МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Проректор по учебной работе

_____ С.Т. Князев
«___» _____ 2018 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

ОБНАРУЖЕНИЕ, ПРЕДУПРЕЖДЕНИЕ И ЛИКВИДАЦИЯ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК

Перечень сведений о рабочей программе модуля	**Учетные данные**
Модуль Обнаружение, предупреждение и ликвидация последствий компьютерных атак	**Код модуля** 1139532 Учебный план № 5347
Образовательная программа Компьютерная безопасность	**Код ОП** 10.05.01/01.02
Траектория образовательной программы (ТОП)	Не предусмотрена
Направление подготовки Компьютерная безопасность	**Код направления и уровня подготовки** 10.05.01
Уровень подготовки Специалитет	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО:** 1 декабря 2016 г., № 1512

Екатеринбург, 2018

Программа модуля составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Департамент	Подпись
1	Синадский Николай Игоревич	к.т.н., доцент	Доцент	Кафедра алгебры и фундаментальной информатики	
2	Баранский Виталий Анатольевич	д.ф.-м.н., профессор	Профессор	Кафедра алгебры и фундаментальной информатики	

Руководитель модуля В.А. Баранский

Рекомендовано учебно-методическим советом Института Математики и Компьютерных наук

Председатель учебно-методического совета А.Ю. Коврижных
Протокол № 12 от 15.12.2016 г.

Согласовано:

Дирекция образовательных программ Р. Х. Токарева

Руководитель ОП, для которой
реализуется модуль В.А. Баранский

ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ «ОБНАРУЖЕНИЕ, ПРЕДУПРЕЖДЕНИЕ И ЛИКВИДАЦИЯ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК»

1.1. Объем модуля, 8 з.е.

1.2. Аннотация содержания модуля

Модуль «Обнаружение, предупреждение и ликвидация последствий компьютерных атак» входит в состав базовой части и предполагает получение студентами компетенций по обнаружению, предупреждению и ликвидации последствий компьютерных атак на критическую информационную инфраструктуру Российской Федерации. В модуль входят следующие дисциплины: «Противодействие созданию и распространению вредоносных программ», «Системы обнаружения и предупреждения компьютерных атак», «Реагирование на компьютерные инциденты».

1. СТРУКТУРА МОДУЛЯ И РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ ПО ДИСЦИПЛИНАМ

Очная форма обучения

Наименования дисциплин с указанием, к какой части образовательной программы они относятся: базовой (Б), вариативной – по выбору вуза (ВВ), вариативной - по выбору студента (ВС).		Семестр изучения	Объем времени, отведенный на освоение дисциплин модуля							
			Аудиторные занятия, час.				Самостоятельная работа, включая все виды текущей аттестации, час.	Промежуточная аттестация (зачет, экзамен), час.	Всего по дисциплине	
			Лекции	Практические занятия	Лабораторные работы	Всего			Час.	Зач. ед.
1.	**(Б)** Противодействие созданию и распространению вредоносных программ	10		34		34	70	З(4).	108	3
2.	**(Б)** Системы обнаружения и предупреждения компьютерных атак	9	17	17		34	34	З(4)	72	2
3.	**(Б)** Реагирование на компьютерные инциденты	9	34	34		68	36	З(4)	108	3
			51	**85**		**136**	**140**	**12**	**288**	**8**

2. ПОСЛЕДОВАТЕЛЬНОСТЬ ОСВОЕНИЯ ДИСЦИПЛИН В МОДУЛЕ

3.1.	**Пререквизиты и постреквизиты в модуле**	1 Системы обнаружения и предупреждения компьютерных атак; Реагирование на компьютерные инциденты 2 Противодействие созданию и распространению вредоносных программ
3.2.	**Кореквизиты**	1 Системы обнаружения и предупреждения компьютерных атак 2 Реагирование на компьютерные инциденты

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ МОДУЛЯ

3.1. Планируемые результаты освоения модуля и составляющие их компетенции

Коды ОП, для которых реализуется модуль	**Планируемые в ОХОП результаты обучения -РО, которые формируются при освоении модуля**	**Компетенции в соответствии с ФГОС ВО, а также дополнительные из ОХОП, формируемые при освоении модуля**
10.05.01/01.02	РО-03 Способность осуществлять проектирование систем защиты информации с учётом актуальных информационных угроз и с использованием современных достижений науки и техники.	ПК-5, способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах;
	РО-04 Способность обеспечивать защищенность и функциональность компьютерных систем, производить их администрирование и профилактику работоспособности.	ПК-5, способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; ПК-10, способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства

		криптографической защиты информации; ПК-12, способностью проводить инструментальный мониторинг защищенности компьютерных систем; ПК-18, способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; ПК-20, способность выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций; ДПК-5, способность восстанавливать работоспособность систем защиты при сбоях и нарушении функционирования;
	РО-06 Способность осуществлять планирование работ по защите информации в компьютерных системах.	ПК-5, способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; ПСК-2.2, способностью на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах;
	РО-07 Способность проводить аудит и аттестацию объектов, обеспечивающих информационную безопасность, на соответствие требованиям государственных и/или корпоративных документов, а также устанавливать режим информационной безопасности на предприятии и контролировать его соблюдение.	ПК-3, способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности; ДПК-3, способность проводить аудит информационной безопасности и составлять итоговые документы аудита, содержащие выводы и рекомендации.
	РО-08 Способность к разработке, анализу и обоснованию адекватности математических моделей процессов, возникающих при функционировании программно-аппаратных средств защиты	ПК-5, способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства

	информации, а также к разработке математических моделей для оценки безопасности компьютерных систем.	криптографической защиты информации; ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах;

4.2 Распределение формирования компетенций по дисциплинам модуля

Дисциплины модуля		ПК-3	ПК-5	ПК-10	ПК-12	ПК-18	ПК-20	ПСК-2.2	ДПК-3	ДПК-5
1	**(Б)** Противодействие созданию и распространению вредоносных программ		*	*		*				
2	**(Б)** Системы обнаружения и предупреждения компьютерных атак	*		*	*			*	*	
3	**(Б)** Реагирование на компьютерные инциденты						*			*

5. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО МОДУЛЮ

5.1. Весовой коэффициент значимости промежуточной аттестации по модулю:
Не предусмотрен

5.2. Форма промежуточной аттестации по модулю:
Не предусмотрена.

