МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

«БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Кафедра математики и физики

УТВЕРЖДАЮ:
Проректор по учебной работе
_____ Е.И. Луковникова
«_____» декабря 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

МЕТОДЫ ОЦЕНКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Б1.В.06

НАПРАВЛЕНИЕ ПОДГОТОВКИ

01.03.02 Прикладная математика и информатика

ПРОФИЛЬ ПОДГОТОВКИ

Инженерия программного обеспечения

Программа академического бакалавриата

Квалификация (степень) выпускника: бакалавр

СОДЕРЖАНИЕ ПРОГРАММЫ **Стр.**

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Вид деятельности выпускника

Дисциплина охватывает круг вопросов, относящихся к организационно-управленческому, проектному и производственно-технологическому видам профессиональной деятельности выпускника в соответствии с компетенциями и видами деятельности, указанными в учебном плане.

Цель дисциплины

Изучение принципов и методов оценки безопасности компьютерных систем на основе комплексного подхода к определению актуальных угроз безопасности в таких системах в рамках обеспечения безопасности информационных систем и технологий в целом, изучение математических основ моделирования процессов оценки безопасности компьютерных систем, получение профессиональных компетенций в области современных технологий оценки безопасности компьютерных систем.

Задачи дисциплины

Освоение студентом:

- обучение студентов базовым понятиям современных методов оценки безопасности компьютерных систем;
- обучение студентов базовым методам оценки безопасности компьютерных систем;
- овладение практическими навыками применения методов оценки безопасности компьютерных систем;
- раскрытие физической сущности построения и эксплуатации компьютерных систем с точки зрения определения актуальных угроз безопасности в таких системах с целью корректного решения задач по применению методов оценки безопасности компьютерных систем.

Код компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
1	2	3
ПК-7	способность к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения.	**Знать:** - основные понятия, идеи, методы, связанные с дисциплинами фундаментальной математики, информатики - методы и средства оценки безопасности компьютерных систем **Уметь:** - систематизировать методы оценки безопасности компьютерных систем. **Владеть:** - навыками оценки действующего уровня защищенности в компьютерных системах. –технологиями анализа рисков.
ПК-9	способность составлять и контролировать план выполняемой работы, планировать необходимые для выполнения работы ресурсы, оценивать результаты собственной	**Знать:** – методы планирования, анализа и корректировки выполнения планов выполняемой работы и оценки результатов; **Уметь:** – составлять, контролировать, корректировать и оценивать результаты деятельности, необходимые

	работы	для выполнения работы. **Владеть:** - навыкам планирования выполняемой работы, оценки ресурсов и результатов собственной деятельности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В.06 – «Методы оценки безопасности компьютерных систем» относится к вариативной части и обязательная для изучения.

Дисциплина «Методы оценки безопасности компьютерных систем» базируется на знаниях, полученных при изучении таких учебных дисциплин, как: физика, построение и функционирование компьютерных систем, распространение сигналов, теории вероятности и математической статистики, теории цифровой обработки сигналов, информатики.

Основываясь на изучении перечисленных дисциплин, «Методы оценки безопасности компьютерных систем» представляет основу для подготовке к преддипломной практики и подготовки к государственной итоговой аттестации

Такое системное междисциплинарное изучение направлено на достижение требуемого ФГОС уровня подготовки по квалификации бакалавр.

3. РАСПРЕДЕЛЕНИЕ ОБЪЕМА ДИСЦИПЛИНЫ

3.1. Распределение объема дисциплины по формам обучения

Форма обучения	*Курс*	*Семестр*	*Трудоемкость дисциплины в часах*						*Курсовая работа (проект), контрольная работа, реферат, РГР*	*Вид промежуточной аттестации*
			Всего часов	*Аудиторных часов*	*Лекции*	*Лабораторные работы*	*Практические занятия*	*Самостоятельная работа*		
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Очная	4	7	108	51	17	17	17	57	-	зачет
Заочная	-	-	-	-	-	-	-	-	-	-
Заочная (ускоренное обучение)	-	-	-	-	-	-	-	-	-	-
Очно-заочная	-	-	-	-	-	-	-	-	-	-

3.2. Распределение объема дисциплины по видам учебных занятий и трудоемкости

Вид учебных занятий	*Трудоемкость (час.)*	*в т.ч. в интерактивной, активной, инновационной формах, (час.)*	*Распределение по семестрам, час*
			7
1	**2**	**3**	**4**
I. Контактная работа обучающихся с преподавателем (всего)	51	20	51
Лекции (Лк)	17	6	17
Лабораторные работы (ЛР)	17	14	17
Практические занятия (ПЗ)	17		17
II.Самостоятельная работа обучаю-	57	-	57

щихся (СР)			
Подготовка к лабораторным работам	36	-	36
Подготовка к зачету	21	-	21
III. Промежуточная аттестация зачет	+	-	+
Общая трудоемкость дисциплины час.	108	-	108
зач. ед.	3	-	3

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Распределение разделов дисциплины по видам учебных занятий - для очной формы обучения:

№ раздела и темы	*Наименование раздела и тема дисциплины*	*Трудоемкость, (час.)*	*Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость; (час.)*			
			учебные занятия			*самостоятельная работа обучающихся**
			лекции	*лабораторные работы*	*семинары/ практические занятия*	
1	2	3	4	5	6	7
1.	**Общие вопросы оценки безопасности компьютерных систем**	**47**	**9**	**9**	**9**	**20**
1.1	Предметная область оценки безопасности компьютерных систем.	15	3	3	3	6
1.2	Исторические сведения и этапы развития оценки безопасности компьютерных систем.	14	2	2	2	8
1.3	Математические основы оценки безопасности компьютерных систем	18	4	4	4	6
2.	**Методы и средства оценки безопасности компьютерных систем**	**32**	**4**	**4**	**4**	**20**
2.1	Анализ рисков в области защиты информации	14	2	2	2	8
2.2	Управление рисками и международные стандарты	9	1	1	1	6
2.3	Технологии анализа рисков	9	1	1	1	6
3.	**Организация оценки безопасности компьютерных систем**	**29**	**4**	**4**	**4**	**17**
3.1	Организация службы информационной безопасности	16	2	2	2	10
3.2	Формирование экспертных систем оценки безопасности компьютерных систем	13	2	2	2	7
	ИТОГО	**108**	**17**	**17**	**17**	**57**

