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

ПРОГРАМНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Б1.ВДВ.07.01

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 проектному и производственно-технологическому виду профессиональной деятельности выпускника в соответствии с компетенциями и видами деятельности, указанными в учебном плане.

Цель дисциплины

Формирование у обучающихся знаний по основам защиты информации в компьютерных системах, при помощи программных средств, а также навыков и умения в применении знаний для конкретных условий.

Развитие в процессе обучения системного мышления, необходимого для решения задач защиты информации с учетом требований системного подхода.

Задачи дисциплины

Дать знания по концепции обеспечения информационной безопасности компьютерных систем:

– программным средствам, реализующим отдельные функциональные требования по защите;

– методам и средствам хранения ключевой информации;

– методам и средствам ограничения доступа к компонентам вычислительных систем;

– защите программ от изменения и контролю целостности.

Код компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
1	2	3
ОПК-4	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности	**знать** – основные стандарты ИБ. **уметь** – решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности. **владеть** – навыками применения информационно-коммуникационных технологий с учетом основных требований информационной безопасности.
ПК-6	Способность формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций	**знать** – принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; – способы формирования суждений о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций. **уметь** – настраивать и эксплуатировать программные

		средства; – разрабатывать политику информационной безопасности. **владеть** – профессиональной терминологией; – навыками формирования суждений о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В.ДВ.07.01 Программные средства защиты информации относится к элективной части.

Дисциплина Программные средства защиты информации базируется на знаниях, полученных при изучении таких учебных дисциплин, как: Методы обеспечения безопасности компьютерных систем, Дискретная математика, Операционные системы, Теоретические основы информационной безопасности, Компьютерные сети.

Основываясь на изучении перечисленных дисциплин, Программные средства защиты информации представляет основу для 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	8	108	48	24	24	-	60	-	Зачет
Заочная	-	-	-	-	-	-	-	-	-	-
Заочная (ускоренное обучение)	-	-	-	-	-	-	-	-	-	-
Очно-заочная	-	-	-	-	-	-	-	-	-	-

3.2. Распределение объема дисциплины по видам учебных занятий и трудоемкости

Вид учебных занятий	*Трудо-емкость (час.)*	*в т.ч. в интерактивной, активной, инновационной формах, (час.)*	*Распределение по семестрам, часам*
			8
1	**2**	**3**	**4**
I. Контактная работа обучающихся с преподавателем (всего)	48	30	48
Лекции (Лк)	24	6	24
Лабораторные работы (ЛР)	24	24	24
II.Самостоятельная работа обучающихся (СР)	60	-	60
Подготовка к лабораторным работам	40	-	40
Подготовка к зачету	20	-	20
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*	
1	**2**	**3**	**4**	**5**	**6**
1.	**Программно-аппаратные средства обеспечения информационной безопасности.**	**54**	**12**	**12**	**30**
1.1.	Методы и средства защиты программного обеспечения.	25	5	5	15
1.2.	Построение изолированной программной среды.	29	7	7	15
2.	**Обеспечение информационной безопасности компьютерных сетей.**	**54**	**12**	**12**	**30**
2.1.	Стандарты информационной безопасности.	54	12	12	30
	ИТОГО	**108**	**24**	**24**	**60**

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.	Программно-аппаратные средства обеспечения информационной безопасности	Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности. Концепция диспетчер адоступа. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите. Их принципы действия и технологические особенности. Взаимодействие с общесистемными компонентами вычислительных систем	Лекция-беседа (2 час.)
1.1.	Методы и средства защиты программного обеспечения	Понятие политики безопасности. Описание типовых политик безопасности. Угрозы безопасности компьютерных систем. Модель политики безопасности на основе дискретных компонент АДЕПТ-50. Методы и средства ограничения доступа к компонентам вычислительных систем. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Методы и средства хранения ключевой информации. Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение. Защита от разрушающих программных воздействий. Защита программ от изменения и контроль целостности	
1.2.	Построение изолированной	Модель компьютерной системы. Понятие монитора безопасности. Обеспечение гарантий выполнения	