5.3. Фонд оценочных средств для проведения промежуточной аттестации по модулю (Приложение 1)

ПРИЛОЖЕНИЕ 1
к рабочей программе модуля

5.3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

5.3.1. ОБЩИЕ КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

Система критериев оценивания результатов обучения в рамках модуля опирается на три уровня освоения: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

5.3.2. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

5.3.2.1. Перечень примерных вопросов для интегрированного экзамена по модулю
Не предусмотрен
5.3.2.2. Перечень примерных тем итоговых проектов по модулю
Не предусмотрен.

6. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В РАБОЧЕЙ ПРОГРАММЕ МОДУЛЯ

Номер листа изменений	Номер протокола заседания проектной группы модуля	Дата заседания проектной группы модуля	Всего листов в документе	Подпись руководителя проектной группы модуля

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ПРОТИВОДЕЙСТВИЕ СОЗДАНИЮ И РАСПРОСТРАНЕНИЮ ВРЕДОНОСНЫХ ПРОГРАММ

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль Обнаружение, предупреждение и ликвидация последствий компьютерных атак	**Код модуля** 1139532 Учебный план № 5347
Образовательная программа Компьютерная безопасность	**Код ОП** 10.05.01/01.02
Траектория образовательной программы (ТОП)	Не предусмотрена
Направление подготовки Компьютерная безопасность	**Код направления и уровня подготовки** 10.05.01
Уровень подготовки Специалитет	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО:** 1 декабря 2016 г., № 1512

Екатеринбург, 2018

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Департамент/ кафедра	Подпись
1	Синадский Николай Игоревич	к.т.н., доцент	Доцент	Кафедра алгебры и фундаментальной информатики	
2	Бакланов Валентин Викторович	к.т.н., доцент	Доцент	Департамент радиоэлектроники и связи	

Руководитель модуля В.А. Баранский

Рекомендовано учебно-методическим советом Института Математики и Компьютерных наук

Председатель учебно-методического совета А.Ю. Коврижных
Протокол № 12 от 15.12.2016 г.

Согласовано:

Дирекция образовательных программ Р. Х. Токарева

Руководитель ОП, для которой
реализуется модуль В.А. Баранский

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «ПРОТИВОДЕЙСТВИЕ СОЗДАНИЮ И РАСПРОСТРАНЕНИЮ ВРЕДОНОСНЫХ ПРОГРАММ»

1.1.Аннотация содержания дисциплины

Дисциплина входит в состав базового модуля «Обнаружение, предупреждение и ликвидация последствий компьютерных атак», изучается в нем последней.

Изучаются основополагающие принципы защиты компьютерной информации от вредоносных программ, возможности и отличительные признаки различных видов вредоносных программ для ЭВМ, порядок применения антивирусного программного обеспечения.

1.2. Язык реализации программы – *русский*

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

- ПК-5, способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;
- ПК-10, способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;
- ПК-18, способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

В результате освоения дисциплины студент должен:

Знать:

- классификацию вредоносных программ и компонентов информационного оружия;
- основные термины и определения в сфере противодействия вредоносным программам;
- признаки опасности и вредоносности компьютерных программ;
- требования по разработке и применению антивирусных средств;
- организацию работы подразделений антивирусной защиты;
- порядок извлечения и передачи на исследование вредоносных программ;
- возможности и отличительные признаки различных видов вредоносных программ для ЭВМ;
- порядок применения антивирусного программного обеспечения;
- принципы исследования потенциально опасных программ для ЭВМ.

Уметь:

- нейтрализовывать вредоносные программы без вспомогательного аппаратного и программного обеспечения;
- рационально применять антивирусные программы отечественных и зарубежных производителей;
- определять факторы и степень опасности вредоносных программ;
- выполнять функции специалиста и эксперта-криминалиста по уголовным делам, возбуждаемым по ст. 273 УК;
- использовать современные методы и алгоритмы защиты от вредоносных программ.

Владеть (демонстрировать навыки и опыт деятельности):

– методикой защиты компьютерной информации от вредоносных программ.

1.4. Объем дисциплины

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	*10*
1.	**Аудиторные занятия**	34	34	34
2.	Лекции			
3.	Практические занятия	34	34	34
4.	Лабораторные работы			
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	**70**	**5.10**	**70**
6.	**Промежуточная аттестация**	**4**	**0,25**	**Зачет(4)**
7.	**Общий объем по учебному плану, час.**	**108**	**39.35**	**108**
8.	**Общий объем по учебному плану, з.е.**	**3**		**3**

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины	Содержание
1	**Классификация вредоносных программ**	Понятие об опасных компьютерных программах и данных. Оценка опасностей, связанных с разработкой и использованием программ для ЭВМ. Состав вредоносных программ и команд. Классификация вредоносных программ по основным свойствам и признакам. Основные признаки и возможности компьютерных вирусов, программных закладок, «логических бомб», сетевых «червей», программ «удаленного администрирования» и иных видов опасных программ. Инструментарий, используемый вирмейкерами для создания вредоносных программ. Изучение функциональных возможностей вредоносных программ. Программные воздействия, заведомо приводящие к опасным последствиям. Сущность вредоносных блокирования, удаления, модификации защищаемой компьютерной информации. Программно-управляемые формы несанкционированного копирования информации. Механизмы вирусного заражения. Виды и формы программно-управляемого нарушения работы ЭВМ. Способы несанкционированного запуска опасных программ и команд. Способы внедрения и запуска вредоносных программ. Уязвимые места программного обеспечения автоматизированных систем, способствующие внедрению, запуску, сокрытию, и распространению вредоносных программ. Способы проникновения вредоносных программ в локальные и сетевые ЭВМ. Потенциально опасные функции операционной системы. Уязвимости ОС и штатного программного обеспечения, способствующие распространению вредоносных программ. Понятие о случайном и безусловном запуске. Внедрение и запуск программного кода на этапах самотестирования ПЭВМ и загрузки операционной системы. Способы подготовки вредоносных программ к автоматическому запуску. Типичные варианты обмана пользователей, провоцирующих их на запуск неизвестных программ. Внедрение и запуск опасных программ с применением «троянских» оболочек. Возможности программ-«джойнеров».
2	**Средства и методы защиты от вредоносных компьютерных программ**	Виды и возможности антивирусных программ. Меры по реализации изолированной программной среды. Статический анализ потенциально опасных программ. Определение истинного типа файла. Просмотр текстовых строк в исполняемых и командных файлах. Рекомендации по дизассемблированию и исследованию программного

