

<i>№ по ред</i>	<i>Дата / Уч. седмица</i>	Разпределение на учебния материал по теми	<i>Брой часове</i>	<i>Нови знания</i>	<i>Преговор</i>	<i>Упражнение</i>	<i>Цели</i>	<i>Очаквани резултати</i>	<i>ЗАБЕЛЕЖКА</i>
1.		Раздел 1. Въведение	6	5	1		Учениците да придобият следните професионални компетентности: -да придобият знания за същността на информационната сигурност; проектиране, изграждане и използване методите и техническите средства за осигуряване на компютърна и мрежова сигурност; -основните уязвимости и заплахи за информацията в информационните системи; -основните методи и средства за достъп до информацията в мрежата; -основните принципи на информационната безопасност;	Учениците да придобият следните компетенции: -проектират, изграждат и използват методите и техническите средства за осигуряване на компютърната сигурност; -познават начините за защита на мрежата; -знаят основните определения и ключови характеристики в това направление; -демонстрират разбиране за същността на информационната сигурност. --познават основните методи за реализиране на заплахите и за защита на информацията и средствата за	
2.	1	Инструктаж по ТБ, ОТ и ППО. Необходимост от мрежова и информационна сигурност	1	1					
3.	2	Дефиниции. Основни особености	1	1					
4.	3	Международни и регионални инициативи	1	1					
5.	4	Заплахи за информационната сигурност. Кибер-престъпност	1	1					
6.	5	Политики за информационна сигурност Основни стандарти и оценка на риска	1	1					
7.	6	Преговор и оценка на знанията	1		1				
8.		Раздел 2. Устойчивост на мрежите	5						
9.	7	Основни концепции на криптографските алгоритми и криптоанализа	1	1					
10.	8	Системи за управление на информационната сигурност (ISO 270XX.Управление на активите	1	1					
11.	9	Сигурност в телекомуникациите. Устойчивост на мрежите	1	1					
12.	10	Виртуални частни мрежи (VPN's)	1	1					
13.	11	Услуги по сигурността	1	1					
14.		Раздел 3. Видове атаки и защита от тях	8	8					
15.	12	Контрол на достъпа. Защита срещу неоторизиран достъп	1	1					
16.	13	Аутентикация, оторизация, електронна идентичност	1	1					
17.	14	Цифрови сертификати,електронни подписи	1	1					
18.	15	Защита срещу зловреден софтуер	1	1					

<i>№ по ред</i>	<i>Дата / Уч. седмица</i>	Разпределение на учебния материал по теми	<i>Брой часове</i>	<i>Нови знания</i>	<i>Преговор</i>	<i>празнене</i>		реализирането им.	ЗАБЕЛЕЖКА
19.	16	Систени за откриване и за защита от пронокуване(IDS/IPS)	1	1			-основните методи и средства за защита на информацията; -защита на мрежата, защитна стена, защитен обмен на електронни съобщения, защита на DNS, DDoS/Botnets защита, защита на Web приложения.		
20.	17	DNS-защита	1	1					
21.	18	DDos/Bothers-защита	1	1					
22.	19	Сигурност на УЕБ-приложенията. Тестове за проникване	1	1					
23.		Раздел 4 Сигурност в мрежата	10						
24.	20	Експлоатационна сигурност	1	1					
25.	21	Управление на уязвимостите	1	1					
26.	22	Боравене с инциденти и докладването им	1	1					
27.	23	CERT (Центрове за реагиране при инциденти в компютърната сигурност)	1	1					
28.	24	Мрежови примамки(Honeypots)	1	1					
29.	25	Автоматизация на сигурността	1	1					
30.	26	Disaster Recovery	1	1					
31.	27	Физическа и организационна сигурност. Сигурност на персонала	1	1					
32.	28	Сигурен софтуер. Облачна сигурност и икономика на сигурността	1	1					
33.	29	Преговор. Проверка на знанията	1		1				
34.		Общ брой часове:	29	27	2				