	программной среды.	политики безопасности. Метод генерации изолированной программной среды при проектировании механизмов гарантированного поддержания политики безопасности. Модели безопасного взаимодействия в КС. Процедура идентификации и аутентификации: защита на уровне расширений Bios, защита на уровне загрузчиков операционной среды.	
2.	Обеспечение информационной безопасности компьютерных сетей.	Программно-аппаратные средства защиты информации в сетях передачи данных. Межсетевые экраны. Свойства экранирующего субъекта. Классификация требований к классам межсетевых экранов	Лекция-беседа (2 час.)
2.1.	Стандарты информационной безопасности.	Роль стандартов информационной безопасности. Документы Государственной технической комиссии России. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности. Основные категории требований к программной и программно- аппаратной реализации средств обеспечения информационной безопасности. Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Требования к процессу сертификации продукта информационных технологий	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.**	Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения	6	Работа в малой группе (6 час)
2	**1.**	Средства и системы защиты программного обеспечения	6	Работа в малой группе(6 час)
3	**1.**	Фиксация программного комплекса	6	Работа в малой группе (6 час)
4	**1.**	Статический анализ исходных текстов на предмет полноты и отсутствия избыточности	6	Работа в малой группе(6 час)
		ИТОГО	**24**	**24**

4.4. Практические занятия

Учебным планом не предусмотрено.

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*		*Σ комп.*	$t_{ср}$, *час*	*Вид учебных занятий*	*Оценка результатов*
		ОПК	*ПК*				
		4	*6*				
1	2	3	4	5	6	7	8
1. Программно-аппаратные средства обеспечения информационной безопасности	54	+	+	2	27	Лк, ЛР	зачет
2. Обеспечение информационной безопасности компьютерных сетей**.**	54	+	+	2	27	Лк, ЛР	зачет
всего часов	**108**	**54**	**54**	**2**	**54**		

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

1. Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014, -314 с.
http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

2. Баранова, Е. К. Криптографические методы защиты информации. Лабораторный практикум : учебное пособие для бакалавриата и магистратуры / Е. К. Баранова, А. В. Бабаш. - Москва : КноРус, 2017. - 200 с.

3. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск : БрГУ, 2010. - 100 с. [электронный ресурс]
http://ecat.brstu.ru/catalog/Учебные%20и%20учебно-методические%20пособия/Информатика%20-%20Вычислительная%20техника%20-%20Программирование/Иванов%20М.Ю.%20Информационные%20технологии.Методы%20криптографии.2010.pdf

4. Ярочкин, В. И. Информационная безопасность : учебник для вузов / В. И. Ярочкин. - Москва : Академический Проект, 2003. - 640 с.

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

№	*Наименование издания*	*Вид занятия*	*Количество экземпляров в библиотеке,* шт.	*Обеспеченность,* (экз./ чел.)
1	**2**	**3**	**4**	**5**
Основная литература				
1.	1. Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014, -314 с. http://biblioclub.ru/index.php?page=book_view_red&book_id=428605	СРС, лк	1 (ЭУ)	1
2.	Партыка, Т. Л. Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. - 5-е изд., перераб. и доп. - Москва : Форум; Инфра-М, 2014. - 432 с.	ЛР, лк	10	0.7
Дополнительная литература				
3.	Бабаш, А. В. Информационная безопасность. Лабораторный практикум : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. - Москва : Кнорус, 2012. - 136 с.	ЛР	10	0.67
4.	Баранова, Е. К. Криптографические методы защиты информации. Лабораторный практикум : учебное пособие для бакалавриата и магистратуры / Е. К. Баранова, А. В. Бабаш. - Москва : КноРус, 2017. - 200 с.	ЛР, СРС	4	0.27
5.	Иванов, М. Ю. Информационная безопасность : методические указания к выполнению лабораторных работ / М. Ю. Иванов. - Братск : БрГУ, 2014. - 44 с.	ЛР	20	1

6.	Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск : БрГУ, 2010. - 100 с. [электронный ресурс] http://ecat.brstu.ru/catalog/Учебные%20и%20учебно-методические%20пособия/Информатика%20-%20Вычислительная%20техника%20-%20Программирование/Иванов%20М.Ю.%20Информационные%20технологии.Методы%20криптографии.2010.pdf	лк, СРС	31(ЭР)	1
7.	Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - Москва : Юрайт, 2012. - 564 с	лк	16	1
8.	Ярочкин, В. И. Информационная безопасность : учебник для вузов / В. И. Ярочкин. - Москва : Академический Проект, 2003. - 640 с.	Лк, СРС	25	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

Обучающийся должен разработать собственный режим равномерного освоения дисциплины. Подготовка студента к предстоящей лекции включает в себя ряд важных познавательно-практических этапов:

– чтение записей, сделанных в процессе слушания и конспектирования предыдущей лекции, вынесение на поля всего, что требуется при дальнейшей работе с конспектом и учебником;

– техническое оформление записей (подчеркивание, выделение главного, выводов, доказательств);

– выполнение практических заданий преподавателя.