		кода. Динамический анализ опасных программ. Запуск программ в виртуальной среде VMWare. Трассировка программ. Возможности программ типа ExeScope и OllyDebugger. Использование мониторов обращений к стеку сетевых драйверов, файлам и системному реестру. Оформление заключений по результатам исследования неизвестных и опасных программ. Способы выявления деструктивной активности вредоносных программ. Понятие о сигнатуре вредоносного программного кода. Принципы антивирусного сканирования памяти ЭВМ. Понятие о механизмах скрытности вредоносных программ. Демаскирующие признаки вредоносного программного кода. Полиморфизм программного кода. «Stealth»-технологии. Способы сокрытия файловых объектов и процессов на уровне ядра операционной системы. Возможности программ-«руткитов». Мониторинг подозрительной активности программ. Статический анализ потенциально опасных программ. Определение истинного типа файла. Просмотр текстовых строк в исполняемых и командных файлах. Рекомендации по дизассемблированию и исследованию программного кода. Динамический анализ опасных программ. Запуск программ в виртуальной среде VMWare. Трассировка программ. Возможности программ типа ExeScope и OllyDebugger. Использование мониторов обращений к стеку сетевых драйверов, файлам и системному реестру. Оформление заключений по результатам исследования неизвестных и опасных программ.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Очная форма обучения

Объем модуля (зач.ед.): 8
Объем дисциплины (зач.ед.): 3

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																							
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер.,	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иноязыч. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
1	Классификация вредоносных программ	**51**	**16**		16		**35**	**12**		12			**16**	2										7	1					
2	Средства и методы защиты от вредоносных компьютерных программ	**53**	**18**		18		**35**	**14**		14			**14**	2										7	1					
	Всего (час), без учета промежуточной аттестации:	**104**	**34**		**34**		**70**	**26**		**26**			**30**	**30**										**14**	**14**					
	Всего по дисциплине (час.):	**108**	**34**				**74**	В т.ч. промежуточная аттестация																			**4**	**0**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1 Лабораторные работы

Не предусмотрено

4.2 Практические занятия

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
1	1	Исследование деструктивных возможностей потенциально опасных программ и команд	4
1	2	Исследование возможностей скрытого внедрения и запуска опасных программ	4
1	3	Исследование интерпретируемых вредоносных программ (командных файлов, макросов и сценариев)	4
1	4	Динамическое исследование вредоносных программ	4
2	5	Виды и возможности антивирусных программ	8
2	6	Выявление деструктивной активности вредоносных программ	8
		Всего:	**34**

4.3. Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

Домашняя работа №1. *Основные свойства вредоносных программ.*
Домашняя работа №2. *Функциональные возможности вредоносных программ.*
Домашняя работа №3. *Анализ опасных программ.*
Домашняя работа №4. *Выявления деструктивной активности вредоносных программ.*

4.3.2. Примерный перечень тем графических работ
Не предусмотрено
4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)
Не предусмотрено
4.3.4 Примерная тематика индивидуальных или групповых проектов
Не предусмотрено
4.3.5. Примерный перечень тем расчетных работ (программных продуктов)
Не предусмотрено
4.3.6. Примерный перечень тем расчетно-графических работ
Не предусмотрено
4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)
Не предусмотрено

4.3.8. Примерная тематика контрольных работ

Контрольная работа №1. *Способы внедрения и запуска вредоносных программ.*
Контрольная работа №2. *Способы выявления деструктивной активности вредоносных программ.*

4.3.9. Примерная тематика коллоквиумов

Не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
Классификация вредоносных программ								*				
Средства и методы защиты от вредоносных компьютерных программ	*							*				

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1. Основная литература

1. Духан Е.И. Применение программно-аппаратных средств защиты компьютерной информации : учебное пособие для студентов вузов, обучающихся по специальностям 090102, 090105, 090106 / Е. И. Духан, Н. И. Синадский, Д. А. Хорьков ; науч. ред. Н. А. Гайдамакин ; Урал. гос. техн. ун-т - УПИ .— Екатеринбург : УГТУ-УПИ, 2008. — 182 с.

9.1.2. Дополнительная литература

1. Касперски К. Техника и философия хакерских атак - записки мыщ`а / Крис Касперски .— 2-е изд., перераб. и доп. — М. : СОЛОН-Пресс, 2005 .— 272 с.

9.2. Методические разработки

1. Бакланов, В. В. Противодействие созданию и распространению вредоносных программ / Бакланов В.В. — 2008 .— Курс "Противодействие созданию и распространению вредоносных программ" является специальным курсом для специальности "Компьютерная безопасность". Излагается классификация вредоносных программ. Обсуждаются методы и средства противодействия созданию и распространению вредоносных программ. Включает учебное пособие, программу дисциплины, сборник лабораторных работ, методические указания, экзаменационные материалы, презентации. Предназначен для студентов специальности "Компьютерная безопасность". — в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11067>.

9.3. Программное обеспечение

ОС Linux

9.4. Базы данных, информационно-справочные и поисковые системы

1. http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»
2. http://www.edu.ru/ - Федеральный портал. Российское образование.
3. http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ
4. http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ

9.5.Электронные образовательные ресурсы

1. Портал информационно-образовательных ресурсов УрФУ http://study.ustu.ru/info/default.aspx
2. Официальный сайт ИРИТ-РтФ http://rtf.ustu.ru
3. Официальный сайт кафедры ТОР УрФУ http://tor.rtf.ustu.ru

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Р-402. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в сеть Интернет.

Р-411. Персональные компьютеры – 15 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в сеть Интернет.

Р-125 Персональные компьютеры – 20 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в сеть Интернет.

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины не устанавливается.

6.2. Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: **коэффициент значимости совокупных результатов лекционных занятий – не предусмотрено**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 1		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Домашняя работа №1	*10,1-15*	*15*
Домашняя работа №2	*10,1-15*	*15*
Домашняя работа №3	*10,1-15*	*15*
Домашняя работа №4	*10,1-15*	*15*
Контрольная работа №1	*10,1-15*	*20*
Контрольная работа №2	*10,1-15*	*20*
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 0,4		
Промежуточная аттестация по практическим/семинарским занятиям – *зачет* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0,6**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий – не предусмотрено		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта
не предусмотрено

6.4. Коэффициент значимости семестровых результатов освоения дисциплины
не предусмотрено

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с отсутствием Дисциплины и ее аналогов, по которым возможно тестирование, на сайтах ФЭПО, Интернет-тренажеры и портале СМУДС УрФУ, тестирование в рамках НТК не проводится.

