Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Организация и технология защиты информации

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО БИЗНЕСА

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Вариативная**
№ дисциплины по учебному плану:	**Б1.В.09.06.02**
Трудоемкость в зачетных единицах:	**8 семестр - 4;**
Часов (всего) по учебному плану:	**144 часа**
Лекции	**8 семестр - 28 часа;**
Практические занятия	**8 семестр - 28 часа;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**8 семестр - 2 часа;**
Самостоятельная работа	**8 семестр - 85,5 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Контрольная работа**	
Промежуточная аттестация:	
Экзамен	**8 семестр - 0,5 часа;**

Москва 2018

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Коляда В.А. Идентификатор: R207b7ba3-KolyadaVA-b380b823	В.А. Коляда
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: освоение обучающимися профессиональных компетенций, заключающихся в общей готовности и способности применять на практике предлагаемые в настоящее время методы защиты конфиденциальной информации (правовые, организационные, программные и аппаратные) при организации и поддержке электронного бизнеса.

Задачи дисциплины

- получения теоретических знаний в области применения защитных механизмов при организации и ведении электронного бизнеса;
- получения практических навыков в области применения защитных механизмов при организации и ведении электронного бизнеса.

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Запланированные результаты обучения**
ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты		знать: - порядок и технологию создания и реорганизации службы информационной безопасности, а также основные методы и технологию управления службой информационной безопасности; - назначение, роль, задачи, функции и виды организационных структур службы информационной безопасности.
ПК-10 способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности		уметь: - осуществлять управление и контроль за деятельностью службы информационной безопасности организации (предприятия) и соблюдения режима защиты информации в структурных подразделениях организации (предприятия); - организовывать все виды работ службы информационной безопасности.
ПК-13 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации		уметь: - определять структуру службы, осуществлять подбор, расстановку и организацию работы должностных лиц службы информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к части, формируемой участниками образовательных отношений блока дисциплин основной профессиональной образовательной программе Организация и технология защиты информации (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа								СР		
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
							КПР	ГК	ИККП	ТК				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Основные модели электронной коммерции	21	8	4	-	4	-	-	-	-	-	13	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Основные модели электронной коммерции"
1.1	Основные модели электронной коммерции	21		4	-	4	-	-	-	-	-	13	-	***Подготовка к контрольной работе:*** Изучение материалов по разделу Основные модели электронной коммерции и подготовка к контрольной работе ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Основные модели электронной коммерции" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Основные модели электронной коммерции" ***Изучение материалов литературных источников:*** [1], 45-98, 224-287 [5], 5-38
2	Угрозы безопасности электронной коммерции и электронных платежей	25		6	-	6	-	-	-	-	-	13	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Угрозы безопасности электронной коммерции и электронных платежей" ***Подготовка к контрольной работе:***
2.1	Угрозы безопасности электронной коммерции и	25		6	-	6	-	-	-	-	-	13	-	Изучение материалов по разделу Угрозы безопасности электронной коммерции и электронных платежей и подготовка к

	электронных платежей												контрольной работе ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Угрозы безопасности электронной коммерции и электронных платежей" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Угрозы безопасности электронной коммерции и электронных платежей" ***Изучение материалов литературных источников:*** [4], 16-40
3	Методы и средства обеспечения информационной безопасности электронного бизнеса	29		8	-	8	-	-	-	-	-	13	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Методы и средства обеспечения информационной безопасности электронного бизнеса" ***Подготовка к контрольной работе:*** Изучение материалов по разделу Методы и средства обеспечения информационной безопасности электронного бизнеса и подготовка к контрольной работе ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Методы и средства обеспечения информационной безопасности электронного бизнеса" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Методы и средства обеспечения информационной безопасности электронного бизнеса" ***Изучение материалов литературных источников:*** [3], 68-101, 135-172
3.1	Методы и средства обеспечения информационной безопасности электронного бизнеса	29		8	-	8	-	-	-	-	-	13	-	