4.2. Содержание дисциплины, структурированное по разделам и темам

№ раздела и темы	*Наименование раздела и темы дисциплины*	*Содержание лекционных занятий*	*Вид занятия в интерактивной, активной, инновационной формах, (час.)*
1	**2**	**3**	**4**
1.	**Общие вопросы оценки безопасности компьютерных систем**		
1.1	Предметная область оценки безопасности компьютерных систем.	Обзор направлений и отраслей оценки безопасности компьютерных систем. Место оценки безопасности компьютерных систем в инфраструктуре информационных систем. Обзор актуальности оценки безопасности компьютерных систем	Лекция-беседа (3 час.)
1.2	Исторические сведения и этапы развития оценки безопасности компьютерных систем.	Обзор основных этапов развития оценки безопасности компьютерных систем.	Лекция-беседа (2 час.)
1.3	Математические основы оценки безопасности компьютерных систем	Математические основы оценки безопасности компьютерных систем	Лекция-беседа (4 час.)
2.	**Методы и средства оценки безопасности компьютерных систем**		
2.1	Анализ рисков в области защиты информации	Международная практика защиты информации. Национальные особенности защиты информации.	Лекция-беседа (2 час.)
2.2	Управление рисками и международные стандарты	Постановка задачи анализа рисков. Методы, использующие оценку рисков на качественном уровне. Методы, использующие оценку рисков на количественном уровне. Методы, использующие смешанную оценку рисков. Управление рисками и международные стандарты	Лекция-беседа (1 час.)
2.3	Технологии анализа рисков	Инструментальные средства анализа рисков. Аудит безопасности и анализ рисков. Анализ защищенности компьютерной системы. Учет возможностей обнаружения атак.	Лекция-беседа (1 час.)
3.	**Организация оценки безопасности компьютерных систем**		
3.1	Организация службы информационной безопасности	Политика безопасности. Оценка рисков и ущербов безопасности компьютерных систем	Лекция-беседа (2 час.)
3.2	Формирование экспертных систем оценки безопасности компьютерных систем	Жизненный цикл компьютерных систем. Модель угроз и принципы обеспечения безопасности компьютерных систем	Лекция-беседа (2 час.)

4.3. Лабораторные работы

.

№ п/п	*Номер раздела дисциплины*	*Наименование лабораторной работы*	*Объем (час.)*	*Вид занятия в интерактивной, активной, инновационной формах, (час.)*
1	**1**	Математическая модель оценки коэффициента влияния отдельно взятого фактора на угрозы информационной безопасности.	5	Занятие в малых группах (2 час.)
3	**2**	Работа с Microsoft Baseline Security Analyzer 2.0	6	Занятие в малых группах (6 час.)
5	**3**	Организация оценки безопасности компьютерных систем	6	Занятия в малых группах (6 час.)
		ИТОГО	**17**	**14**

4.4. Практические занятия

№ п/п	*Номер раздела дисциплины*	*Наименование практического занятия*	*Объем (час.)*	*Вид занятия в интерактивной, активной, инновационной формах, (час.)*
1	**1,2,3**	Проведение анализа защищенности объекта защиты информации	8	-
2	**1,2,3**	Проведение анализа увеличения защищенности объекта защиты информации	9	-
		ИТОГО	**17**	**-**

4.5 Контрольные мероприятия: курсовой проект (курсовая работа), контрольная работа, РГР, реферат

Учебным планом не предусмотрено.

5. МАТРИЦА СООТНЕСЕНИЯ РАЗДЕЛОВ УЧЕБНОЙ ДИСЦИПЛИНЫ К ФОРМИРУЕМЫМ В НИХ КОМПЕТЕНЦИЯМ И ОЦЕНКЕ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Компетенции / *№, наименование разделов дисциплины*	*Кол-во часов*	*Компетенции* *ПК*		*Σ комп.*	$t_{ср}$, *час*	*Вид учебных занятий*	*Оценка результатов*
		7	*9*				
1	2	3	4	6	7	8	9
1. Общие вопросы оценки безопасности компьютерных систем	47	+	+	2	23,5	Лк, ЛР, ПЗ	зачет
2. Методы и средства оценки безопасности компьютерных систем	32	+	+	2	16	Лк, ЛР, ПЗ	зачет
3. Организация оценки безопасности компьютерных систем	29	+	+	2	14,5	Лк, ЛР, ПЗ	зачет
всего часов	**108**	**54**	**54**	**2**	**54**	-	-

6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1. Сычев Ю.Н. Основы информационной безопасности: учебно-практическое пособие/Ю.Н. Сычев.-М.: Изд. центр ЕАОИ, 2010.-328 с.

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№	*Наименование издания*	*Вид занятия* (*Лк, ЛР*)	*Количество экземпляров в библиотеке,* **шт.**	*Обеспеченность,* **(экз./ чел.)**
1	2	3	4	5
Основная литература				
1.	Прохорова О.В. Информационная безопасность и защита информации: учебник/ О.В. Прохорова.-Самара: СГАСУ, 2014.-113 с. http://biblioclub.ru/index.php?page=book_view_red&book_id=438331	Лк, ЛР,ПЗ	1 (ЭУ)	1
2.	Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций: направление подготовки «Информационная безопасность», специальность «Экономическая безопасность» / Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-205 с. http://biblioclub.ru/index.php?page=book_view_red&book_id=362895	Лк, ЛР,ПЗ	1 (ЭУ)	1
3.	Нестеров С.А. Основы информационной безопасности: учебное пособие/ С.А. Нестеров.- СПб.: изд-во Политехн. уни-та, 2014.-322 с. http://biblioclub.ru/index.php?page=book_view_red&book_id=363040	Лк, ЛР,ПЗ	1 (ЭУ)	1
Дополнительная литература				
4.	Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605	Лк, ЛР,ПЗ	1 комплект	
5.	Загинайлов Ю.Н. Теория информационной безопасности методология защиты информации: учебное пособие/ Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-253 с. http://biblioclub.ru/index.php?page=book_view_red&book_id=276557	Лк, ЛР,ПЗ	1 (ЭУ)	1

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ» НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В процессе обучения студенты могут использовать общие ресурсы:

1.Электронный каталог библиотеки БрГУ
http://irbis.brstu.ru/CGI/irbis64r_15/cgiirbis_64.exe?LNG=&C21COM=F&I21DBN=BOOK&P21DBN=BOOK&S21CNR=&Z21ID=.

2. Электронная библиотека БрГУ
http://ecat.brstu.ru/catalog .

3. Электронно-библиотечная система «Университетская библиотека online»
http://biblioclub.ru .

4. Электронно-библиотечная система «Издательство «Лань»
http://e.lanbook.com .

5. Информационная система "Единое окно доступа к образовательным ресурсам"
http://window.edu.ru .

6. Научная электронная библиотека eLIBRARY.RU http://elibrary.ru .

7. Университетская информационная система РОССИЯ (УИС РОССИЯ)
https://uisrussia.msu.ru/ .

8. Национальная электронная библиотека НЭБ
http://xn--90ax2c.xn--p1ai/how-to-search /.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Планирование и организация времени, необходимого для изучения дисциплины:

Важным условием успешного освоения дисциплины является создание студентом системы правильной организации своего труда, позволяющей распределить учебную нагрузку равномерно в соответствии с графиком образовательного процесса.

Большую помощь в этом может оказать составление плана работы на семестр, месяц, неделю, день. Его наличие позволит подчинить свободное время целям учебы, трудиться более успешно и эффективно. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Все задания к лабораторным работам, а также задания, вынесенные на самостоятельную работу, рекомендуется выполнять непосредственно после соответствующей темы лекционного курса, что способствует лучшему усвоению материала, позволяет своевременно выявить и устранить «пробелы» в знаниях, систематизировать ранее пройденный материал, на его основе приступить к овладению новыми знаниями, умениями и навыками.

Подготовка к лекционному занятию включает выполнение всех видов заданий, рекомендованных к каждой лекции, т.е.задания выполняются еще до лекционного занятия по соответствующей теме.

Лабораторные работы позволяют развивать у студентов творческое теоретическое мышление, умение самостоятельно изучать литературу, анализировать практику; учат четко формулировать мысль, вести дискуссию, то есть имеют исключительно важное значение в развитии самостоятельного мышления.

