытаний.

Ход проведения приемо-сдаточных испытаний Заказчик и Исполнитель документируют в Протоколе проведения испытаний

7.2. Общие требования к приемке работы

На основании Протокола проведения испытаний Исполнитель совместно с Заказчиком подписывает Акт приемки-сдачи программы в эксплуатацию.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1	5
Выполнены пункты 1-3	10
Максимальный балл	10

Перечень вопросов для зачета:

1. Формирование политики управления инцидентами ИБ. Основное содержание политики управления инцидентами ИБ.

2. Создание группы реагирования на инциденты ИБ. Цель создания. Роли группы реагирования на инциденты ИБ .

3. Подготовка к обработке инцидентов ИБ. Классификация инцидентов ИБ по значимости.

4. Обеспечение осведомленности и обучение управлению инцидентами. Цель осведомления об управлении инцидентами ИБ. Цель обучения управлению инцидентами ИБ.

5. Тестирование системы управления инцидентами ИБ.

6. Первичная оценка событий ИБ. Цель проведения первичной оценки. Последовательность действий при проведении первичной оценки.

7. Вторичная оценка инцидента ИБ. Цель проведения вторичной оценки. Последовательность действий при проведении вторичной оценки.

8. Сдерживание, устранение инцидента ИБ и восстановление после него.

9. Формирование и хранение свидетельств инцидентов ИБ.

10. Определение инцидента неавторизованного доступа. Цели инцидента неавторизованного доступа.

11. Определение инцидента отказа в обслуживании. Цели инцидента отказа в обслуживании. Примеры инцидентов отказа в обслуживании.

12. Определение инцидента сбора информации. Цели инцидента сбора информации.

13. Определение инцидента внедрения вредоносного кода. Средства реализации инцидента внедрения вредоносного кода. Цели инцидента.

14. Определение инцидента несоответствующего использования. Примеры инцидентов несоответствующего использования.

15. Стратегии управления непрерывностью функционирования АС для помещений и технологий.

16. Стратегии управления непрерывностью функционирования АС для данных.

17. Стратегии управления непрерывностью функционирования АС для поставщиков.

18. Стратегии управления непрерывностью функционирования АС для компьютеров.

19. Стратегии управления непрерывностью функционирования АС для серверов.

20. Стратегии управления непрерывностью функционирования АС для локальной сети.

21. Привести пример формы сообщения «Отчет о событии ИБ» сотрудника, обнаружившего нештатную ситуацию, имеющую отношение к ИБ.

22. Привести пример формы сообщения «Отчет об инциденте ИБ» сотрудника ГРИИБ, проводившего первичную оценку событий ИБ.

23. Привести пример матрицы для определения значимости инцидентов неавторизованного доступа.

24. Определить предвестники и указатели инцидентов неавторизованного доступа.

25. Определить меры по сдерживанию, устранению инцидентов неавторизованного доступа и восстановлению после них.

26. Привести пример матрицы для определения значимости инцидентов отказа в обслуживании.

27. Определить предвестники и указатели инцидентов отказа в обслуживании.

28. Определить меры по сдерживанию, устранению инцидентов отказа в обслуживании и восстановлению после них.

29. Привести пример матрицы для определения значимости инцидентов сбора информации3

30. Определить предвестники и указатели инцидентов сбора информации.

31. Определить меры по сдерживанию, устранению инцидентов сбора информации и восстановлению после них.

32. Привести пример матрицы для определения значимости инцидентов внедрения вредоносного кода.

33. Определить предвестники и указатели инцидентов внедрения вредоносного кода.

34. Определить меры по сдерживанию, устранению инцидентов внедрения вредоносного кода и восстановлению после них.

35. Привести пример матрицы для определения значимости инцидентов несоответствующего использования.

36. Определить предвестники и указатели инцидентов несоответствующего использования. Определить меры по сдерживанию, устранению инцидентов несоответствующего использования и восстановлению после них.