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

При проведении независимого тестового контроля как формы промежуточной аттестации применяется методика оценивания результатов, предлагаемая разработчиками тестов. Процентные показатели результатов независимого тестового контроля переводятся в баллы промежуточной аттестации по 100-балльной шкале в БРС:

– в случае балльной оценки по тесту (блокам, частям теста) переводится процент набранных баллов от общего числа возможных баллов по тесту;
– при отсутствии балльной оценки по тесту переводится процент верно выполненных заданий теста, от общего числа заданий.

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий

Не предусмотрено

8.3.2. Примерные контрольные задачи в рамках учебных занятий

Домашняя работа №1.

1) *Привести основные признаки и возможности сетевых «червей»,*

2) *Привести основные признаки и возможности программ «удаленного администрирования».*

Домашняя работа №2.

1) *Опишите виды программных воздействий, заведомо приводящих к опасным последствиям.*

2) В чем состоит сущность вредоносного блокирования, удаления, модификации защищаемой компьютерной информации**?**

Домашняя работа №3.

1) *Как осуществляется статический анализ потенциально опасных программ?*

2) *Как осуществляется динамический анализ опасных программ?*

Домашняя работа №4.

1) *Опишите принципы антивирусного сканирования памяти ЭВМ.*

2) *Дайте классификацию механизмов скрытности вредоносных программ.*

Примерные контрольные задачи в рамках контрольных работ

Контрольная работа №1.

1) *Перечислите основные виды способов подготовки вредоносных программ к автоматическому запуску.*

2) *Перечислите основные варианты обмана пользователей, провоцирующих их на запуск неизвестных программ.*

3) *Когда открытый порт может свидетельствовать о наличии уязвимости:*

- когда данный порт используется уязвимой сетевой службой

- когда данный порт принадлежит перечню используемых шпионскими программами

- в обоих перечисленных случаях?

Контрольная работа №2.

1) *Перечислите основные механизмы скрытности вредоносных программ.*

2) *Дайте классификацию демаскирующих признаков вредоносного программного кода.*

3) *Какие объекты HTML должны исследоваться на предмет наличия уязвимостей класса*

Cross-Site Scripting:
- пользовательские формы ввода
- скрытые CGI-параметры, хранимые в HTML
- ссылки, содержащие CGI-параметры
- любая информация, передаваемая серверу в виде GET- и POST-запросов

8.3.3. Примерные контрольные кейсы
Не предусмотрено
8.3.4. Перечень примерных вопросов для зачета
1. Виды антивирусных программ. Достоинства и недостатки антивирусных сканеров.
2. Мониторинг как средство и метод противодействия вредоносным программам. Контроль целостности защищаемых файлов и иммунизация.
3. Особенности, признаки и стадии жизненного цикла компьютерных вирусов. Виды компьютерных вирусов.
4. Компьютерные программы как инструмент шпионажа. Распространенные виды программных закладок.
5. Особенности «логических бомб». Возможности вредоносных программ удаленного администрирования.
6. Особенности распространения и вредоносные функции «сетевых червей». Программные атаки на ресурсы компьютерных систем и сетей.
7. Классификация вредоносных программ по тяжести деструктивных последствий.

8.3.5. Перечень примерных вопросов для экзамена
Не предусмотрено
8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации
Не предусмотрено
8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля
Не предусмотрено
8.3.8. Интернет-тренажеры
Не предусмотрено

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

РЕАГИРОВАНИЕ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль Обнаружение, предупреждение и ликвидация последствий компьютерных атак	**Код модуля** 1139532 Учебный план № 5347
Образовательная программа Компьютерная безопасность	**Код ОП** 10.05.01/01.02
Направление подготовки Компьютерная безопасность	**Код направления и уровня подготовки** 10.05.01
Уровень подготовки Специалитет	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО:** 1 декабря 2016 г., № 1512

Екатеринбург, 2018

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Департамент	Подпись
1	Синадский Николай Игоревич	к.т.н., доцент	Доцент	Кафедра алгебры и фундаментальной информатики	
2	Бакланов Валентин Викторович	к.т.н., доцент	Доцент	Радиоэлектроники и связи	

Руководитель модуля В.А. Баранский

Рекомендовано учебно-методическим советом Института Математики и Компьютерных наук

Председатель учебно-методического совета А.Ю. Коврижных
Протокол № 12 от 15.12.2016 г.

Согласовано:

Дирекция образовательных программ Р. Х. Токарева

Руководитель ОП, для которой
реализуется модуль В.А. Баранский

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «РЕАГИРОВАНИЕ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ»

1.1.Аннотация содержания дисциплины

Дисциплина входит в состав базового модуля «Обнаружение, предупреждение и ликвидация последствий компьютерных атак», изучается в одно время с дисциплиной «Системы обнаружения и предупреждения компьютерных атак», перед дисциплиной «Противодействие созданию и распространению вредоносных программ».

Дисциплина посвящена изучению процесса управления и реагирования на инциденты информационной безопасности (ИБ).

1.2. Язык реализации программы – *русский*

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

- ПК-20, способность выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций;
- ПКД-5, способность восстанавливать работоспособность систем защиты при сбоях и нарушении функционирования.

В результате освоения дисциплины студент должен:

Знать:

- принципы построения системы управления инцидентами ИБ;
- современные подходы к управлению и расследованию инцидентов ИБ;
- основные российские и международные стандарты в сфере управления инцидентами ИБ;
- последовательность действий по реагированию на инциденты ИБ;

Уметь:

- осуществлять сбор технических данных с компонентов информационной инфраструктуры;
- выполнять поиск (выделение) из собранных технических данных содержательной (семантической) информации, ее анализ и оформлению;
- организовывать наличие технических данных на этапах создания и эксплуатации информационной инфраструктуры;
- выполнять работы по восстановлению работоспособности информационных систем при реагировании на инциденты ИБ;

Владеть (демонстрировать навыки и опыт деятельности):

- техническими средствами и инструментами для сбора и обработки технических данных;
- методиками восстановления работоспособности информационных систем.