Подготовка к лабораторной работе включает два этапа.

На первом этапе студент планирует свою самостоятельную работу которая включает: уяснение задания на самостоятельную работу; подбор рекомендованной литературы; составление план работы, в котором определяются основные пункты предстоящей подготовки. Составление плана дисциплинирует и повышает организованность в работе. Второй этап включает непосредственную подготовку к лабораторной работе.

Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов.

9.1. Методические указания для обучающихся по выполнению лабораторных работ

Лабораторная работа №1: Математическая модель оценки коэффициента влияния отдельно взятого фактора на угрозы информационной безопасности.

Цель работы научиться строить математические модели безопасности.
Задание: Рассчитать коэффициент влияния человеческого фактора на угрозы информационной безопасности.
Порядок выполнения работы:
Проведем анализ экспертных оценок угроз информационной безопасности с условием присутствия в них влияния человеческого фактора. Большинство экспертных оценок угроз информационной безопасности можно разделить на две группы: вероятность возникновения угрозы и её критичность.
С точки зрения вероятности выделяются ошибки персонала и несанкционированный доступ. Наиболее критичными являются кража информации, халатность сотрудников и их неправомерные действия.
Определенные исследования за длительный период указывают на рост вероятности возникновения угроз безопасности с присутствием человеческого фактора.
Помимо этого можно выделить общие статистики, в которых явно выделен человеческий фактор, как причина возникновения белее половины всех угроз безопасности.
Форма отчетности
Отчет по лабораторной работе должен содержать следующие сведения:
- название и цель работы;
- подробности и описание этапов выполнения заданий.
Задание для самостоятельной работы:
Получить математическую модель оценки коэффициента влияния отдельно взятого фактора на угрозы информационной безопасности и рассмотреть её на примере человеческого фактора.
Рекомендации по выполнению:
Составим примерную таблицу. Для критичности представим следующую градацию: низкая 0-33, средняя 34-66, высокая 67-100. Малым влиянием человеческого фактора в данном примере можно пренебречь, так как будет находиться среднее значение коэффициента влияния для наиболее подверженных влиянию угроз информационной безопасности.
Таблица. Показатели угроз информационной безопасности

Угроза	Вероятность,%	Критичность,%	Присутствие ч/ф
НСД	25	73	+
Ошибки персонала	20	21	+
Кража информации	17	57	+
Халатность	12	38	+
Вирусы	15	68	-
Стихийные бедствия	1	89	-
Программные сбои	10	42	-

Согласно исследованию CompTIA [10] в 52% случаях возникновения угрозы информационной безопасности основополагающим фактором был именно человеческий, то есть , тогда коэффициент влияния человеческого фактора равен:

Критичность угрозы информационной безопасности «НСД» под действием человеческого фактора определяется следующим образом: В данном конкретном случае значение коэффициента влияния человеческого фактора получилось 0,7, однако полученное значение

может принимать разные значения для конкретного предприятия в зависимости от исходных данных.

Основная литература

1. Прохорова О.В. Информационная безопасность и защита информации: учебник/ О.В. Прохорова.-Самара: СГАСУ, 2014.-113 с.

2. Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций: направление подготовки «Информационная безопасность», специальность «Экономическая безопасность» / Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-205 с.

3. Нестеров С.А. Основы информационной безопасности: учебное пособие/ С.А. Нестеров.- СПб.: изд-во Политехн. уни-та, 2014.-322 с.

Дополнительная литература

4. Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM)

5. Загинайлов Ю.Н. Основы информационной безопасности методология защиты информации: учебное пособие/ Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-253 с.

Контрольные вопросы для самопроверки:

1. Что такое несанкционированный доступ?

2. Как проявляется рост вероятности возникновения угроз безопасности с присутствием человеческого фактора

Лабораторная работа №2: Использование Microsoft Security Assessment Tool (MSAT)

Цель работы познакомиться с разработанной Microsoft программой для самостоятельной оценки рисков, связанных с безопасностью - Microsoft Security Assessment Tool (MSAT).

Задание:

1. Подробно опишите реально существующее или вымышленное малое предприятие:

- сферу деятельности;
- состав и структуру информационной системы;
- особенности организации процесса защиты информации;
- применяемые методы и средства.

Порядок выполнения работы

В ходе работы, пользователь, выполняющий роль аналитика, ответственного за вопросы безопасности, отвечает на две группы вопросов.

Первая из них посвящена бизнес-модели компании, и призвана оценить риск для бизнеса, с которым компания сталкивается в данной отрасли и в условиях выбранной бизнес-модели. Создается так называемый профиль риска для бизнеса (ПРБ).

Форма отчетности

Отчет по лабораторной работе должен содержать следующие сведения:
- название и цель работы;
- скриншоты этапов работы программы MSAT с описанием.

Задание для самостоятельной работы:
С помощью программы MSAT проведите оценку рисков для предприятия.

Рекомендации по выполнению:

Вопросы этого этапа разбиты на 6 групп. Первая касается общих сведений о компании - название, число компьютеров, серверов и т.д. Вторая группа вопросов озаглавлена "Безопасность инфраструктуры". Примеры вопросов - "использует ли компания подключение к Интернет", "размещаются ли службы, используемые как внешними, так и внутренними клиентами, в одном и том же сегменте" и т.д. Остальные группы - "Безопасность приложений", "Безопасность операций", "Безопасность персонала", "Среда".

Когда проведен первый этап оценки, полученная информация обрабатывается (для этого требуется подключение к Интернет), после чего начинается второй этап анализа. Для технических специалистов он будет более интересен, т.к. касается используемых в компании политик, средств и механизмов защиты.

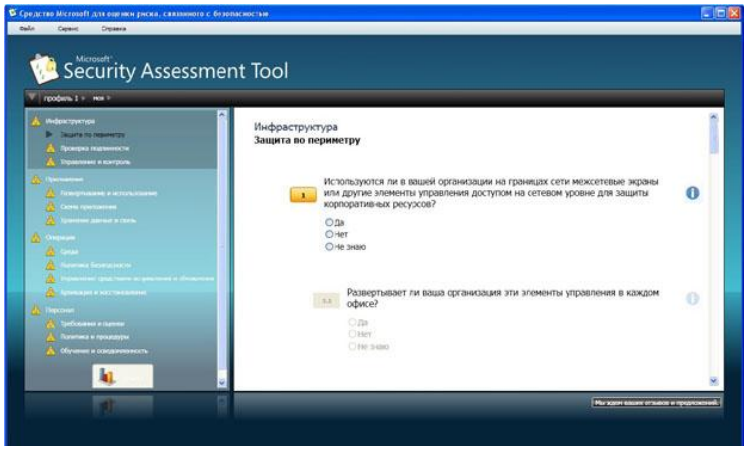

Рис.2. Анализ используемых механизмов защиты

Вопросы организованы в соответствии с концепцией многоуровневой (эшелонированной) защиты. Сначала рассматривается защита инфраструктуры (защита периметра, аутентификация…), затем вопросы защиты на уровне приложений, далее проводится анализ безопасности операций (определена ли политика безопасности, политика резервного копирования и т.д.), последняя группа вопросов касается работы с персоналом (обучение, проверка при приеме на работу и т.д.).