План лекционных занятий

(18 часов)

1. Формирование политики управления инцидентами ИБ. Основное содержание политики управления инцидентами ИБ. Создание группы реагирования на инциденты ИБ. Цель создания. Роли группы реагирования на инциденты ИБ . Подготовка к обработке инцидентов ИБ. Классификация инцидентов ИБ по значимости. Обеспечение осведомленности и обучение управлению инцидентами. Цель осведомления об управлении инцидентами ИБ. Цель обучения управлению инцидентами ИБ.Тестирование системы управления инцидентами ИБ.
2. Первичная оценка событий ИБ. Цель проведения первичной оценки. Последовательность действий при проведении первичной оценки. Вторичная оценка инцидента ИБ. Цель проведения вторичной оценки. Последовательность действий при проведении вторичной оценки.
3. Сдерживание, устранение инцидента ИБ и восстановление после него. Формирование и хранение свидетельств инцидентов ИБ. Определение инцидента неавторизованного доступа. Цели инцидента неавторизованного доступа. Определение инцидента отказа в обслуживании. Цели инцидента отказа в обслуживании. Примеры инцидентов отка-

за в обслуживании. Определение инцидента сбора информации. Цели инцидента сбора информации.

4. Определение инцидента внедрения вредоносного кода. Средства реализации инцидента внедрения вредоносного кода. Цели инцидента. Определение инцидента несоответствующего использования. Примеры инцидентов несоответствующего использования.
5. Стратегии управления непрерывностью функционирования АС для помещений и технологий. Стратегии управления непрерывностью функционирования АС для данных. Стратегии управления непрерывностью функционирования АС для поставщиков. Стратегии управления непрерывностью функционирования АС для компьютеров. Стратегии управления непрерывностью функционирования АС для серверов. Стратегии управления непрерывностью функционирования АС для локальной сети.
6. Матрицы для определения значимости инцидентов неавторизованного доступа. Предвестники и указатели инцидентов неавторизованного доступа. Меры по сдерживанию, устранению инцидентов неавторизованного доступа и восстановлению после них. Матрицы для определения значимости инцидентов отказа в обслуживании. Предвестники и указатели инцидентов отказа в обслуживании. Меры по сдерживанию, устранению инцидентов отказа в обслуживании и восстановлению после них.
7. Матрицы для определения значимости инцидентов сбора информации. Предвестники и указатели инцидентов сбора информации. Меры по сдерживанию, устранению инцидентов сбора информации и восстановлению после них. Матрицы для определения значимости инцидентов внедрения вредоносного кода. Предвестники и указатели инцидентов внедрения вредоносного кода. Меры по сдерживанию, устранению инцидентов внедрения вредоносного кода и восстановлению после них.
8. Матрицы для определения значимости инцидентов несоответствующего использования. Предвестники и указатели инцидентов несоответствующего использования. Меры по сдерживанию, устранению инцидентов несоответствующего использования и восстановлению после них.

Темы семинарских занятий

(36 часов)

1. Формирование политики управления инцидентами ИБ. Основное содержание политики управления инцидентами ИБ.

2. Создание группы реагирования на инциденты ИБ. Цель создания. Роли группы реагирования на инциденты ИБ .

3. Подготовка к обработке инцидентов ИБ. Классификация инцидентов ИБ по значимости.

4. Обеспечение осведомленности и обучение управлению инцидентами. Цель осведомления об управлении инцидентами ИБ. Цель обучения управлению инцидентами ИБ.

5. Тестирование системы управления инцидентами ИБ.

6. Первичная оценка событий ИБ. Цель проведения первичной оценки. Последовательность действий при проведении первичной оценки.

7. Вторичная оценка инцидента ИБ. Цель проведения вторичной оценки. Последовательность действий при проведении вторичной оценки.

8. Сдерживание, устранение инцидента ИБ и восстановление после него.

9. Формирование и хранение свидетельств инцидентов ИБ.