Подготовка к лабораторным работами содержит:

- изучение теоретического материала, содержащегося в учебной литературе, изучение лекционного материала,

- знакомство с заданиями на лабораторную работу;

- составление плана выполнения лабораторной работы.

Наиболее продуктивной является самостоятельная работа в библиотеке, где доступны основные и дополнительные печатные и электронные источники.

При выполнении приведенных выше рекомендаций подготовка к зачету сведется к повторению изученного и совершенствованию навыков применения теоретических положений и различных методов решения к стандартным и нестандартным заданиям.

9.1. Методические указания для обучающихся по выполнению лабораторных работ.

Лабораторная работа №1 Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения

Цели работы:

• закрепление полученных теоретических знаний по теме «Обеспечение безопасности программного обеспечения»;

• формирование практических умений и навыков защиты программного обеспечения от вредоносных программ п несанкционированного исследования, копирования и распространения.

Задание:

1. Приведите классификацию вредоносных программ по критерию «способ внедрения с помощью средств автоматизации программирования». Продемонстрируйте эти способы.
2. Опишите различные типы вирусов в соответствии с представленной классификацией. Приведите примеры компьютерных вирусов, с которыми вы сталкивались. К какому типу вирусов вы их отнесете?
3. Опишите средства нейтрализации компьютерных вирусов. Приведите примеры использования антивирусных комплексов.
4. Приведите классификацию методов и средств защиты программ от несанкционированного исследования.
5. Расскажите о защищенных операционных системах на основе ОС Linux.

Указания по выполнению задания. Следует обратить внимание на свойства защищенности программ на этапах производства, поставки и эксплуатации программных комплексов.

Форма отчетности

1. Наименование лабораторной работы.
2. Перечень классификаций вредоносных программ.
3. Выводы

Задание для самопроверки

1. Методы защиты программ от компьютерных вирусов.
2. Методы защиты программ от несанкционированного исследования.
3. Методы обфускации программ.
4. Методы защиты программ от несанкционированного копирования.
5. Создание защищенных операционных систем

Основная литература

1. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. - 5-е изд., перераб. и доп. - Москва : Форум; Инфра-М, 2014.

Дополнительная литература

1. .Бабаш, А. В. Информационная безопасность. Лабораторный практикум : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. - Москва : Кнорус, 2012. - 136 с.
2. Баранова, Е. К. Криптографические методы защиты информации. Лабораторный практикум : учебное пособие для бакалавриата и магистратуры / Е. К. Баранова, А. В. Бабаш. - Москва : КноРус, 2017. - 200 с.
3. Иванов, М. Ю. Информационная безопасность : методические указания к выполнению лабораторных работ / М. Ю. Иванов. - Братск : БрГУ, 2014. - 44 с

Контрольные вопросы для самопроверки:

1. Что представляет собой статический и динамический анализ программ? При помощи каких средств проводится такой анализ?
2. Как оценивается подобие целевой и исследуемой программ с точки зрения наличия вредоносных программ?
3. Каковы критерии классификации компьютерных вирусов?
4. В чем суть обфускации программ?
5. Каково определение эффективного вероятностного обфускатора?

Лабораторная работа 2 Средства и системы защиты программного обеспечения

Цели работы:

- закрепление полученных теоретических знаний
- формирование практических умений и навыков разработки и эксплуатации средств и систем защиты программного обеспечения.

Задание:

1. Перечислите достоинства и недостатки статических и динамических способов исследования ПО.
2. Объясните и сравните на конкретных примерах принципы работы дизассемблеров, декомпиляторов, трассировщиков, следящих систем при исследовании ПО.
3. Опишите способы проведения испытаний ПО. оценки качества и сертификации программных средств.
4. Опишите показатели качества ПО разных уровней, последовательность операций при выборе номенклатуры показателей качества НО.
5. Проведите оценку значений показателей качества ПО на тестовом примере.
6. Перечислите основные этапы проведения испытании ПО и последовательность действий при этом.
7. Приведите пример структурно-функциональной схемы инструментальных средств поддержки создания безопасного программного обеспечения.
8. Проведите сравнительный анализ не менее двух антивирусных комплексов. существующих на отечественном рынке, и определите их основные достоинства м недостатки.