После ответа на все вопросы программа вновь обращается к удаленному серверу и генерирует отчеты. Наибольший интерес для технических специалистов представляет "Полный отчет". В частности, он содержит предлагаемый список приоритетных действий.

Основная литература

1. Прохорова О.В. Информационная безопасность и защита информации: учебник/ О.В. Прохорова.-Самара: СГАСУ, 2014.-113 с.

2. Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций: направление подготовки «Информационная безопасность», специальность «Экономическая безопасность» / Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-205 с.

3. Нестеров С.А. Основы информационной безопасности: учебное пособие/ С.А. Нестеров.- СПб.: изд-во Политехн. уни-та, 2014.-322 с.

Дополнительная литература

4. Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM)

5. Загинайлов Ю.Н. Основы информационной безопасности методология защиты информации: учебное пособие/ Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-253 с.

Контрольные вопросы для самопроверки:

Назовите способы и средства защиты информации.

Что такое система защиты информации?

Сформулируйте рекомендации по увеличению уровня защищенности компьютерных систем.

Лабораторная работа №3: Организация оценки безопасности компьютерных систем

Цель работы: провести оценку безопасности компьютерной системы.

Задание: Изучить международные и национальные стандарты и спецификации в области ИБ — от "Оранжевой книги" до ISO 15408. Получить навыки определения сильных и слабых стороны этих документов.

Порядок выполнения работы:

1. Разработать интерфейс пользователя «Оранжевая книга» как оценочный стандарт».
2. Разработать интерфейс пользователя «Информационная безопасность распределенных систем. Рекомендации X.800».
3. Разработать интерфейс пользователя «Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"
4. Разработать интерфейс пользователя «Гармонизированные критерии Европейских стран»
5. Разработать интерфейс пользователя « Руководящие документы Гостехкомиссии России»

Форма отчетности

Отчет по лабораторной работе должен содержать следующие сведения:
- название и цель работы;
- подробности и описание этапов выполнения заданий.

Задание для самостоятельной работы:

Изучить международные и национальные стандарты и спецификации в области ИБ — от "Оранжевой книги" до ISO 15408. Получить навыки определения сильных и слабых стороны этих документов.

Рекомендации по выполнению:

Потребители рассматривают квалификацию уровня безопасности ИТ-продукта как метод определения соответствия ИТ-продукта их запросам. Обычно эти запросы составляются на основании результатов проведенного анализа рисков и выбранной политики безопасности. "Единые критерии" играют существенную роль в процессе формирования запросов потребителей, так как содержат механизмы, позволяющие сформулировать эти запросы в виде стандартизованных требований. Это позволяет потребителям принять обоснованное решение о возможности использования тех или иных продуктов. Наконец, "Единые критерии" предоставляют потребителям механизм Профилей защиты, с помощью которого они могут выразить специфичные для них требования, не заботясь о механизмах их реализации.

Производители должны использовать "Единые критерии" в ходе проектирования и разработки ИТ-продуктов, а также для подготовки к квалификационному анализу и сертификации. Этот документ дает возможность производителям на основании анализа запросов потребителей определить набор требований, которым должен удовлетворять разрабатываемый ими продукт.

Эксперты по квалификации используют этот документ в качестве основных критериев определения соответствия средств защиты ИТ-продукта требованиям, предъявляемым к нему потребителями и угрозам, действующим в среде его эксплуатации. "Единые критерии" описывают только общую схему проведения квалификационного анализа и сертификации, но не регламентируют процедуру их осуществления. Вопросам методологии квалификационного анализа и сертификации посвящен отдельный документ — "Общая методология оценки безопасности информационных технологий" [20].

Таким образом, "Единые критерии" обеспечивают нормативную поддержку процесса выбора ИТ-продукта, к которому предъявляются требования функционирования в условиях действия определенных угроз, служат руководящим материалом для разработчиков таких систем, а также регламентируют технологию их создания и процедуру оценки обеспечиваемого уровня безопасности.

"Единые критерии" рассматривают информационную безопасность, во-первых, как совокупность конфиденциальности и целостности информации, обрабатываемой ИТ-продуктом, а также доступности ресурсов ВС, и, во-вторых, ставят перед средствами защиты задачу противодействия угрозам, актуальным для среды эксплуатации этого продукта и реализации политики безопасности, принятой в этой среде эксплуатации.

Основная литература

6. Прохорова О.В. Информационная безопасность и защита информации: учебник/ О.В. Прохорова.-Самара: СГАСУ, 2014.-113 с.

7. Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций: направление подготовки «Информационная безопасность», специальность «Экономическая безопасность» / Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-205 с.

8. Нестеров С.А. Основы информационной безопасности: учебное пособие/ С.А. Нестеров.- СПб.: изд-во Политехн. уни-та, 2014.-322 с.

Дополнительная литература

9. Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM)

10. Загинайлов Ю.Н. Основы информационной безопасности методология защиты информации: учебное пособие/ Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-253 с.

Контрольные вопросы для самопроверки:

1.Ознакомиться со стандартами и спецификациями в области информационной безопасности
2.Выполнить практическое задание.
3.Ответить на контрольные вопросы.

Практическая работа №1: Проведение анализа защищенности объекта защиты информации.

Цель работы

- исследование терминологической базы
- закрепление знаний основного понятийного аппарата, применяемого в области защиты информации
- формирование навыка работы с нормативными документами по исследуемому вопросу
- анализ угроз информационной безопасности.

Задание:

Необходимо провести анализ защищенности объекта защиты информации по следующим разделам:

1. Виды возможных угроз
2. Характер происхождения угроз
3. Классы каналов несанкционированного получения информации
4. Источники появления угроз

Порядок выполнения работы

1. Изучить теоретический материал;
2. Согласно Вашему варианту проанализируйте возможные пути воздействия на информацию;
3. По составленной схеме проанализируйте:

3.1. Виды возможных угроз
3.2. Характер происхождения угроз
3.3. Классы каналов несанкционированного получения информации
3.4. Источники появления угроз

Форма отчетности

Отчет по практической работе должен содержать следующие сведения:

1. Название и цель работы;
2. Схема возможных путей воздействия на информацию;
3. Списки, составленные по ходу задания.

Задание для самостоятельной работы:

1. Изучить причины нарушения целостности информации;
2. Рассмотреть потенциально возможные злоумышленные действия
3. Определить класс защищенности автоматизированной системы

Рекомендации по выполнению:

Понятие *«информационная безопасность» (ИБ)* рассматривается как *состояние защищенности потребностей личности, общества и государства в информации, при котором обеспечиваются их существование и прогрессивное развитие независимо от наличия внутренних и внешних информационных угроз.* Тогда с позиции обеспечения ИБ можно определить, что под *информационной угрозой понимается воздействие дестабилизирующих факторов на состояние информированности, подвергающее опасности жизненно важные интересы личности, общества и государства.*

В законе РФ «О безопасности» дано определение угрозы безопасности как совокупности условий, факторов, создающих опасность жизненно важным интересам личности, обще-

ства и государства. Под *угрозой информации* в системах ее обработки понимается возможность возникновения на каком -либо этапе жизнедеятельности системы такого явления или события, следствием которого могут быть нежелательные воздействия на информацию. К настоящему времени известно большое количество разноплановых угроз различного происхождения, таящих в себе различную опасность для информации. Для системного представления их удобно классифицировать по виду, возможным источникам, предпосылкам появления и характеру проявления.