4	Политика информационной безопасности. Построение систем безопасности электронного бизнеса	33		10	-	10	-	-	-	-	-	13	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Политика информационной безопасности. Построение систем безопасности электронного бизнеса" ***Подготовка к контрольной работе:*** Изучение материалов по разделу Политика информационной безопасности. Построение систем безопасности электронного бизнеса и подготовка к контрольной работе ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Политика информационной безопасности. Построение систем безопасности электронного бизнеса" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Политика информационной безопасности. Построение систем безопасности электронного бизнеса" ***Изучение материалов литературных источников:*** [2], 6-27, 85-98
4.1	Политика информационной безопасности. Построение систем безопасности электронного бизнеса	33		10	-	10	-	-	-	-	-	13	-	
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**144.0**		**28**	**-**	**28**	**-**	**2**	**-**	**-**	**0.5**	**52**	**33.5**	
	Итого за семестр	**144.0**		**28**	**-**	**28**	**2**		**-**		**0.5**	**85.5**		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Основные модели электронной коммерции

1.1. Основные модели электронной коммерции

Введение в дисциплину. Основные понятия и термины электронной коммерции и бизнеса. Понятие электронной коммерции. Краткий обзор основных понятий. Типология электронной коммерции. Структура основных бизнес-моделей электронной коммерции. Основные отличия и особенности моделей. Основы построения и использования банковских информационных систем. Основные задачи и функции. Обзор банковских информационных систем. Виртуальные банки. Интернет-банкинг. Особенности электронных методов платежа. Цифровая наличность..

2. Угрозы безопасности электронной коммерции и электронных платежей

2.1. Угрозы безопасности электронной коммерции и электронных платежей

Потенциальные угрозы электронного бизнеса. Основные задачи обеспечения безопасности информации хозяйствующего субъекта при ведении электронного бизнеса. Построение модели злоумышленника. Классификация преступлений в электронном бизнесе. Классификация и общая характеристика компьютерных преступлений. Анализ и оценка последствий компьютерных преступлений на основе современной статистики..

3. Методы и средства обеспечения информационной безопасности электронного бизнеса

3.1. Методы и средства обеспечения информационной безопасности электронного бизнеса

Правовые основы обеспечения информационной безопасности. Законодательство и нормативно-правовое регулирование в сфере информационной безопасности. Проблемы обеспечения безопасности электронного бизнеса при работе в Internet. Методы и средства защиты информации при работе в Internet. Методы контроля и разграничения доступа к информации. Применение брандмауэров для защиты информации в системах электронного бизнеса. Использование механизмов и средств криптографической защиты информации в системах электронного бизнеса. Аутентификация. Схемы аутентификации на основе симметричных систем. Электронная цифровая подпись. Хеширование сообщений. Криптографические алгоритмы. Основы безопасности электронной торговли при использовании пластиковых карт. Классификация пластиковых карт. Обеспечение безопасности банковских терминалов. Защищенные протоколы (SSL, SET). Методы защиты информации в наиболее известных платежных системах..

4. Политика информационной безопасности. Построение систем безопасности электронного бизнеса

4.1. Политика информационной безопасности. Построение систем безопасности электронного бизнеса

Стандарт Центрального банка России по защите информации (СТО БР ИББС-1.0–2008 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (с изменениями 2010 и 2014 г.). Основы построения и менеджмента систем безопасности электронного бизнеса. Аудит систем информационной безопасности электронного бизнеса.