1.4. Объем дисциплины

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	*9*
1.	**Аудиторные занятия**	**68**	**68**	**68**
2.	Лекции	34	34	34
3.	Практические занятия	34	34	34
4.	Лабораторные работы			
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	**36**	**10,20**	**36**
6.	**Промежуточная аттестация**	**4**	**0,25**	**Зачет(4)**
7.	**Общий объем по учебному плану, час.**	**108**	**78,45**	**108**
8.	**Общий объем по учебному плану, з.е.**	**3**		**3**

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины	Содержание
1	**Управление инцидентами информационной безопасности**	Понятие инцидентов ИБ. Нормативная база в сфере управления инцидентами ИБ. Система управления инцидентами ИБ. Обработка событий и инцидентов ИБ. Реагирование на инциденты ИБ. Организация процесса обработки технических данных в рамках реагирования на инциденты ИБ.
2	**Сбор и анализ технических данных при реагировании на инциденты**	Организация процесса обработки технических данных в рамках реагирования на инциденты ИБ: сбор технических данных с компонентов информационной инфраструктуры; поиск (выделение) из собранных технических данных содержательной (семантической) информации, ее анализ и оформлению; распространение (передача) выделенной и оформленной содержательной (семантической) информации; обеспечение наличия технических данных на этапах создания и эксплуатации информационной инфраструктуры. Сбор и фиксация информации об инцидентах ИБ: способ выявления инцидента ИБ; источник информации об инциденте ИБ; содержание информации об инциденте ИБ, полученной от источника; сценарий реализации инцидента ИБ; дата и время выявления инцидента ИБ; состав информационной инфраструктуры, задействованной в реализации инцидента ИБ, в том числе пострадавшей от инцидента ИБ, уровень ее критичности; способы подключения информационной инфраструктуры, задействованной в реализации инцидента ИБ, к сети Интернет или сетям общего пользования; информация об операторе связи и провайдере сети Интернет. Проверка целостности (неизменности) собранных данных, маркирование носителей собранных данных. Криминалистическое копирование (создания образов) энергонезависимых технических данных запоминающих устройств СВТ методом побитового копирования. Копирование содержимого оперативной памяти СВТ и получение данных операционных систем. Копирование протоколов (журналов) регистрации. Копирование сетевого трафика. Поиск (выделение) содержательной (семантической) информации, ее анализ и оформление. Структура протокола обработки технических данных. Технические средства и инструменты для сбора и

		обработки технических данных: технические средства выполнения криминалистической копии (создания образа) запоминающих устройств и содержимого оперативной памяти СВТ; технические средства получения данных операционных систем о сетевых конфигурациях, о сетевых соединениях, об открытых файлах, о запущенных процессах, об открытых сессиях доступа.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Очная форма обучения

Объем модуля (зач.ед.): 8
Объем дисциплины (зач.ед.): 3

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																							
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иноязы. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
1	Управление инцидентами информационной безопасности	**49**	**32**	16	16		**17**	**12**	6	6														**5**	1					
2	Сбор и анализ технических данных при реагировании на инциденты	**55**	**36**	18	18		**19**	**14**	7	7														**5**	1					
	Всего (час), без учета промежуточной аттестации:	**104**	**68**	**34**	**34**		**36**	**26**	**13**	**13**														**10**	**10**					
	Всего по дисциплине (час.):	**108**	**68**				**40**	В т.ч. промежуточная аттестация																			**4**	**0**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1 Лабораторные работы

Не предусмотрено

4.2 Практические занятия

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
1	1	Криминалистическое копирование (создания образов) энергонезависимых технических данных запоминающих устройств СВТ методом побитового копирования	6
1	2	Копирование содержимого оперативной памяти СВТ и получение данных операционных систем	6
1	3	Копирование протоколов (журналов) регистрации	4
2	4	Копирование сетевого трафика	4
2	5	Поиск (выделение) содержательной (семантической) информации, ее анализ и оформление	4
2	6	Программный инструментарий эксперта-криминалиста	4
2	7	Механизмы компьютерного следообразования	6
		Всего:	**34**

4.3. Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

Не предусмотрено

4.3.2. Примерный перечень тем графических работ

Не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

Не предусмотрено

4.3.4 Примерная тематика индивидуальных или групповых проектов

Не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

Не предусмотрено

4.3.6. Примерный перечень тем расчетно-графических работ

Не предусмотрено

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

Не предусмотрено

4.3.8. Примерная тематика контрольных работ

Контрольная работа №1. *Обработки технических данных в рамках реагирования на инциденты ИБ.*
Контрольная работа №2. *Программный инструментарий эксперта-криминалиста.*

4.3.9. Примерная тематика коллоквиумов

Не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
Управление инцидентами информационной безопасности	*							*				
Сбор и анализ технических данных при реагировании на инциденты	*							*				

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1. Основная литература

1. Синадский Н.И. Анализ и восстановление данных на носителях с файловой системой NTFS : учеб. пособие / Н. И. Синадский ; науч. ред. В. В. Бакланов .— Екатеринбург : [ГОУ ВПО УГТУ-УПИ], 2007 .— 136 с. 90 экз.

9.1.2. Дополнительная литература

1. Бакланов В.В. Введение в информационную безопасность. Направления информационной защиты : курс лекций : учеб. пособие для вузов / В. В. Бакланов .— Екатеринбург : Изд-во Уральского университета, 2007 .— 232 с. — (Приоритетный национальный проект "Образование") (Математика. Компьютерные науки) .— Библиогр.: с. 229-232 .— ISBN 5-7996-0259-5.
2. Расторгуев С.П. Основы информационной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям "Компьютер. безопасность", "Комплекс. обеспечение информ. безопасности автоматизир. систем" и "Информ. безопасность телекоммуникац. систем" / С. П. Расторгуев .— Москва : Академия, 2007 .— 188 с. ; 22 см .— (Высшее профессиональное образование, Информационная безопасность) .— Слов. терминов: с. 182-185. — Библиогр.: с. 180-181 (39 назв.). — Допущено в качестве учебного пособия. — ISBN 978-5-7695-3098-2.

9.2. Методические разработки

1. Синадский Н.И. Учебно-методический комплекс дисциплины "Защита информации в компьютерных сетях" [Электронный ресурс] / Н. И. Синадский ; Федер. агентство по образованию, Урал. гос. ун-т им. А. М. Горького, ИОНЦ "Информационная безопасность" [и др.] .— Электрон. дан. (13,3 Мб) .— Екатеринбург : [б. и.], 2008 .— 1 электрон. опт. диск (CD-ROM) .— Загл. с этикетки диска .— <URL:http://elar.urfu.ru/handle/10995/1654>.