10. Определение инцидента неавторизованного доступа. Цели инцидента неавторизованного доступа.

11. Определение инцидента отказа в обслуживании. Цели инцидента отказа в обслуживании. Примеры инцидентов отказа в обслуживании.

12. Определение инцидента сбора информации. Цели инцидента сбора информации.

13. Определение инцидента внедрения вредоносного кода. Средства реализации инцидента внедрения вредоносного кода. Цели инцидента.

14. Определение инцидента несоответствующего использования. Примеры инцидентов несоответствующего использования.

15. Стратегии управления непрерывностью функционирования АС для помещений и технологий.

16. Стратегии управления непрерывностью функционирования АС для данных.

17. Стратегии управления непрерывностью функционирования АС для поставщиков.

18. Стратегии управления непрерывностью функционирования АС для компьютеров.

19. Стратегии управления непрерывностью функционирования АС для серверов.

20. Стратегии управления непрерывностью функционирования АС для локальной сети.

21. Привести пример формы сообщения «Отчет о событии ИБ» сотрудника, обнаружившего нештатную ситуацию, имеющую отношение к ИБ.

22. Привести пример формы сообщения «Отчет об инциденте ИБ» сотрудника ГРИИБ, проводившего первичную оценку событий ИБ.

23. Привести пример матрицы для определения значимости инцидентов неавторизованного доступа.

24. Определить предвестники и указатели инцидентов неавторизованного доступа.

25. Определить меры по сдерживанию, устранению инцидентов неавторизованного доступа и восстановлению после них.

26. Привести пример матрицы для определения значимости инцидентов отказа в обслуживании.

27. Определить предвестники и указатели инцидентов отказа в обслуживании.

28. Определить меры по сдерживанию, устранению инцидентов отказа в обслуживании и восстановлению после них.

29. Привести пример матрицы для определения значимости инцидентов сбора информации3

30. Определить предвестники и указатели инцидентов сбора информации.

31. Определить меры по сдерживанию, устранению инцидентов сбора информации и восстановлению после них.

32. Привести пример матрицы для определения значимости инцидентов внедрения вредоносного кода.

33. Определить предвестники и указатели инцидентов внедрения вредоносного кода.

34. Определить меры по сдерживанию, устранению инцидентов внедрения вредоносного кода и восстановлению после них.

35. Привести пример матрицы для определения значимости инцидентов несоответствующего использования.

36. Определить предвестники и указатели инцидентов несоответствующего использования. Определить меры по сдерживанию, устранению инцидентов несоответствующего использования и восстановлению после них.

Критерии оценки (в баллах) *(должны строго соответствовать рейтинг плану по макс. и мин. колич. баллов и только для тех, кто учится с использованием модульно-рейтинговой системы обучения и оценки успеваемости студентов):*

- 0,55 баллов выставляется студенту, если выполнил задание на 100%

- 0,36 баллов выставляется студенту, если выполнил задание на 75%

- 0,2 баллов выставляется студенту, если выполнил задание на 50%

- 0 баллов выставляется студенту, если не выполнил задание

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Лукаш, Ю.А. Контроль персонала как составляющая безопасности и развития бизнеса : учебное пособие / Ю.А. Лукаш. - 2-е изд., стер. - Москва : Издательство «Флинта», 2017. - 24 с. - ISBN 978-5-9765-1377-8 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=115078.

2. Милославская, Н.Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса : учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Москва : Горячая линия - Телеком, 2013. - 170 с. : ил. - (Вопросы управления информационной безопасностью. Вып. 3). - Библиогр. в кн. - ISBN 978-5-9912-0273-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253577.