Указания по выполнению задания. Следует обратить внимание па прикладные области применения средств защиты программного обеспечения.

Форма отчетности

1. Наименование лабораторной работы.
2. Перечень достоинств и недостатков статических и динамических способов исследования ПО.
3. Выводы

Задание для самостоятельной работы:

1. Средства и системы тестирования программного обеспечения при испытаниях его на технологическую безопасность.
2. Показатели качества программного обеспечения. Выбор номенклатуры показателей качества ПО с точки зрения его защищенности.
3. Организационные и методологические вопросы проведения испытаний ПО.
4. Построение программно-аппаратных комплексов для контроля технологической безопасности программ. Состав инструментальных средств контроля безопасности ПО при его разработке.
5. Структура и принципы построения программно-аппаратных средств контрольно-испытательного стенда испытания технологической безопасности ПО.
6. Средства и комплексы защиты программ от компьютерных вирусов. Обфускаторы программ. Средства обеспечения целостности и достоверности используемого программного кода. Средства защиты программ от несанкционированного копирования.
7. Операционные системы в защищенном исполнении. Создание операционных систем с открытым исходным кодом в защищенном исполнении.

Основная литература

1. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. - 5-е изд., перераб. и доп. - Москва : Форум; Инфра-М, 2014.

Дополнительная литература

1. .Бабаш, А. В. Информационная безопасность. Лабораторный практикум : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. - Москва : Кнорус, 2012. - 136 с.
2. Баранова, Е. К. Криптографические методы защиты информации. Лабораторный практикум : учебное пособие для бакалавриата и магистратуры / Е. К. Баранова, А. В. Бабаш. - Москва : КноРус, 2017. - 200 с.
3. Иванов, М. Ю. Информационная безопасность : методические указания к выполнению лабораторных работ / М. Ю. Иванов. - Братск : БрГУ, 2014. - 44 с

Контрольные вопросы для самопроверки:

1. Каков состав методического обеспечения проведения испытаний программ?
2. Каковы показатели качества ПО разных уровней, последовательность операции при выборе номенклатуры показателей качества ПО?
3. В чем особенности технологии создания сложных программных комплексов и действии разработчиков при обеспечении технологической безопасности ПО?
4. Какие виды работ включает в себя контроль безопасности общего и специального ПО на этане исследования и испытаний ПО?
5. Какие требования предъявляются к контрольно-испытательному стенду испытания технологической безопасности ПО?
6. Как обеспечивается функциональная эквивалентность программ до и после их обфускации?
7. Какой базовый функционал присутствует в типовых антивирусных программах?
8. Разработка каких дистрибутивов операционной системы с открытыми исходными кодами обеспечила бы учет специфики объектов, потенциально уязвимых для кибератак? Каковы основные компоненты такого дистрибутива?

Лабораторная работа 3 Фиксация программного комплекса

Цели работы:

- закрепление полученных теоретических знаний
- формирование практических умений и навыков исследования конкретных программ на предмет отсутствия недекларированных возможностей при помощи утилиты «ФИКС».

Задание :

1. Изучите эксплуатационную документацию на утилиту «ФИКС».
2. Активируйте работу утилиты «ФИКС» в режиме «Фиксация версии» для выбранного программного комплекса. Значение параметра «Статус комплекса* установите в окне New. Изучите сформированные отчеты, определите, какую именно информацию они содержат.
3. Повторите п. 2, выбирая каждый из доступных алгоритмов расчета контрольных сумм.
4. Повторите п. 2. последовательно выбирая опции «Уточнение*, «Выбор файлов», «Семантика* и Zip. Обратите внимание на влияние этих опций на выполнение утилиты и вид сформированных отчетов.
5. Внесите изменение в состав выбранного программного комплекса и проведите повторную активацию утилиты «ФИКС» в режиме «Фиксация версий», установив значение параметра «Статус комплекса» в окне New.
6. Реализуйте утилиту «ФИКС» в режиме «Сравнение версий* для ранее созданных отчетов. Изучите сформированный отчет.

Форма отчетности:

1. Наименование лабораторной работы.
2. Скриншоты работы утилиты «ФИКС»
3. Выводы.