9.3. Программное обеспечение

ОС Linux, Windows, Mac OS X

9.4. Базы данных, информационно-справочные и поисковые системы

1. http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»
2. http://www.edu.ru/ - Федеральный портал. Российское образование.
3. http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ
4. http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ

9.5.Электронные образовательные ресурсы

1. Портал информационно-образовательных ресурсов УрФУ http://study.ustu.ru/info/default.aspx
2. Официальный сайт ИРИТ-РтФ http://rtf.ustu.ru
3. Официальный сайт кафедры ТОР УрФУ http://tor.rtf.ustu.ru

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Р-402. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в сеть Интернет.

Р-411. Персональные компьютеры – 15 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в сеть Интернет.

Р-125 Персональные компьютеры – 20 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в сеть Интернет.

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины не устанавливается.

6.2. Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: **коэффициент значимости совокупных результатов лекционных занятий – 0,6**		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Контрольная работа №1	*9,1-17*	*50*
Контрольная работа №2	*9,1-17*	*50*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – зачет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0,4		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Практические занятия	*9,1-17*	*100*
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий – не предусмотрено		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта
не предусмотрено

6.4. Коэффициент значимости семестровых результатов освоения дисциплины
не предусмотрено

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с отсутствием Дисциплины и ее аналогов, по которым возможно тестирование, на сайтах ФЭПО, Интернет-тренажеры и портале СМУДС УрФУ, тестирование в рамках НТК не проводится.

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

При проведении независимого тестового контроля как формы промежуточной аттестации применяется методика оценивания результатов, предлагаемая разработчиками тестов. Процентные показатели результатов независимого тестового контроля переводятся в баллы промежуточной аттестации по 100-балльной шкале в БРС:

– в случае балльной оценки по тесту (блокам, частям теста) переводится процент набранных баллов от общего числа возможных баллов по тесту;
– при отсутствии балльной оценки по тесту переводится процент верно выполненных заданий теста, от общего числа заданий.

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий

Не предусмотрено

8.3.2. Примерные контрольные задачи для контрольных работ

Контрольная работа №1.

1) *Опишите методы сбора технических данных с компонентов информационной инфраструктуры на инциденты ИБ;*

2) *Укажите способы выделения из собранных технических данных семантической информации на инциденты ИБ;*

Контрольная работа №2.

1) *Укажите методы криминалистического копирования энергонезависимых технических данных запоминающих устройств СВТ методом побитового копирования.*

2) *Укажите методы копирование содержимого оперативной памяти СВТ и получение данных операционных систем на инциденты ИБ.*

8.3.3. Примерные контрольные кейсы

Не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

1. Понятие инцидентов ИБ.
2. Нормативная база в сфере управления инцидентами ИБ.
3. Система управления инцидентами ИБ.
4. Обработка событий и инцидентов ИБ.
5. Реагирование на инциденты ИБ.
6. Организация процесса обработки технических данных в рамках реагирования на инциденты ИБ.
7. Сбор технических данных с компонентов информационной инфраструктуры.
8. Поиск (выделение) из собранных технических данных содержательной (семантической) информации, ее анализ и оформлению.
9. Распространение (передача) выделенной и оформленной содержательной (семантической) информации.
10. Обеспечение наличия технических данных на этапах создания и эксплуатации информационной инфраструктуры.

11. Сбор и фиксация информации об инцидентах ИБ.
12. Проверка целостности (неизменности) собранных данных, маркирование носителей собранных данных.
13. Криминалистическое копирование (создания образов) энергонезависимых технических данных запоминающих устройств СВТ методом побитового копирования.
14. Копирование содержимого оперативной памяти СВТ и получение данных операционных систем.
15. Копирование протоколов (журналов) регистрации.
16. Копирование сетевого трафика.
17. Поиск (выделение) содержательной (семантической) информации, ее анализ и оформление.
18. Структура протокола обработки технических данных.
19. Технические средства и инструменты для сбора и обработки технических данных.

8.3.5. Перечень примерных вопросов для экзамена

Не предусмотрено

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

Не предусмотрено

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

Не предусмотрено

8.3.8. Интернет-тренажеры

Не предусмотрено

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

СИСТЕМЫ ОБНАРУЖЕНИЯ И ПРЕДУПРЕЖДЕНИЯ КОМПЬЮТЕРНЫХ АТАК

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль Обнаружение, предупреждение и ликвидация последствий компьютерных атак	**Код модуля** 1139532 Учебный план № 5347
Образовательная программа Компьютерная безопасность	**Код ОП** 10.05.01/01.02
Направление подготовки Компьютерная безопасность	**Код направления и уровня подготовки** 10.05.01
Уровень подготовки Специалитет	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО:** 1 декабря 2016 г., № 1512

Екатеринбург, 2018

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Департамент/ кафедра	Подпись
1	Синадский Николай Игоревич	к.т.н., доцент	Доцент	Кафедра алгебры и фундаментальной информатики	
2	Бакланов Валентин Викторович	к.т.н., доцент	Доцент	Департамент радиоэлектроники и связи	

Руководитель модуля В.А. Баранский

Рекомендовано учебно-методическим советом Института Математики и Компьютерных наук

Председатель учебно-методического совета А.Ю. Коврижных
Протокол № 12 от 15.12.2016 г.

Согласовано:

Дирекция образовательных программ Р. Х. Токарева

Руководитель ОП, для которой
реализуется модуль В.А. Баранский

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «СИСТЕМЫ ОБНАРУЖЕНИЯ И ПРЕДУПРЕЖДЕНИЯ КОМПЬЮТЕРНЫХ АТАК»

1.1.Аннотация содержания дисциплины

Дисциплина входит в состав базового модуля «Обнаружение, предупреждение и ликвидация последствий компьютерных атак», изучается в одно время с дисциплиной «Реагирование на компьютерные инциденты», перед дисциплиной «Противодействие созданию и распространению вредоносных программ».

Дисциплина посвящена изучению подходов и принципов проектирования и эксплуатации систем аудита информационной безопасности и обнаружения компьютерных атак. В дисциплине излагаются методы обнаружения компьютерных атак и принципы построения систем обнаружения атак. Рассматривается методология проведения аудита информационной безопасности.

1.2. Язык реализации программы – *русский*

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

- ПК-3, способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности;
- ПК-10, способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;
- ПК-12, способностью проводить инструментальный мониторинг защищенности компьютерных систем;
- ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах;
- ПКД-3, способность проводить аудит информационной безопасности и составлять итоговые документы аудита, содержащие выводы и рекомендации.