Дополнительная литература:

1. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк ; Высшая Школа Экономики Национальный Исследовательский Университет. - Москва : Издательский дом Высшей школы экономики, 2015. - 574 с. : ил. - Библиогр. в кн. - ISBN 978-5-7598-0698-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=440285

2. Милославская, Н.Г. Технические, организационные и кадровые аспекты управления информационной безопасностью : учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Москва : Горячая линия - Телеком, 2013. - 216 с. : ил. - (Вопросы управления информационной безопасностью. Вып. 4). - Библиогр. в кн. - ISBN 978-5-9912-0274-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253578

3. Инструментальный контроль и защита информации : учебное пособие / Н.А. Свинарев, О.В. Ланкин, А.П. Данилкин и др. ; Министерство образования и науки РФ, ФГБОУ ВПО «Воронежский государственный университет инженерных технологий». - Воронеж : Воронежский государственный университет инженерных технологий, 2013. - 192 с. : табл., ил. - Библиогр. в кн. - ISBN 978-5-00032-018-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=255905

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы

1. Справочная правовая система «КонсультантПлюс» – http://www.consultant-plus.ru.
2. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
3. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
4. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
5. www.fstec.ru –сайт ФСТЭК России
6. www.fsb.ru – сайт ФСБ России
7. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
8. http://univertv.ru/video/matematika/ – Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);

9. www.newlibrary.ru – Новая электронная библиотека;
10. www. edu.ru – Федеральный портал российского образования;
11. www.elibrary.ru – Научная электронная библиотека;
12. www.nehudlit.ru – Электронная библиотека учебных материалов.
13. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
14. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
15. Система централизованного тестирования БашГУ (Moodle).GNU General Public License

6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения	
1. ***учебная аудитория для проведения занятий лекционного типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус). **2.** ***учебная аудитория для проведения лабораторных работ*****:** Лаборатория полигон технической защиты информации № 508 (гуманитарный корпус), компьютерный класс, аудитория 404 (гуманитарный корпус), аудитория 420 (гуманитарный корпус). **3.** ***учебная аудитория для проведения занятий семинарского типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитар-	Лекции, практические занятия, лабораторные занятия, групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным коротк-кофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTEL-Corei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMIC-MPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт APAPT MA1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт APAPT MA1225 – 1 шт. **Аудитория № 416**	1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные. 2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные. 3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License. Лицензии бессрочные.

ный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). **4.** ***учебная аудитория для проведения групповых и индивидуальных консультаций:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **5.** ***учебная аудитория для текущего контроля и промежуточной аттестации:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **6.** ***помещения для самостоятельной работы:*** читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус). **7.*помещение для хранения и профилактического обслуживания учебного оборудования:*** ауди-		Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран. **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 608** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 609** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 610** Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м. **Аудитория № 613** Учебная мебель, доска, моноблок стационарный – 15 шт. **Компьютерный класс аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Компьютерный класс аудитория № 404** Учебная мебель, компьютеры -15 штук. **Аудитория 402 читальный зал биб-**	

тория № 523 (гуманитарный корпус).		**лиотеки** Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные. **Лаборатория полигон технической защиты информации № 508** Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технической защиты информации, комплекс мониторинга WiFi сетей "Зодиак II", универсальный ком-плект инструментов для проведения работ по специальным провер-кам и специальным обследованиям Калейдоскоп-П2, многофункциональный поисковый прибор ST-031M "Пиранья", нелинейный локатор «Лорнет», анализатор электромагнитного поля "Кордон". **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.	

Приложение 1

МИНОБРНАУКИ РОССИИ
ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Содержание рабочей программы
дисциплины (7 семестр)

Вид работы	**Объем дисциплины**
Общая трудоемкость дисциплины (ЗЕТ / часов)	2 ЗЕТ / 72 часа
Учебных часов на контактную работу с преподавателем:	54,2
лекций	18
практических/ семинарских	36
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	17,8
Учебных часов на подготовку к зачету	