Виды угроз Определив понятие «угроза государству, обществу и личности» в широком смысле, рассмотрим его относительно не посредственного воздействия на конфиденциальную информацию, обрабатываемую на каком-либо объекте (кабине те, предприятии, фирме). Анализируя возможные пути воздействия на информацию, представляемую как совокупность *n* информационных элементов, связанных между собой логическими связями (рис. 1), можно выделить основные нарушения:

— физической целостности (уничтожение, разрушение элементов);

— логической целостности (разрушение логических связей);

— содержания (изменение блоков информации, внешнее навязывание ложной информации);

— конфиденциальности (разрушение защиты, уменьшение степени защищенности информации),

— прав собственности на информацию (несанкционированное копирование, использование).

С учетом этого для таких объектов систем угроза информационной безопасности представляет реальные или потенциально возможные действия или условия, приводящие к овладению конфиденциальной информацией, хищению, искажению, изменению, уничтожению ее и сведений о самой системе, а также к прямым материальным убыткам.

*Предпосылки появления угр**оз*** Существуют следующие предпосылки, или причины, появления угроз:

— *объективные* (количественная или качественная недостаточность элементов системы) — не связанные непосредственно с деятельностью людей и вызывающие случайные по характеру происхождения угрозы;

— *субъективные* — непосредственно связанные с деятельностью человека и вызывающие как преднамеренные (деятельность разведок иностранных государств, промышленный шпионаж, деятельность уголовных элементов и недобросовестных сотрудников), так и непреднамеренные (плохое психофизиологическое состояние, недостаточная подготовка, низкий уровень знаний) угрозы информации.

Взаимодействие угроз можно представить на рис . 3

Перечисленные разновидности предпосылок интерпретируются следующим образом:

— *количественная недостаточность* — физическая не хватка одного или нескольких элементов системы обработки, вызывающая нарушения технологического процесса обработки или перегрузку имеющихся элементов;

— *качественная недостаточность* — несовершенство конструкции (организации) элементов системы, в силу чего может появляться возможность случайного или преднамеренного негативного воздействия на обрабатываемую или хранимую ин формацию;

— *деятельность разведорганов иностранных государств* — специально организуемая деятельность государственных органов разведки , профессионально ориентированных на добывание необходимой информации всеми доступными способами и средствами;

— *промышленный шпионаж:* — негласная деятельность отечественны х и зарубежных промышленных организаций (фирм), направленная на по лучение незаконным путем конфиденциальной информации, используемой для достижения промышленных, коммерческих, политических или подрывных целей;

— *злоумышленные действия уголовных элементов* — хищение информации, средств ее обработки или компьютерных программ в целях наживы или их разрушение в интересах конкурентов;

— плохое *психофизиологическое состояние* — постоянное или временное психофизиологическое состояние сотрудников, приводящее при определенных нестандартных внешних воздействиях к увеличению ошибок и сбоев в обслуживании систем обработки информации или непосредственно к разглашению конфиденциальной информации;

— *недостаточная качественная подготовка сотрудников* — уровень теоретической и практической подготовки персонала к выполнению задач по защите информации, недостаточная степень которого может привести к нарушению процесса функционирования системы защиты информации.

Под действием рассмотренных выше угроз может произойти утечка защищаемой информации, то есть несанкционированное, неправомерное завладение соперником данной информацией и возможность использования ее в своих, в ущерб интересам собственника (владельца) информации, целях. При этом образуется канал утечки информации, *под которым* понимается физический путь от источника конфиденциальной информации к злоумышленнику. Для его возникновения необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства восприятия и фиксации информации на стороне злоумышленника .

С учетом все х возможных путей утечки информации рассмотрим модель канала ее утечки (рис. 5), которую формально можно представить следующим выражением:

EOC = {I, C, Z, S, N, R}, (1)

где I — множество источников конфиденциальной и нформации;

C — множество объектов сис темы обработки информации (СОИ);

Z = {Za, Zn, ZOT} — множество механизмов защиты технического и организационно-технического типа;

S= {o, a, e, *m)* — среда распространения сигналов, включающая оптическую, акустическую, электромагнитную и материально -вещественную составляющие;

N = {Nc, NH} — множество шумовых сигналов естественного и искусственного происхождения;

R — оптимальный приемник перехвата.

Легальные каналы утечки информации — это использование соперником открытых источников информации (литературы, периодических изданий и т. п), обратный инжиниринг, выведывание под благовидным предлогом информации у лиц, располагающих интересующей соперника информацией, и других возможностей. В основу классификации ПНЦИ положен показатель, характеризующий степень участия в этом процессе человека. В соответствии с таким подходом ПНЦИ делятся на два вида (объективные и субъективные) и на следующие классы

Для предотвращения возможной утечки конфиденциальной информации и нарушения ее целостности на объектах ее обработки разрабатывается и внедряется система защиты информации. Система защиты информации — совокупность взаимосвязанных средств, методов и мероприятий, направленных на предотвращение уничтожения, искажения, несанкционированного получения конфиденциальных сведений, отображенных физическими полями, электромагнитными, световыми и звуковыми волнами или вещественно-материальными носителями в виде сигналов, образов, символов, технических решений и процессов.

Основная литература

11. Прохорова О.В. Информационная безопасность и защита информации: учебник/ О.В. Прохорова.-Самара: СГАСУ, 2014.-113 с.

12. Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций: направление подготовки «Информационная безопасность», специальность «Экономическая безопасность» / Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-205 с.

13. Нестеров С.А. Основы информационной безопасности: учебное пособие/ С.А. Нестеров.- СПб.: изд-во Политехн. уни-та, 2014.-322 с.

Дополнительная литература

14. Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM)

15. Загинайлов Ю.Н. Основы информационной безопасности методология защиты информации: учебное пособие/ Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-253 с.

Контрольные вопросы для самопроверки:

1. Каковы причины нарушения целостности информации?
2. Назовите потенциально возможные злоумышленные действия.
3. Как определить класс защищенности автоматизированной системы?

Практическая работа №2: Проведение анализа увеличения защищенности объекта защиты информации.

Цель работы: исследование терминологической базы; закрепление знаний основного понятийного аппарата, применяемого в области защиты информации; формирование навыка работы с нормативными документами по исследуемому вопросу; анализ угроз информационной безопасности

Задание: проведение анализа защищенности объекта защиты информации

Порядок выполнения работы

Необходимо предложить анализ увеличения защищенности объекта защиты информации по следующим разделам:

- Определить требования к защите информации
- Классифицировать автоматизированную систему
- Определить факторы, влияющие на требуемый уровень защиты информации

Форма отчетности:

Отчет по практической работе должен содержать следующие сведения:

1. Название и цель работы;
2. Схема возможных путей воздействия на информацию;
3. Списки, составленные по ходу задания.