В результате освоения дисциплины студент должен:

Знать:

- технологии обнаружения компьютерных атак и их возможности;
- структуру и содержание основных организационно-распорядительных документов: политики безопасности, инструкции по обеспечению безопасности информации;
- основные уязвимости и типовые атаки на современные компьютерные системы;
- способы анализа применяемых методов и средств защиты информации на предмет адекватности политике безопасности;
- возможности и особенности использования специализированных программно-аппаратных средств при проведении аудита информационной безопасности;

Уметь:

- разрабатывать правила и настраивать системы обнаружения атак с целью выявления типичных сетевых вторжений;
- анализировать техническую документацию, нормативно-правовые и методические документы, относящиеся к вопросам информационной безопасности;
- выполнять анализ и описание применяемых мер защиты при выполнении аудита информационной безопасности;

– выполнять анализ технического уровня обеспечения информационной безопасности с использованием специализированных программных средств;
– составлять итоговые документы аудита информационной безопасности, содержащие выводы и рекомендации.

Владеть (демонстрировать навыки и опыт деятельности):

– средствами администрирования систем обнаружения компьютерных атак;
– средствами и системами аудита информационной безопасности;
– методикой проведения аудита информационной безопасности.

1.4. Объем дисциплины

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	*9*
1.	**Аудиторные занятия**	**34**	**34**	**34**
2.	Лекции	17	17	17
3.	Практические занятия	17	17	17
4.	Лабораторные работы			
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	**34**	**5,10**	**34**
6.	**Промежуточная аттестация**	**4**	**0,25**	**Зачет (4)**
7.	**Общий объем по учебному плану, час.**	**72**	**39,35**	**72**
8.	**Общий объем по учебному плану, з.е.**	**2**		**2**

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины	Содержание
1	**Эксплуатация систем обнаружения компьютерных атак**	Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий. Технологии обнаружения компьютерных атак и их возможности. Прямые и косвенные признаки атак. Методы обнаружения атак. Сигнатурный анализ и обнаружение аномалий. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА. Требования, предъявляемые к СОА. Стандартизация в области обнаружения атак. Архитектура СОА. Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования. Технологии построения СОА. Единая архитектура СОА в рамках концепции CIDF. Формат обмена сообщениями систем обнаружения вторжений IDMEF. Платформа построения систем управления событиями безопасности типа Prelude. Эксплуатация СОА. Варианты размещения СОА. Размещение сенсоров СОА. Реагирование на инциденты. Проблемы, связанные с СОА. Технология интеллектуальных многоагентных систем. Понятие агентов защиты. Архитектура многоагентных систем. Агентно-ориентированная система моделирования атак, многоагентная система обнаружения вторжений. Спецификация «системного ядра» многоагентной системы. Проектирование компонентов многоагентной СОА. Разработка сенсоров различного типа. Протоколы информирования о событиях, зафиксированных сенсором. Методологии обнаружения атак: простой поиск по шаблону, поиск по шаблону с сохранением состояния, разбор протоколов, эвристический анализ, обнаружение аномалий, анализ соответствия политике безопасности. Основные математические методы, лежащие в основе обнаружения аномалий, и их реализации в СОА. Модель системы корреляции событий информационной безопасности. Формирование правил обнаружения и сценариев сложных атак. Получение информации об актуальных компьютерных атаках из баз данных уязвимостей компьютерных систем. Структура баз

		данных CVE и BugTraq. Анализ эффективности применяемых СОА. Организация тестирования СОА. Генерация фонового сетевого трафика. Генерация трафика, содержащего сетевые атаки. Критерии тестирования СОА и их параметры.
2	**Эксплуатация систем аудита информационной безопасности**	Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ. Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем. Международные, государственные и ведомственные стандарты и рекомендации в области информационной безопасности. Анализ адекватности основных документов, регламентирующих применение нормативно-правовых и организационных методов обеспечения информационной безопасности. Оценка адекватности модели нарушителя, принятой в организации. Оценка инструкций пользователей и администраторов компьютерных систем. Описание и оценка адекватности организационных методов защиты, применение которых декларируется в политике безопасности. Анализ эффективности применения средств межсетевого экранирования. Анализ конфигурационных файлов. Методика тестирования межсетевых экранов. Определение местоположения защищаемой информации. Анализ технического проекта сети. Описание структуры сети и физического местоположения объектов информатизации, обрабатывающих защищаемую информацию. Описание средств и методов защиты, применение которых декларируется в технической документации. Определение структуры информационно-телекоммуникационных сетей. Программные средства анализа топологии вычислительной сети. Определение маршрутов прохождения сетевых пакетов. Обнаружение объектов сети. Построение схемы сети. Выявление телекоммуникационного оборудования. Выявление и построение схемы информационных потоков защищаемой информации. Сетевой мониторинг на основе использования механизма WMI и протоколов ICMP, SNMP и CDP. Применение систем автоматизированного построения схемы сети. Средства и методы выявления уязвимостей в программном обеспечении узлов компьютерной сети. Цели и принципы зондирования узлов сети. Использование коммерческих и свободно распространяемых средств аудита безопасности компьютерных систем. Особенности средств активного аудита. Применение средств анализа

		защищенности серверов приложений. Применение средств автоматизации комплексного аудита информационной безопасности. Структура и функции комплексных экспертных систем аудита безопасности. Учет структуры аппаратно-программных средств объекта информатизации. Ранжирование обнаруженных уязвимостей по степени воздействия на защищаемую информацию. Описание выявленных уязвимостей и определение мер защиты, их устраняющих. Формирование выводов и рекомендаций по устранению обнаруженных недостатков. Проектирование систем анализа защищенности. Обобщенные архитектуры систем активного и пассивного анализа защищенности. Модуль генерирования комплекса сценариев атак. Модуль обновления баз данных уязвимостей компьютерных систем.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Очная форма обучения

Объем модуля (зач.ед.): 8
Объем дисциплины (зач.ед.): 2

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																							
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иноязы. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
1	Эксплуатация систем обнаружения компьютерных атак	**36**	**18**	9	9		**18**	**13**	6	7														5	1					
2	Эксплуатация систем аудита информационной безопасности	**32**	**16**	8	8		**16**	**11**	5	6														5	1					
	Всего (час), без учета промежуточной аттестации:	**68**	**34**	**17**	**17**		**34**	**24**	**11**	**13**														**10**	**10**					
	Всего по дисциплине (час.):	**72**	**34**				**38**	В т.ч. промежуточная аттестация																			**4**	**0**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1 Лабораторные работы