Форма контроля:
Зачет 7 семестр

7 семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / Сем	ЛР	СРС		
1	2	3	4	5	6	7	8
1	Формирование политики управления инцидентами ИБ. Основное содержание политики управления инцидентами ИБ. Создание группы реагирования на инциденты ИБ. Цель создания. Роли группы реагирования на инциденты ИБ . Подготовка к обработке инцидентов ИБ. Классификация инцидентов ИБ по значимости. Обеспечение осведомленности и обучение управлению инцидентами. Цель осведомления об управлении инцидентами ИБ. Цель обучения управлению инцидентами ИБ.Тестирование системы управления инцидентами ИБ.	2	4		2	Самостоятельное изучение рекомендуемых источников и материалов	Практическое задание Письменная контрольная работа
2	Первичная оценка событий ИБ. Цель проведения первичной оценки. Последовательность действий при проведении первичной оценки. Вторичная оценка инцидента ИБ. Цель проведения вторичной оценки. Последовательность действий при проведении вторичной оценки.	2	4		2	Самостоятельное изучение рекомендуемых источников и материалов	Практическое задание Письменная контрольная работа
3	Сдерживание, устранение инцидента ИБ и восстановление после него. Формирование и хранение свидетельств инцидентов ИБ. Определение инцидента неавторизованного доступа. Цели инцидента неавторизованного доступа. Определение инцидента отказа в обслуживании. Цели инцидента отказа в обслуживании. Примеры инцидентов отказа	2	4		2	Самостоятельное изучение рекомендуемых источников и материалов	Практическое задание Письменная контрольная работа

	в обслуживании. Определение инцидента сбора информации. Цели инцидента сбора информации.						
4	Определение инцидента внедрения вредоносного кода. Средства реализации инцидента внедрения вредоносного кода. Цели инцидента. Определение инцидента несоответствующего использования. Примеры инцидентов несоответствующего использования.	2	4		2	Самостоятельное изучение рекомендуемых источников и материалов	Практическое задание Письменная контрольная работа
5	Стратегии управления непрерывностью функционирования АС для помещений и технологий. Стратегии управления непрерывностью функционирования АС для данных. Стратегии управления непрерывностью функционирования АС для поставщиков. Стратегии управления непрерывностью функционирования АС для компьютеров. Стратегии управления непрерывностью функционирования АС для серверов. Стратегии управления непрерывностью функционирования АС для локальной сети.	2	4		2	Самостоятельное изучение рекомендуемых источников и материалов	Практическое задание Письменная контрольная работа
6	Матрицы для определения значимости инцидентов неавторизованного доступа. Предвестники и указатели инцидентов неавторизованного доступа. Меры по сдерживанию, устранению инцидентов неавторизованного доступа и восстановлению после них. Матрицы для определения значимости инцидентов отказа в обслуживании. Предвестники и указатели инцидентов отказа в обслуживании. Меры по сдерживанию, устранению инцидентов отказа в обслуживании и восстановлению после них.	2	4		2	Самостоятельное изучение рекомендуемых источников и материалов	Практическое задание Письменная контрольная работа

7	Матрицы для определения значимости инцидентов сбора информации. Предвестники и указатели инцидентов сбора информации. Меры по сдерживанию, устранению инцидентов сбора информации и восстановлению после них..	2	4		2	Самостоятельное изучение рекомендуемых источников и материалов	Практическое задание Письменная контрольная работа
8	Матрицы для определения значимости инцидентов внедрения вредоносного кода. Предвестники и указатели инцидентов внедрения вредоносного кода. Меры по сдерживанию, устранению инцидентов внедрения вредоносного кода и восстановлению после них	2	4		2	Самостоятельное изучение рекомендуемых источников и материалов	Практическое задание Письменная контрольная работа
9	Матрицы для определения значимости инцидентов несоответствующего использования. Предвестники и указатели инцидентов несоответствующего использования. Меры по сдерживанию, устранению инцидентов несоответствующего использования и восстановлению после них.	2	4		1.8	Самостоятельное изучение рекомендуемых источников и материалов	Практическое задание Письменная контрольная работа
	Итого	18	36		17,8		