1	Назва дысцыпліны	Матэматычныя асновы абароны інфармацыі
2	Курс навучання, спецыяльнасць	3, 1-31 03 09 Камп'ютарная матэматыка і сістэмны аналіз
3	Семестр навучання	5
4	Колькасць крэдытаў	2
5	Прозвішча, імя, імя па бацьку лектара	Дацэнт Чаргінец Дзмітрый Мікалаевіч, к.ф.-м.н.
6	Мэты вывучання дысцыпліны	Падрыхтоўка спецыялістаў, здольных выкарыстоўваць фундаментальныя матэматычныя веды ў якасці асновы пры выкананні прыкладных даследаванняў
7	Папярэднія патрабаванні	Камп'ютарная матэматыка (1,2 семестры), Алгебра і тэорыя лікаў
8	Змест дысцыпліны	Рашоткі. LLL-алгарытм. Атакі на крыптасістэму RSA пры дапамозе LLL-алгарытму. Дыскрэтнае лагарыфмаванне. Электронны лічбавы подпіс, подпіс Эль-Гамаля, подпіс Шнорра. Эліптычныя крывыя.
9	Рэкамендуемая літаратура	1. Маховенко Е.Б. Теоретико-числовые методы в криптографии / Е.Б. Маховенко. – М.: Гелиос АРВ, 2006. – 320с. 2. Тилборг, Х.К.А. ван. Основы криптологии / Х.К.А. ван Тилборг. – М.: Мир, 2006. – 471 с. 3. Харин, Ю.С. Математические основы криптологии / Ю.С. Харин, В.И. Берник, Г.В. Матвеев. – Минск: БГУ, 1999. – 319 с. 4. Харин, Ю.С. Компьютерный практикум по математическим методам защиты информации : Учеб. пособие для студ. матем. и инженерно-технических спец. вузов / Ю.С.Харин, С.В.Агиевич. - Мн. : БГУ, 2001. - 190с. 5. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2003. – 328 с. 6. Смарт, Н. Криптография / Н. Смарт ; пер. с англ. С. А. Кулешова под ред. С. К. Ландо. - Москва : Техносфера, 2006. - 525 с.
10	Метады выкладання	Змяшаны з элементамі дыстанцыйнага навучання, праблемны, даследчы
11	Мова навучання	Руская
12	Умовы (патрабаванні) бягучы кантроль	Справаздачы па лабараторных работах з іх вуснай абаронай. Адзнака на экзамене выстаўляецца з улікам: бягучай ацэнкі – 40%, вуснага адказу на экзамене – 60%.
13	Форма бягучай атэстацыі	Экзамен