3.3. Темы практических занятий

1. Основные понятия безопасности электронного бизнеса;
2. Угрозы информационной безопасности и их классификация;
3. Основные защитные механизмы;
4. Анализ законодательства РФ и других нормативно-правовых документов, регламентирующих отношения субъектов в информационной сфере и деятельность организаций по защите информации;
5. Состав и организационная структура системы обеспечения информационной безопасности.;
6. Электронные платежные системы. Классификация и особенности применения в РФ.;
7. Основные принципы внедрения платежных систем в электронную коммерцию;
8. Определение требований к защищенности ресурсов;
9. Обработка кредитных карт и цифровой наличности;
10. Задачи, решаемые средствами защиты информации от несанкционированного доступа;
11. Проблемы обеспечения безопасности в сетях;
12. Способы устранения уязвимостей и противодействия вторжениям нарушителей;
13. Межсетевые экраны. Назначение и виды;
14. Основные защитные механизмы: фильтрация пакетов, трансляция сетевых адресов, промежуточная аутентификация, проверка почты, виртуальные частные сети, противодействия атакам, нацеленным на нарушение работоспособности сетевых служб, дополнительные функции;
15. Контроль информационного наполнения (контента) электронной почты и Web-трафика. Компоненты и функционирование систем контроля контента;
16. Средства выявления уязвимостей узлов сетей и средства обнаружения атак на узлы, протоколы и сетевые службы.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Основные модели электронной коммерции"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Угрозы безопасности электронной коммерции и электронных платежей"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Методы и средства обеспечения информационной безопасности электронного бизнеса"
4. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Политика информационной безопасности. Построение систем безопасности электронного бизнеса"

3.6 Тематика курсовых проектов/курсовых работ

Курсовой проект/ работа не предусмотрены

3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)				Оценочное средство (тип и наименование)
		1	2	3	4	
Знать:						
назначение, роль, задачи, функции и виды организационных структур службы информационной безопасности	ПК-4(Компетенция)	+				Контрольная работа/Контрольное задание № 1 «Основные модели электронной коммерции»
порядок и технологию создания и реорганизации службы информационной безопасности, а также основные методы и технологию управления службой информационной безопасности	ПК-4(Компетенция)		+			Контрольная работа/2.Контрольное задание № 2 «Модель угроз безопасности
Уметь:						
организовывать все виды работ службы информационной безопасности	ПК-10(Компетенция)			+		Контрольная работа/3.Контрольное задание № 3 «Схемы аутентификации на основе симметричных систем. Электронная цифровая подпись. Хеширование сообщений. Криптографические алгоритмы"
осуществлять управление и контроль за деятельностью службы информационной безопасности организации (предприятия) и соблюдения режима защиты информации в структурных подразделениях организации (предприятия)	ПК-10(Компетенция)				+	Контрольная работа/4.Контрольное задание № 4 "Стандарт Центрального банка"
определять структуру службы, осуществлять подбор, расстановку и организацию работы должностных лиц службы информационной безопасности	ПК-13(Компетенция)		+			Контрольная работа/2.Контрольное задание № 2 «Модель угроз безопасности

4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

4.1. Текущий контроль успеваемости

8 семестр

Форма реализации: Письменная работа

1. 2.Контрольное задание № 2 «Модель угроз безопасности (Контрольная работа)
2. 3.Контрольное задание № 3 «Схемы аутентификации на основе симметричных систем. Электронная цифровая подпись. Хеширование сообщений. Криптографические алгоритмы" (Контрольная работа)
3. 4.Контрольное задание № 4 "Стандарт Центрального банка" (Контрольная работа)
4. Контрольное задание № 1 «Основные модели электронной коммерции» (Контрольная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №8)

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих

В диплом выставляется оценка за 8 семестр.

