УЧЕБНА ПРАКТИКА Мрежова и информационна сигурност 12а 2021/2022 – СПП

№ по ред	Дата / Уч. седмица	Разпределение на учебния материал по теми	Брой часове	Нови знания	Претовор	Упражнение	Цели	Очаквани резултати	ЗАБЕ-ЛЕЖКА
	1.	**Интруктаж по ТБ, ОТ и ППО** **Раздел 1. Въведение:** Необходимост от мрежова и информационна сигурност;	2	1		1	Обучението по предмета има за цел чрез усвояване на предвидените по програмата знания и умения учениците да придобият професионални компетентности за изграждане и поддържане на оптична или безжични мрежа.	В края на обучението ученикът придобива следните компетентности: - знае правилата за безопасни условия на труд при работа с оптични кабели; - знае основните принципи при монтажа на оптични и безжични устройства; - конфигурира рутер за работа в безжична мрежа	
	2.	Дефиниции. Основни особености;	2	1	1				
	3.	Международни и регионални инициативи;	2	1		1			
	4.	Заплахи за информационната сигурност. Кибер-престъпност;	2	1	1				
	5.	Политики за информационна сигурност;	2	1		1			
	6.	Основни стандарти и оценка на риска;	2	1	1				
	7.	**Раздел 2. Устойчивост на мрежите:** Основни концепции на криптографските алгоритми и криптоанализа;	2	1		1			
	8.	Системи за управление на информационната сигурност (ISO 270XX);	2	1	1				
	9.	Управление на активите;	2	1		1			
	10.	Сигурност в телекомуникациите. Устойчивост на мрежите;	2	1	1				
	11.	Виртуални частни мрежи (VPN's); Услуги по сигурността	2	1		1			
	12.	**Раздел 3. Видове атаки и защита от тях:** Контрол на достъпа. Защита срещу неоторизиран достъп;	2	1	1				
	13.	Аутентикация, оторизация, електронна идентичност	2	1		1			

	14.	Цифрови сертификати, електронни подписи;	2	1	1				
	15.	Защита срещу зловреден софтуер;	2	1		1			
	16.	Системи за откриване и за защита от проникване (IDS / IPS);	2	1	1				
	17.	DNS-защита; DDos / Botnets-защита;	2	1		1			
	18.	Сигурност на УЕБ-приложенията; Тестове за проникване;	2	1	1				
	19.(1)	***2 – ри СРОК,*** **Раздел 4. Сигурност в мрежата:** Експлоатационна сигурност;	2	1		1			
	20.(2)	Управление на уязвимостите;	2	1	1				
	21.(3)	Боравене с инциденти и докладването им;	2	1		1			
	22.(4)	CERT (Центрове за реагиране при инциденти в компютърната сигурност);	2	1	1				
	23.(5)	Мрежови примамки (Honeypots);	2	1		1			
	24.(6)	Автоматизация на сигурността;	2	1	1				
	25.(7)	Disaster Recovery;	2	1		1			
	26.(8)	Физическа и организационна сигурност. Сигурност на персонала;	2	1	1				
	27.(9)	Сигурен софтуер;	2	1		1			
	28.(10)	Облачна сигурност и икономика на сигурността	2	1	1				
	29.(11)	РЕЗЕРВ	2	1		1			
ВСИЧКО ЧАСОВЕ			**58**	29	14	15			

Преподавател: инж. Георги Сачков