Основная литература

2. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. - 5-е изд., перераб. и доп. - Москва : Форум; Инфра-М, 2014.

Дополнительная литература

4. .Бабаш, А. В. Информационная безопасность. Лабораторный практикум : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. - Москва : Кнорус, 2012. - 136 с.
5. Баранова, Е. К. Криптографические методы защиты информации. Лабораторный практикум : учебное пособие для бакалавриата и магистратуры / Е. К. Баранова, А. В. Бабаш. - Москва : КноРус, 2017. - 200 с.
6. Иванов, М. Ю. Информационная безопасность : методические указания к выполнению лабораторных работ / М. Ю. Иванов. - Братск : БрГУ, 2014. - 44 с

Контрольные вопросы для самопроверки :

1. Каково назначение утилиты «ФИКС»?
2. Какие криптографические алгоритмы используются для расчета контрольных сумм в «ФИКС»?
3. Где в файловой системе хранятся отчеты, формируемые в режимах «Фиксация версий» и «Фиксация и контроль каталога»?

Лабораторная работа 4 Статический анализ исходных текстов на предмет полноты и отсутствия избыточности

Цели работы:

закрепление полученных теоретических знаний

Задание:

1. Изучите представленный комплект программной документации и составьте отчет о соответствии его требованиям РД НДВ.
2. Изучите состав представленного набора исходных текстов программ. Составьте отчет о количестве и типе файлов исходных текстов, входящих в набор, и используемых языках и технологиях программирования.
3. Выполните контрольную сборку дистрибутива программного комплекса из набора исходных текстов, обоснуйте вывод о полноте представленных исходных текстов в случае успешной сборки.
4. Выполните контрольную сборку дистрибутива программного комплекса из набора исходных текстов. По результатам сборки выявите файлы, подозрительные с точки зрения избыточности. Для каждого из выявленных фалов обоснуйте его избыточность либо отсутствие избыточности.

Форма отчетности:

Вводная часть:

1. Постановка темы и цели занятия.
2. Актуализация теоретических знаний, необходимых для проведения практического занятия или выполнения лабораторной работы.

Основная часть:

1. Разработка и согласование методики выполнения задания.
2. Проведение инструктажа.
3. Определение способов фиксации полученных результатов и формата отчетных

материалов.

4. Выполнение задания формирование отчета по результатам его выполнения.

Заключительная часть:

1. Обобщение и систематизация полученных результатов.
2. Подведение итогов практического занятия или лабораторной работы и оценка работы студентов.

Основная литература

3. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. - 5-е изд., перераб. и доп. - Москва : Форум; Инфра-М, 2014.

Дополнительная литература

7. .Бабаш, А. В. Информационная безопасность. Лабораторный практикум : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. - Москва : Кнорус, 2012. - 136 с.
8. Баранова, Е. К. Криптографические методы защиты информации. Лабораторный практикум : учебное пособие для бакалавриата и магистратуры / Е. К. Баранова, А. В. Бабаш. - Москва : КноРус, 2017. - 200 с.
9. Иванов, М. Ю. Информационная безопасность : методические указания к выполнению лабораторных работ / М. Ю. Иванов. - Братск : БрГУ, 2014. - 44 с

Контрольные вопросы для самопроверки :

1. Каким должен быть состав программной документации, представляемой на сертификацию по третьему уровню контроля не декларированных возможностей?
2. Какие требования предъявляются к стендам для проведения анализа программного обеспечения?
3. Как осуществляется проверка соответствия исходных текстов объектному коду?
4. В чем состоит контроль связей но управлению информации?
5. Статический анализ исходных текстов программного обеспечения.
6. Проверка соответствия исходных файлов объектному коду.
7. Использование утилиты ЛИСТ для статического анализа исходных кодов.