Задание для самостоятельной работы:

- Выбрать или разработать способы и средства защиты информации
- Построить архитектуру систем защиты информации
- Сформулировать рекомендации по увеличению уровня защищенности

Рекомендации по выполнению:

Система защиты информации (СЗИ) в самом общем виде может быть определена как организованная совокупность всех средств, методов и мероприятий, выделяемых (предусматриваемых) на объекте информатизации (ОИ) для решения в ней выбранных задач по защите. Введением понятия СЗИ определяется тот факт, что все ресурсы, выделяемые для защиты информации, должны объединяться в единую, целостную систему, которая является функционально самостоятельной подсистемой любого ОИ. Таким образом, важнейшим концептуальным требованием к СЗИ является требование адаптируемости, то есть способности к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования ОИ. Важность требования адаптируемости обусловливается, с одной стороны, возможностью изменяться перечисленным факторам, а с другой — отношением процессов защиты информации к слабоструктурированным, то есть имеющим высокий уровень неопределенности. Управление же слабоструктурированными процессами может быть эффективным лишь при условии адаптируемости системы управления. Помимо общего концептуального требования, к СЗИ предъявляется еще целый ряд более конкретных, целевых требований, которые могут быть разделены на:

— функциональные;
— эргономические;
— экономические;
— технические;
— организационные.

Сформированная к настоящему времени система включает следующий перечень общеметодологических принципов:

— концептуальное единство;
— адекватность требованиям;
— гибкость (адаптируемость);
— функциональная самостоятельность;
— удобство использования;
— минимизация предоставляемы х прав;
— полнота контроля;
— адекватность реагирования;
— экономичность.

Концептуальное единство означает, что архитектура, технология, организация и обеспечение функционирования как СЗИ в целом, так и составных ее компонентов должны рассматриваться и реализовываться в строгом соответствии с основными положениями е диной концепции защиты информации. Адекватность требованиям означает, что СЗИ должна строиться в строгом соответствии с требованиями к за щите, которые, в свою очередь, определяются категорией соответствующего объекта и значениями параметров, влияющих на защиту информации.

Основы архитектурного построения СЗИ

Рассмотрим далее основные вопросы архитектурного построения СЗИ, которая, как отмечалось выше, является функциональной подсистемой ОИ. Следовательно, ее архитектура также должна быть аналогичной архитектуре ОИ и представлять собой функциональное, организационное и структурное построение.

Функциональным построением любой системы называется организованная совокупность функционально разграниченных элементов СЗИ (рис.2). Исходя из анализа необходимости нейтрализации основных видов угроз информации и реализации основных методов за щиты информации, а также в соответствии с подходами, определенными руководящим документом Государственной технической комиссии, функциональное построение СЗИ можно представить совокупностью следующих подсистем.

1. Ограничения доступа. Подсистема должна выполнять функции идентификации, проверки подлинности (аутентификации) и контроля доступа пользователей конфиденциальной информацией и программ (процессов) к ресурсам:
— системе;
— терминалам;
— ЭВМ (ПЭВМ), типам сети ЭВМ (ПЭВМ);
— каналам связи;
— внешним устройствам ЭВМ (ПЭВМ);
— программам;
— томам, каталогам, файлам, записям, полям записей;
— носителям конфиденциальной информации.

Данные функции могут реализовываться на объекте с помощью специализированных систем контроля и управления доступом (СКУД), включающих программные средства аутентификации и регистрации и технические устройства ограничения доступа. Доступ к ПЭВМ в основном обеспечивается программными средствами защиты. В настоящее время на действующих объектах ИТКС СН ограничение доступа осуществляется главным образом организационными методами. При наличии на объекте информационных ресурсов с несколькими степенями конфиденциальности и пользователей с различными правами доступа подсистема должна реализовывать механизм разграничения доступа, в основе которого могут лежать существующие модели такого доступа (на основе матрицы доступа, мандатные, многоуровневые модели).

2. Криптографической защиты. Подсистема реализует функцию шифрования конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, а также на съемные носители данных (ленты, диски, дискеты, микрокассеты и т. п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа, а также информации, передаваемой по линиям связи. Доступ к операциям шифрования и/или криптографическим клю-

чам контролируется посредством подсистемы управления доступом. Криптографическая подсистема реализуется в виде:
— программно-аппаратных или программных средств, разрабатываемых (используемых) на основе действующих алгоритмов криптографического преобразования, криптосхемы, реализующей выбранный алгоритм, или других аттестованных аппаратных средств, предназначенных для шифрования/дешифрования с целью снятия грифа секретности информации, записываемой на учтенных носителях, внешних запоминающих устройствах ЭВМ (накопителях) или передаваемой по линиям связи;
— других криптографических средств для шифрования/дешифрования информации, включая служебную информацию СЗИ НСД (ключи, пароли, таблицы санкционирования и т. п.).
3. Обеспечения целостности. Является обязательной для любой СЗИ и включает организационные, программно-аппаратные и другие средства и методы, обеспечивающие:
— контроль целостности программных средств АС и СЗИ на предмет их несанкционированного изменения;
— периодическое и/или динамическое тестирование функций СЗИ НСД с помощью специальных программных средств;
— наличие администратора (службы) защиты информации, ответственного за ведение, нормальное функционирование и контроль работы СЗИ НСД;
— восстановление СЗИ НСД при отказе и сбое;
— резервирование информационных ресурсов на других типах носителей;
— применение сертифицированных (аттестованных) средств и методов защиты, сертификация которых проводится специальными и испытательными центрами.

Основная литература

1. Прохорова О.В. Информационная безопасность и защита информации: учебник/ О.В. Прохорова.-Самара: СГАСУ, 2014.-113 с.
2. Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций: направление подготовки «Информационная безопасность», специальность «Экономическая безопасность» / Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-205 с.
3. Нестеров С.А. Основы информационной безопасности: учебное пособие/ С.А. Нестеров.- СПб.: изд-во Политехн. уни-та, 2014.-322 с.

Дополнительная литература

4. Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM)
5. Загинайлов Ю.Н. Основы информационной безопасности методология защиты информации: учебное пособие/ Ю.Н. Загинайлов.-М.: Берлин: Директ-Медиа, 2015.-253 с.

Контрольные вопросы для самопроверки:

Назовите способы и средства защиты информации.

Что такое система защиты информации?

Сформулируйте рекомендации по увеличению уровня защищенности компьютерных систем.

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Для проведения лекций по дисциплине используются специализированные аудитории с мультимедийным оборудованием или с возможностями подключения к такому оборудованию, позволяющему демонстрировать на большом экране приемы работы с персональным компьютером и другой лекционный материал.

Для проведения лабораторных занятий по дисциплине и для самостоятельной работы студентов используются специализированные аудитории, оснащенные терминалами и персональными компьютерами, подключенными к центральному серверу, обеспечивающему технические характеристики обслуживания терминалов или персональных компьютеров, по-

зволяющие при проведении лабораторных занятий использовать современное программное обеспечение.
ОС Windows 7 Professional
Microsoft Office 2007 Russian Academic OPEN No Level
Антивирусное программное обеспечение Kaspersky Security.

