

Täiendusõppe õppekava EVC0190 - Krüptograafia alused Virumaa kolledž

õppekava kood	EVC0190
nimetus e.k.	Krüptograafia alused
nimetus v.k.	Основы криптографии
maht tundides	32 sh. kontaktõpe - 32, iseseisev õpe - 0, muu - 0
õppekava maht (EAP)	1
hindamiskriteeriumid e.k.	Kõik laboritööd on tehtud vähemalt 75%-le. Kohustuslik: vähemalt 70% kontakttundides osalemine.
hindamiskriteeriumid v.k.	Все лабораторные работы выполнены не менее чем на 75%. Обязательно: участие не менее чем в 70% контактных занятий.
eesmärgid e.k.	Anda baasteadmisi ja oskusi krüptograafias.
eesmärgid v.k.	Дать базовые знания и навыки в области криптографии.
õpiväljundid e.k.	Õppija saab põhilistest krüptograafia printsiipidest aru. Saab kasutada baasmeetodeid. Teab uusi meetodeid ja algoritme.
õpiväljundid v.k.	Обучающийся понимает основные принципы криптографии. Умеет использовать основные методы. Знает новые методы и алгоритмы.
sisu e.k.	Krüptograafia mõiste. Krüptograafia ajalugu. Klassikalised šifrid. Sümmeetrilised algoritmid. DES ja AES algoritmid. Asümmeetrilised algoritmid. Diffie-Hellman algoritm, Kerberos. Hash funktsioonid. Autentimine ja digitaalallkiri. Krüptograafia kasutamine rakendustes.
sisu v.k.	Понятие криптографии. История криптографии. Классические шифры. Симметричные алгоритмы. Алгоритмы DES и AES. Асимметричные алгоритмы. Алгоритм Диффи-Хеллмана, Kerberos. Хеш-функции. Аутентификация и цифровая подпись. Использование криптографии в приложениях.
eeldused e.k.	IT baasteadmised.
eeldused v.k.	Базовые знания в области ИТ.
sihtgrupp e.k.	IT valdkonna töötajad.
sihtgrupp v.k.	ИТ-персонал.