Примечание: Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Лапидус, Л. В. Цифровая экономика. Управление электронным бизнесом и электронной коммерцией : учебник для вузов по направлениям 38.03.01 "Экономика", 38.03.02 "Менеджмент" (квалификация (степень) "бакалавр") / Л. В. Лапидус, Моск. гос. ун-т им. М.В. Ломоносова (МГУ) . – Москва : ИНФРА-М, 2021 . – 479 с. – (Высшее образование . Бакалавриат) . - ISBN 978-5-16-013640-0 .;
2. Ерохин, В. В. Безопасность информационных систем : учебное пособие / В. В. Ерохин, Д. А. Погонышева, И. Г. Степченко, Брянский гос. ун-т им. академика И. Г. Петровского . – 3-е изд., стер . – М. : Флинта : Наука, 2016 . – 184 с. - ISBN 978-5-9765-1904-6 .;
3. Галатенко, В.А. Основы информационной безопасности : учебное пособие для вузов по специальности 351400 "Прикладная информатика" / В.А. Галатенко ; Ред. В. Б. Бетелин . – 4-е изд . – М. : Интернет-Ун-т информ. технологий : БИНОМ. Лаборатория знаний, 2012 . – 205 с. – (Основы информационных технологий) . - ISBN 978-5-94774-821-5 .;
4. А. В. Моргунов- "Информационная безопасность", Издательство: "Новосибирский государственный технический университет", Новосибирск, 2019 - (83 с.) https://biblioclub.ru/index.php?page=book&id=576726;
5. Быстренина И. Е.- "Электронная коммерция", (2-е изд.), Издательство: "Дашков и К", Москва, 2019 - (90 с.) https://e.lanbook.com/book/119257.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Майнд Видеоконференции.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:
1. **ЭБС Лань** - https://e.lanbook.com/
2. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **База данных Web of Science** - http://webofscience.com/
5. **База данных Scopus** - http://www.scopus.com
6. **Национальная электронная библиотека** - https://rusneb.ru/
7. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
8. **Журнал Science** - https://www.sciencemag.org/
9. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
10. **База открытых данных Министерства труда и социальной защиты РФ** - https://rosmintrud.ru/opendata
11. **База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ** - http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/
12. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
13. **Официальный сайт Федерального агентства по техническому регулированию и метрологии** - http://protect.gost.ru/
14. **Открытая университетская информационная система «РОССИЯ»** - https://uisrussia.msu.ru
15. **Официальный сайт Министерства науки и высшего образования Российской Федерации** - https://minobrnauki.gov.ru
16. **Информио** - https://www.informio.ru/

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
	А-300, Учебная аудитория "А"	кресло рабочее, парта, стеллаж, стол преподавателя, стол учебный, стул, трибуна, микрофон, мультимедийный проектор, экран, доска маркерная, колонки, техническая аппаратура, кондиционер, телевизор
Учебные аудитории для проведения практических занятий, КР и КП	М-511, Учебная аудитория	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
Учебные аудитории для проведения	М-511, Учебная аудитория	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска

лабораторных занятий		маркерная, компьютер персональный
Учебные аудитории для проведения промежуточной аттестации	М-511, Учебная аудитория	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-303, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	М-511, Учебная аудитория	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Обеспечение безопасности электронного бизнеса

(название дисциплины)

8 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Контрольное задание № 1 «Основные модели электронной коммерции» (Контрольная работа)

КМ-2 2.Контрольное задание № 2 «Модель угроз безопасности (Контрольная работа)

КМ-3 3.Контрольное задание № 3 «Схемы аутентификации на основе симметричных систем. Электронная цифровая подпись. Хеширование сообщений. Криптографические алгоритмы" (Контрольная работа)

КМ-4 4.Контрольное задание № 4 "Стандарт Центрального банка" (Контрольная работа)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	16
1	Основные модели электронной коммерции					
1.1	Основные модели электронной коммерции		+			
2	Угрозы безопасности электронной коммерции и электронных платежей					
2.1	Угрозы безопасности электронной коммерции и электронных платежей			+		
3	Методы и средства обеспечения информационной безопасности электронного бизнеса					
3.1	Методы и средства обеспечения информационной безопасности электронного бизнеса				+	
4	Политика информационной безопасности. Построение систем безопасности электронного бизнеса					
4.1	Политика информационной безопасности. Построение систем безопасности электронного бизнеса					+
		Вес КМ, %:	25	25	25	25