11.ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Вид занятия *(Лк, Лр , кр)*	***Наименование аудитории***	***Перечень основного оборудования***	***№ Лр***
1	**3**	**4**	**5**
Лк	Лекционная аудитория		№ 1.1 -3.2
ПЗ	Лаборатория технических средств защиты информации	Оборудование 16-ПК i5-2500/H67/4Gb/500Gb (монитор TFT19 Samsung E1920NR); интерактивная доска Smart Board X885ix со встроенным проектором UX60	
ЛР	Лаборатория технических средств защиты информации	Оборудование 16-ПК i5-2500/H67/4Gb/500Gb (монитор TFT19 Samsung E1920NR); интерактивная доска Smart Board X885ix со встроенным проектором UX60	№ 1-5
СР	Читальный зал №1	Оборудование 10 ПК i5-2500/H67/4Gb(монитор TFT19 Samsung); принтер HP LaserJet P2055D	-

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1. Описание фонда оценочных средств (паспорт)

№ компетенции	Элемент компетенции	Раздел	Тема	ФОС
ПК-7	способность к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения	1. Общие вопросы оценки безопасности компьютерных систем	1.1. Предметная область оценки безопасности компьютерных систем.	Вопросы к зачету 1.1 – 1.2
			1.2 Исторические сведения и этапы развития оценки безопасности компьютерных систем.	Вопрос к зачету 1.3
			1.3 Математические основы оценки безопасности компьютерных систем	Вопросы к зачету 1.4 – 1.5
ПК-9	способность составлять и контролировать план выполняемой работы, планировать необходимые для выполнения работы ресурсы, оценивать результаты собственной работы	2. Методы и средства оценки безопасности компьютерных систем	2.1 Анализ рисков в области защиты информации	Вопросы к зачету 2.1 – 2.4
			2.2 Управление рисками и международные стандарты	Вопросы к зачету 2.5. – 2.10
			2.3 Технологии анализа рисков	Вопросы к зачету 2.11 – 2.17
		3. Организация оценки безопасности компьютерных систем	3.1 Организация службы информационной безопасности	Вопросы к зачету 3.1 - 3.5
			3.2 Формирование экспертных систем оценки безопасности компьютерных систем	Вопросы к зачету 3.6 – 3.11

1. Вопросы к зачету, 7 семестр

№ п/п	Компетенции		ВОПРОСЫ К ЗАЧЕТУ 7 семестр	№ и наименование раздела
	Код	Определение		
1	2	3	4	5
1.	ПК-7	способность к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения	1.1 Предметная область оценки безопасности компьютерных систем	1. Общие вопросы оценки безопасности компьютерных систем.
			1.2 Этапы развития оценки безопасности компьютерных систем	
			1.3 Законодательная и нормативно-правовая база в области оценки безопасности компьютерных систем	
			1.4 Основные методы оценки безопасности компьютерных систем	
			1.5 Основные средства оценки безопасности компьютерных систем	
			2.1 Современные подходы к управлению рисками в компьютерных системах	**2.** Методы и средства оценки безопасности компьютерных систем
			2.2 Риск-модель компьютерной системы Алгоритм вычисления комплексного риска	
			2.3 Алгоритм управления информационными рисками	
			2.4 Политика безопасности. Критерии оценки безопасности информационных технологий	
			2.5 Аудит безопасности, оценка действующего уровня защищенности в компьютерных системах	
			2.6 Средства защиты в компьютерных системах	
			2.7 Технология оценки рисков в компьютерных системах	
			2.8 Оценка потенциального ущерба при осуществлении угроз в компьютерных системах	
			2.9 Теоретико-вероятностный метод оценки рисков в компьютерных системах	
			2.10 Экспертный метод оценки рисков в компьютерных системах	
			2.11Статистический метод оценки рисков в компьютерных системах	
	ПК-9	способность составлять и кон-	2.12 Вероятностно-статистический метод оценки рисков в компьютерных	

		тролировать план выполняемой работы, планировать необходимые для выполнения работы ресурсы, оценивать результаты собственной работы	системах	
			2.13 Взаимосвязь угроз, уязвимостей и рисков	
			2.14 Оценки защищенности на основе модели комплекса механизмов защиты	
			2.15 Семантические показатели защищенности компьютерных систем	
			2.16 Нечеткие оценки защищенности компьютерных систем	
			2.17 Комплексные оценки защищенности	
			3.1 Организационные меры по обеспечению безопасности в компьютерных системах	**3.** Организация оценки безопасности компьютерных систем
			3.2 Методы тестирования системы защиты	
			3.3 Система обнаружения вторжений	
			3.4 Жизненный цикл компьютерных систем.	
			3.5 Защита информации от несанкционированного доступа	
			3.6 Защита от копирования. Защита от вирусов	
			3.7 Руководство по разработке профилей защиты и заданий по информационной безопасности компьютерных систем	
			3.8 Парольная защита	
			3.9 Биометрическая защита компьютерных систем	
			3.10 Порядок организации оценки безопасности компьютерных систем	
			3.11 Технические меры обеспечения безопасности компьютерных систем	

3. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
Знать: *(ПК-7)* - основные понятия, идеи, методы, связанные с дисциплинами фундаментальной математики, информатики - методы и средства	**Отлично**	Демонстрирует все показатели на высоком уровне. Обучающийся всесторонне и глубоко владеет знаниями в области методов оценки безопасности компьютерных систем, технологиями анализа рисков, сложными навыками, способен уверенно ориентироваться в практических ситуациях. Достигнут высокий уровень формирования компетенций.

оценки безопасности компьютерных систем *(ПК-9)* – методы планирования, анализа и корректировки выполнения планов выполняемой работы и оценки результатов; **Уметь:** *(ПК-7)* - систематизировать методы оценки безопасности компьютерных систем. *(ПК-9)* – составлять, контролировать, корректировать и оценивать результаты деятельности, необходимые для выполнения работы. **Владеть:** *(ПК-7)* - навыками оценки действующего уровня защищенности в компьютерных системах. – технологиями анализа рисков. *(ПК-9)* - навыкам планирования выполняемой работы, оценки ресурсов и результатов собственной деятельности.		
	Хорошо	Демонстрирует более половины показателей на достаточном и высоком уровне. Обучающийся владеет знаниями в области методов оценки безопасности компьютерных систем, технологиями анализа рисков, проявляет соответствующие навыки в практических ситуациях, но имеют место некоторые неточности в демонстрации освоения материала. Достигнут повышенный уровень формирования компетенции.
	Удовлетворительно	Демонстрирует основную часть показателей на достаточном уровне. Обучающийся частично проявляет знания и навыки в области методов оценки безопасности компьютерных систем, технологиями анализа риск, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается. Достигнут только базовый уровень формирования компетенции.
	Неудовлетворительно	Демонстрирует большинство показателей на недостаточном и крайне низком уровне. Обучающийся не владеет необходимыми знаниями и навыками в области методов оценки безопасности компьютерных систем, технологиями анализа риск и не старается их применять. Не достигнут базовый уровень формирования компетенции.

4.Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности

Дисциплина Методы обеспечения безопасности компьютерных систем направлена на углубление знаний о сборе и анализе исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности, а так же проведение проектных, расчетов элементов систем обеспечения информационной безопасности.

Изучение дисциплины предусматривает:

– лекции,
– лабораторные работы;
– практические работы;
– зачет;
– самостоятельную работу студента в объемах часов, соответствующих учебному плану направления.

Студентам необходимо овладеть навыками и умениями применения изученных методов для разработки и реализации профессионально ориентированных проектов в последующей учебной деятельности, а так же ключевыми понятиями являющиеся основой усвоения учебного материала по дисциплине.

При подготовке к экзамену особое внимание необходимо уделить рекомендациям и замечаниям преподавателей, ведущих аудиторные занятия по дисциплине.

В процессе проведения лабораторных занятий происходит закрепление знаний, формирование умений и навыков применения различных методов решения стандартных ситуаций.

Самостоятельную работу необходимо начинать с чтения лекций и учебников.