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

ОС Windows 7 Professional
Microsoft Office 2007 Russian Academic OPEN No Level
Антивирусное программное обеспечение Kaspersky Security
ОС Linux
LibreOffice

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	Лаборатория параллельных вычислений	Оборудование Интерактивная доска Smart Board X885ix со встроенным проектором UX60	№ 1.1 -3.2
ЛР	Лаборатория параллельных вычислений	Оборудование 14-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
ОПК-4	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности	**1.** Программно-аппаратные средства обеспечения информационной Безопасности	1.1. Методы и средства защиты программного обеспечения	Вопросы к зачету 1-2
			1.2.Построение изолированной программной среды.	Вопросы к зачету 3-4
		2. Обеспечение информационной безопасности компьютерных сетей.	2.1. Стандарты информационной безопасности	Вопросы к зачету 5-6
ПК-6	Способность формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций	**1.** Программно-аппаратные средства обеспечения информационной Безопасности	1.1. Методы и средства защиты программного обеспечения	Вопросы к зачету 7-10
			1.2.Построение изолированной программной среды.	Вопросы к зачету 11-15
		2. Обеспечение информационной безопасности компьютерных сетей.	2.1. Стандарты информационной безопасности	Вопросы к зачету 5-16 20

2. Вопросы к зачету

№ п/п	Компетенции		ВОПРОСЫ К ЗАЧЕТУ	№ и наименование раздела
	Код	Определение		
1	2	3	4	5
1.	ОПК-4	Способность решать стандартные	1. Основные принципы создания программно-аппаратных средств обеспечения информационной	**1** Программно-аппаратные средства

		задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности	безопасности	обеспечения информационной Безопасности
			2. Концепция диспетчера доступа.	**1** Программно-аппаратные средства обеспечения информационной безопасности
			3. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите.	**1** Программно-аппаратные средства обеспечения информационной безопасности
			4. Показатели защищенности средств вычислительной техники от несанкционированного доступа.	**1** Программно-аппаратные средства обеспечения информационной безопасности
			5. Классы защищенности автоматизированных систем.	**2** Обеспечение информационной безопасности компьютерных сетей.
			6. Требования к процессу сертификации продукта информационных технологий	**2** Обеспечение информационной безопасности компьютерных сетей.
2	ПК-6	Способность формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций	7. Понятие политики безопасности.	**1** Программно-аппаратные средства обеспечения информационной безопасности
			8. Описание типовых политик безопасности.	**1** Программно-аппаратные средства обеспечения информационной безопасности
			9. Угрозы безопасности компьютерных систем..	**1** Программно-аппаратные средства обеспечения информационной безопасности
			10. Методы и средства ограничения доступа к компонентам вычислительных систем	**1** Программно-аппаратные средства обеспечения

				информационной безопасности
			11. Модель компьютерной системы.	**1** Программно-аппаратные средства обеспечения информационной безопасности
			12. Понятие монитора безопасности.	**1** Программно-аппаратные средства обеспечения информационной безопасности
			13. Программно-аппаратные средства защиты информации в сетях передачи , данных	**1** Программно-аппаратные средства обеспечения информационной безопасности
			14. Межсетевые экраны.	**1** Программно-аппаратные средства обеспечения информационной безопасности
			15. Свойства экранирующего субъекта.	**1** Программно-аппаратные средства обеспечения информационной безопасности
			16. Классификация требований к классам межсетевых экранов	**2** Обеспечение информационной безопасности компьютерных сетей.
			17. Роль стандартов информационной безопасности.	**2** Обеспечение информационной безопасности компьютерных сетей.
			18. Модель политики безопасности на основе дискретных компонент АДЕПТ-50.	**2** Обеспечение информационной безопасности компьютерных сетей.
			19. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.	**2** Обеспечение информационной безопасности компьютерных сетей.

			20. Основные категории требований кпрограммной и программно-аппаратной реализации средствобеспечения информационнойбезопасности.	**2** Обеспечение информационной безопасности компьютерных сетей.

3. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
Знать (*ОПК-4*): основные стандарты ИБ *(ПК-6)*: – принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; – способы формирования суждений о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций. **Уметь** (*ОПК-4*): – решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности. *(ПК-6)*: – настраивать и эксплуатировать программные средства; – разрабатывать политику информационной безопасности;	**зачтено**	Студент знает: - способы формирования суждений о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций; умеет : - настраивать и эксплуатировать программные средства, - разрабатывать политику информационной безопасности; - решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности Владеет – - профессиональной терминологией; -навыками формирования суждений о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций**.** – навыками применения информационно-коммуникационных технологий с учетом основных требований информационной безопасности.