Не предусмотрено

4.2 Практические занятия

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
1	1	Применение сигнатурных систем обнаружения атак типа Snort	3
1	2	Обнаружение сетевых компьютерных атак с использованием комплекса Cisco IDS Sensor	3
1	3	Обнаружение комплексных компьютерных атак с использованием комплекса Cisco MARS	3
2	4	Анализ технической документации и составление технического описания объекта аудита информационной безопасности	1
2	5	Применение инструментальных средств для анализа соответствия технической документации и существующей топологии сети объекта аудита информационной безопасности	1
2	6	Получение информации об аппаратно-программной конфигурации компьютерной системы	2
2	7	Использование коммерческих и свободно распространяемых средств аудита безопасности компьютерных систем	2
2	8	Применение средств автоматизации комплексного аудита информационной безопасности	2
		Всего:	**17**

4.3. Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

Не предусмотрено

4.3.2. Примерный перечень тем графических работ

Не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

Не предусмотрено

4.3.4 Примерная тематика индивидуальных или групповых проектов

Не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

Не предусмотрено

4.3.6. Примерный перечень тем расчетно-графических работ
Не предусмотрено
4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)
Не предусмотрено
4.3.8. Примерная тематика контрольных работ

Контрольная работа №1. *Методологии обнаружения атак.*
Контрольная работа №2. *Аудит безопасности компьютерных систем.*

4.3.9. Примерная тематика коллоквиумов
Не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
Эксплуатация систем обнаружения компьютерных атак	*							*				
Эксплуатация систем аудита информационной безопасности	*							*				

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1. Основная литература

1. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс: учебное пособие / А.Н. Андрончик, А.С. Коллеров, Н.И. Синадский, М.Ю.

Щербаков; под ред. Н.И. Синадского. – Екатеринбург: УрФУ, 2011. – 160 с.

9.1.2. Дополнительная литература

1. Бил Дж. и др. Snort 2.1 Обнаружение вторжений. – М.: Бином, 2009. – 656 с.

9.2. Методические разработки

1. Синадский Н.И. Учебно-методический комплекс дисциплины "Защита информации в компьютерных сетях" [Электронный ресурс] / Н. И. Синадский ; Федер. агентство по образованию, Урал. гос. ун-т им. А. М. Горького, ИОНЦ "Информационная безопасность" [и др.] .— Электрон. дан. (13,3 Мб) .— Екатеринбург : [б. и.], 2008 .— 1 электрон. опт. диск (CD-ROM) .— Загл. с этикетки диска .— <URL:http://elar.urfu.ru/handle/10995/1654>.

9.3. Программное обеспечение

ОС Linux

9.4. Базы данных, информационно-справочные и поисковые системы

1. http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»
2. http://www.edu.ru/ - Федеральный портал. Российское образование.
3. http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ
4. http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ

9.5.Электронные образовательные ресурсы

1. Портал информационно-образовательных ресурсов УрФУ http://study.ustu.ru/info/default.aspx
2. Официальный сайт ИРИТ-РтФ http://rtf.ustu.ru
3. Официальный сайт кафедры ТОР УрФУ http://tor.rtf.ustu.ru

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Р-402. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в сеть Интернет.

Р-411. Персональные компьютеры – 15 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в сеть Интернет.

Р-125 Персональные компьютеры – 20 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в сеть Интернет.

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины не устанавливается.
6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,4		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Контрольная работа №1	*9,1-17*	*50*
Контрольная работа №2	*9,1-17*	*50*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – зачет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0,6		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Практические занятия	*9,1-17*	*100*
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –не предусмотрено		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта
не предусмотрено
6.4. Коэффициент значимости семестровых результатов освоения дисциплины
не предусмотрено

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с отсутствием Дисциплины и ее аналогов, по которым возможно тестирование, на сайтах ФЭПО, Интернет-тренажеры и портале СМУДС УрФУ, тестирование в рамках НТК не проводится.

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

При проведении независимого тестового контроля как формы промежуточной аттестации применяется методика оценивания результатов, предлагаемая разработчиками тестов. Процентные показатели результатов независимого тестового контроля переводятся в баллы промежуточной аттестации по 100-балльной шкале в БРС:

– в случае балльной оценки по тесту (блокам, частям теста) переводится процент набранных баллов от общего числа возможных баллов по тесту;
– при отсутствии балльной оценки по тесту переводится процент верно выполненных заданий теста, от общего числа заданий.

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий

Не предусмотрено

8.3.2. Примерные задачи в рамках контрольных работ

Контрольная работа №1.

1) *Опишите методологию обнаружения атак с помощью простого поиска по шаблону и поиска по шаблону с сохранением состояния.*

2) *Опишите методологию обнаружения атак с помощью разбора протоколов, обнаружения аномалий, анализа соответствия политике безопасности.*

3) *Какие математические методы лежат в основе обнаружения аномалий, и как они реализуются в СОА?*

Контрольная работа №2.

1) *Укажите цели и задачи проведения аудита безопасности компьютерных систем.*

2) *Опишите этапы и методы проведения аудита безопасности.*

3) *Какие нормативно-правовые и организационные основы имеет проведение аудита безопасности компьютерных систем?*

8.3.3. Примерные контрольные кейсы

Не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

1. Классификация атак на компьютерные сети.
2. Основные типы сетевых атак.
3. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов.
4. Сигнатурный анализ и обнаружение аномалий.
5. Классификация систем обнаружения атак.
6. Требования, предъявляемые к СОА.
7. Архитектура СОА.
8. Варианты размещения СОА.
9. Архитектура многоагентных СОА.
10. Методологии обнаружения атак.
11. Модель системы корреляции событий информационной безопасности.
12. Цели и задачи проведения аудита безопасности.
13. Этапы и методы проведения аудита безопасности, результаты работ

14. Средства и методы выявления уязвимостей в программном обеспечении узлов компьютерной сети.
15. Особенности средств активного аудита.
16. Структура и функции комплексных экспертных систем аудита безопасности.
17. Обобщенные архитектуры систем активного и пассивного анализа защищенности.

8.3.5. Перечень примерных вопросов для экзамена

Не предусмотрено

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

Не предусмотрено

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

Не предусмотрено

8.3.8. Интернет-тренажеры

Не предусмотрено