В процессе консультации с преподавателем обучающийся выясняет наличие пробелов в знаниях и способах решения разных ситуаций.

Работа с литературой является важнейшим элементом в получении знаний по дисциплине. Прежде всего, необходимо воспользоваться списком рекомендуемой по данной дисциплине литературой. Дополнительные сведения по изучаемым темам можно найти в периодической печати и Интернете.

Предусмотрено проведение аудиторных занятий в виде разнообразных тренингов и ситуаций общения в сочетании с внеаудиторной работой.

Приложение 2

АННОТАЦИЯ
рабочей программы дисциплины
Методы оценки безопасности компьютерных систем

1. **Цель и задачи дисциплины**

Изучение принципов и методов оценки безопасности компьютерных систем на основе комплексного подхода к определению актуальных угроз безопасности в таких системах в рамках обеспечения безопасности информационных систем и технологий в целом, изучение математических основ моделирования процессов оценки безопасности компьютерных систем, получение профессиональных компетенций в области современных технологий оценки безопасности компьютерных систем.

Основные задачи дисциплины:

- обучение студентов базовым понятиям современных методов оценки безопасности компьютерных систем;
- обучение студентов базовым методам оценки безопасности компьютерных систем;
- овладение практическими навыками применения методов оценки безопасности компьютерных систем;
- раскрытие физической сущности построения и эксплуатации компьютерных систем с точки зрения определения актуальных угроз безопасности в таких системах с целью корректного решения задач по применению методов оценки безопасности компьютерных систем.

2. **Структура дисциплины**

2.1 Распределение трудоемкости по отдельным видам учебных занятий, включая самостоятельную работу: Лк.-17 час., ЛР-17час., ПР-17час, СР-48 час.

Общая трудоемкость дисциплины составляет**...**144 часа, 4 зачетных единиц.

2.2 Основные разделы дисциплины:

1 - Общие вопросы оценки безопасности компьютерных систем.
2 - Методы и средства оценки безопасности компьютерных систем.
3 - Организация оценки безопасности компьютерных систем.

3. **Планируемые результаты обучения (перечень компетенций)**

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПК-7 способность к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения.

ПК-9 - способность составлять и контролировать план выполняемой работы, планировать необходимые для выполнения работы ресурсы, оценивать результаты собственной работы

4. **Виды промежуточной аттестации**: зачет.

Приложение 3

Протокол о дополнениях и изменениях в рабочей программе
на 20___-20___ учебный год

1. В рабочую программу по дисциплине вносятся следующие дополнения:
_____
_____

2. В рабочую программу по дисциплине вносятся следующие изменения:

_____
_____
_____

Протокол заседания кафедры №____ от «___» _____ 20 ___ г.,
(разработчик)

Заведующий кафедрой _____ _____
(подпись) *(Ф.И.О.)*

Приложение 4

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ ПО ДИСЦИПЛИНЕ

1. Описание фонда оценочных средств (паспорт)

№ компетенции	Элемент компетенции	Раздел	Тема	ФОС
ПК-7	способность к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения	1. Общие вопросы оценки безопасности компьютерных систем	1.1. Предметная область оценки безопасности компьютерных систем.	Индивидуальное задание Отчет по ПЗ
			1.2 Исторические сведения и этапы развития оценки безопасности компьютерных систем.	Индивидуальное задание Отчет по ПЗ
			1.3 Математические основы оценки безопасности компьютерных систем	Индивидуальное задание Отчет по ПЗ
ПК-9	способность составлять и контролировать план выполняемой работы, планировать необходимые для выполнения работы ресурсы, оценивать результаты собственной работы	2. Методы и средства оценки безопасности компьютерных систем	2.1 Анализ рисков в области защиты информации	Индивидуальное задание Отчет по ПЗ
			2.2 Управление рисками и международные стандарты	Индивидуальное задание Отчет по ПЗ
			2.3 Технологии анализа рисков	Индивидуальное задание Отчет по ПЗ
		3. Организация оценки безопасности компьютерных систем	3.1 Организация службы информационной безопасности	Индивидуальное задание Отчет по ПЗ
			3.2 Формирование экспертных систем оценки безопасности компьютерных систем	Индивидуальное задание Отчет по ПЗ

2. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
Знать: *(ПК-7)* - основные понятия, идеи, методы, связанные с дисциплинами фундаментальной математики, информатики - методы и средства оценки безопасности компьютерных систем *(ПК-9)* – методы планирования, анализа и корректировки выполнения планов выполняемой работы и оценки результатов; **Уметь:** *(ПК-7)* - систематизировать методы оценки безопасности компьютерных систем. *(ПК-9)* – составлять, контролировать, корректировать и оценивать результаты деятельности, необходимые для выполнения работы. **Владеть:** *(ПК-7)* - навыками оценки дейст-	**Отлично**	Демонстрирует все показатели на высоком уровне. Обучающийся всесторонне и глубоко владеет знаниями в области методов оценки безопасности компьютерных систем, технологиями анализа рисков, сложными навыками, способен уверенно ориентироваться в практических ситуациях. Достигнут высокий уровень формирования компетенций.
	Хорошо	Демонстрирует более половины показателей на достаточном и высоком уровне. Обучающийся владеет знаниями в области методов оценки безопасности компьютерных систем, технологиями анализа рисков, проявляет соответствующие навыки в практических ситуациях, но имеют место некоторые неточности в демонстрации освоения материала. Достигнут повышенный уровень формирования компетенции.
	Удовлетворительно	Демонстрирует основную часть показателей на достаточном уровне. Обучающийся частично проявляет знания и навыки в области методов оценки безопасности компьютерных систем, технологиями анализа риск, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается. Достигнут только базовый уровень формирования компетенции.

вующего уровня защищенности в компьютерных системах. – технологиями анализа рисков. *(ПК-9)* - навыкам планирования выполняемой работы, оценки ресурсов и результатов собственной деятельности.	**Неудовлетворительно**	Демонстрирует большинство показателей на недостаточном и крайне низком уровне. Обучающийся не владеет необходимыми знаниями и навыками в области методов оценки безопасности компьютерных систем, технологиями анализа риск и не старается их применять. Не достигнут базовый уровень формирования компетенции.

Программа составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 01.03.02 Прикладная математика и информатика от «12» марта 2015 г. №228

для набора 2015 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «13» июля 2015 г. №475

для набора 2016 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «06»июня 2016 г. №429

для набора 2017 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «06» марта 2017 г. №125

для набора 2018 года и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «12» марта 2018 г. №130

Программу составил:

Сташок О.В. к.т.н, доцент каф. математики и физики _____

Рабочая программа рассмотрена и утверждена на заседании кафедры математики и физики

от «21» ноября 2018 г., протокол № 3

Заведующий кафедрой
Математики и физики _____ О.И.Медведева

СОГЛАСОВАНО:
Заведующий выпускающей кафедрой МиФ _____ О.И Медведева

Директор библиотеки _____ Т.Ф.Сотник

Рабочая программа одобрена методической комиссией ЕН факультета

от «20» декабря 2018 г., протокол № 4
Председатель методической комиссии факультета _____ М.А. Варданян

СОГЛАСОВАНО:
Начальник
учебно-методического управления _____ Г.П. Нежевец

Регистрационный №_____

(методический отдел)