Владеть (*ОПК-4*): – навыками применения информационно-коммуникационных технологий с учетом основных требований информационной безопасности. *(ПК-6)*: – профессиональной терминологией; навыками формирования суждений о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций**.**	**не зачтено**	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

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

Дисциплина Программные средства защиты информации направлена на ознакомление обучающихся с существующими программными средствами защиты информации, и приобретения практических навыков в применении полученных знаний в условиях работы на конкретных объектах информационной безопасности, а так же осуществления поиска, хранения, обработки и анализа информации из различных источников и представления ее в соответствующем виде для дальнейшего использования в практической деятельности.

Изучение дисциплины Программные средства защиты информации предусматривает:

- лекции,
- лабораторные работы;
- зачет;
- самостоятельную работу.

В ходе освоения раздела 1 «. Программно-аппаратные средства обеспечения информационной» обучающиеся должны уяснить основные принципы создания программно-аппаратных средств обеспечения, их принципы действия и технологические особенности. Взаимодействие с общесистемными компонентами вычислительных систем

В ходе освоения раздела 2 «Обеспечение информационной безопасности компьютерных сетей» обучающиеся должны познакомиться с основными стандартами информационной безопасности.

Студентам необходимо овладеть навыками и умениями применения изученных методов для разработки и реализации защитных средств информации.

В процессе изучения дисциплины рекомендуется на первом этапе обратить внимание на специфику применения программных средств защиты информации. Овладение ключевыми понятиями является 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, связанных с защитой информации.

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

Приложение 2

АННОТАЦИЯ
рабочей программы дисциплины
Программные средства защиты информации

1. Цель и задачи дисциплины

Целью изучения дисциплины является: формирование у студентов знаний по основам защиты информации в компьютерных системах при помощи программных средств, а также навыков и умения в применении знаний для конкретных условий.

Задачами изучения дисциплины являются:

Получение студентами знаний по концепции обеспечения информационной безопасности компьютерных систем:

– программным средствам, реализующим отдельные функциональные требования по защите;

– методам и средствам хранения ключевой информации;

– методам и средствам ограничения доступа к компонентам вычислительных систем;

– защите программ от изменения и контролю целостности;

2. Структура дисциплины

2.1 Распределение трудоемкости по отдельным видам учебных занятий, включая самостоятельную работу: Лк.-24 час., ЛР-24 час.; СР 60 час.

Общая трудоемкость дисциплины составляет 108 часов, 3 зачетных единиц.

2.2 Основные разделы дисциплины:

1 - Программно-аппаратные средства обеспечения информационной безопасности.

2 - Обеспечение информационной безопасности компьютерных сетей.

3. Планируемые результаты обучения (перечень компетенций)

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ОПК-4 - Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности.

ПК-6 - Способность формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций.

4. Вид 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
ОПК-4	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности	**1.** Программно-аппаратные средства обеспечения информационной Безопасности **2.** Обеспечение информационной безопасности компьютерных сетей.	1.1. Методы и средства защиты программного обеспечения 1.2.Построение изолированной программной среды. 2.1. Стандарты информационной безопасности	Отчет по ЛР
ПК-6	Способность формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций	**1.** Программно-аппаратные средства обеспечения информационной Безопасности **2.** Обеспечение информационной безопасности компьютерных сетей.	1.1. Методы и средства защиты программного обеспечения 1.2.Построение изолированной программной среды. 2.1. Стандарты информационной безопасности	

2. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
Знать (*ОПК-4*): основные стандарты ИБ *(ПК-6)*: – принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; – способы формирования суждений о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций. **Уметь** (*ОПК-4*): – решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности. *(ПК-6)*: – настраивать и эксплуатировать программные средства; – разрабатывать политику информационной безопасности; **Владеть** (*ОПК-4*): – навыками применения	**зачтено**	Студент демонстрирует сформированность дисциплинарных компетенций на итоговом уровне, обнаруживает всестороннее, систематическое и глубокое знание: - принципов и методов противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; - способов формирования суждений о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций; - основных стандартов ИБ ; умеет - настраивать и эксплуатировать программные средства, - разрабатывать политику информационной безопасности; - решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности Владеет : – - профессиональной терминологией; -навыками формирования суждений о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций**.**

информационно-коммуникационных технологий с учетом основных требований информационной безопасности. *(ПК-6)*: – профессиональной терминологией; навыками формирования суждений о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций**.**	**не зачтено**	Студент демонстрирует сформированность дисциплинарных компетенций на уровне ниже базового, проявляется недостаточность знаний, умений, навыков. Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

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)