



РЕПУБЛИКА БЪЛГАРИЯ
Заместник-министър на образованието и науката

ЗАПОВЕД

№ РД 09-..... 2022 г.

На основание чл. 13д, ал. 2, т. 1 от Закона за професионалното образование и обучение, при спазване изискванията на чл. 66, ал. 1 и 2 от Административнопроцесуалния кодекс, във връзка с осигуряването на обучението по учебен предмет и Заповед № РД 09-3893/15.08.2022 г. на министъра на образованието и науката

УТВЪРЖДАВАМ

учебна програма за специфична професионална подготовка по учебния **предмет мрежова и информационна сигурност – теория**, за професионалното направление код **523 „Електроника, автоматика, комуникационна и компютърна техника“**, професия код **523050 „Техник на компютърни системи“**, специалност код **5230502 „Компютърни мрежи“** съгласно приложението.

Учебната програма влиза в сила от учебната 2022/2023 година.

X

МАРИЯ ГАЙДАРОВА
Зам.-министър на образованието и науката

МИНИСТЕРСТВО НА ОБРАЗОВАНИЕТО И НАУКАТА

У Ч Е Б Н А П Р О Г Р А М А
ЗА СПЕЦИФИЧНА ПРОФЕСИОНАЛНА ПОДГОТОВКА
ПО
УЧЕБНИЯ ПРЕДМЕТ
МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ
ТЕОРИЯ

Утвърдена със Заповед № РД 09-.....2022 г.

ПРОФЕСИОНАЛНО НАПРАВЛЕНИЕ:

Код 523 „Електроника, автоматика, комуникационна и компютърна техника“

ПРОФЕСИЯ:

Код 523050 „Техник на компютърни системи“

СПЕЦИАЛНОСТ:

Код 5230502 „Компютърни мрежи“

София

2022 година

I. ОБЩО ПРЕДСТАВЯНЕ НА УЧЕБНАТА ПРОГРАМА

Учебната програма по учебния предмет **мрежова и информационна сигурност – теория**, е предназначена за специалност код 5230502 „Компютърни мрежи“ от професия код 523050 „Техник на компютърни системи“ от професионално направление код 523 „Електроника, автоматика, комуникационна и компютърна техника“.

Съдържанието на учебния предмет дава възможност обучаемите да получат знания за заплахите за сигурността на информацията в информационните системи, методите и средствата за несанкциониран достъп до информация, както и основните принципи и методи, използвани за защитата ѝ.

Обучението по предмета се извършва в междупредметна връзка с изучавания в общообразователна подготовка предмет: информационни технологии и във взаимовръзка с изучаваните по специфична подготовка предмети: мрежови протоколи и технологии и компютърни архитектури и периферни устройства, безжични и оптични мрежови технологии.

Професионалните компетентности по учебния предмет се формират чрез усвояването на знания и умения, свързани с устойчивостта и сигурността на мрежите, както и видовете атаки и защита от тях.

II. ЦЕЛИ НА ОБУЧЕНИЕТО ПО УЧЕБНИЯ ПРЕДМЕТ

Обучението по учебния предмет **мрежова и информационна сигурност – теория**, има за цел запознаване на учениците с основните понятия, стандарти и техники в областта на мрежовата и информационна сигурност. Това ще им позволи в бъдеще професионално да решават задачи, свързани с избор на ефективни средства за защита на компютърни системи и мрежи и ще могат да ги прилагат на практика.

За постигане на основната цел на обучението по предмета е необходимо учениците да усвоят знания за:

- същността на информационната сигурност;
- проектиране, изграждане и използване методите и техническите средства за осигуряване на компютърна 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;
- 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.

III. УЧЕБНО СЪДЪРЖАНИЕ

1. Разпределение на учебното време

Общият брой часове по учебния предмет **мрежова и информационна сигурност – теория**, е определен в типовите учебни планове за съответната специалност в специфичната професионална подготовка.

Варианти	Вариант I	Вариант II
Брой часове по типов учебен план	18	29

2. Раздели, теми и препоръчителен брой часове

Учебното съдържание е структурирано в четири раздела. За всеки раздел са записани препоръчителен брой учебни часове и теми. Учебните часове се разпределят по раздели и теми в началото на всяка учебна година от учителя, в зависимост от възможностите и интересите на учениците, методите на обучение и планираната в училищния учебен план разширена професионална подготовка.

№	Наименование на разделите и темите	Вариант I	Вариант II
		Препоръчителен брой часове	Препоръчителен брой часове
I.	Въведение	3	5
1.1.	Необходимост от мрежова и информационна сигурност. Дефиниции и основни особености		
1.2.	Международни и регионални инициативи. Политики за информационна сигурност		
1.3.	Заплахи за информационната сигурност. Кибер-престъпност. Основни стандарти и оценка на риска		
II.	Устойчивост на мрежите	3	6
2.1.	Основни концепции на криптографските алгоритми и криптоанализа		
2.2.	Системи за управление на информационната сигурност (ISO 270XX). Управление на активите		
2.3.	Сигурност в телекомуникациите. Устойчивост на мрежите		
2.4.	Виртуални частни мрежи (VPN's)		
2.5.	Услуги по сигурността		
III.	Видове атаки и защита от тях	6	9
3.1.	Контрол на достъпа. Защита срещу неоторизиран достъп		
3.2.	Аутентикация, оторизация, електронна идентичност. Цифрови сертификати, електронни подписи		

№	Наименование на разделите и темите	Вариант I	Вариант II
		Препоръчителен брой часове	Препоръчителен брой часове
3.3.	Защита срещу зловреден софтуер. Системи за откриване и за защита от проникване (IDS / IPS)		
3.4.	DNS – защита. DDos/Botnets – защита		
3.5.	Сигурност на УЕБ-приложенията		
3.6.	Тестове за проникване		
IV.	Сигурност в мрежата	6	9
4.1.	Експлоатационна сигурност. Управление на уязвимостите		
4.2.	Боравене с инциденти и докладването им. CERT (Центрове за реагиране при инциденти в компютърната сигурност)		
4.3.	Мрежови примамки (Honeypots)		
4.4.	Автоматизация на сигурността и Disaster Recovery		
4.5.	Физическа и организационна сигурност. Сигурност на персонала. Сигурен софтуер		
4.6.	Облачна сигурност и икономика на сигурността		
	ОБЩ ПРЕПОРЪЧИТЕЛЕН БРОЙ ЧАСОВЕ:	18	29

IV. ОЧАКВАНИ РЕЗУЛТАТИ ОТ УЧЕНОТО – ЗНАНИЯ, УМЕНИЯ И КОМПЕТЕНТНОСТИ

В резултат от обучението ученикът трябва да притежава следните знания, умения и компетентности:

1. Знания за:

- основните определения и ключовите характеристики в мрежовата и информационна сигурност;
- най-важните политики, подходи, стандарти и заплахи срещу мрежовата и информационна сигурност;
- начините на защита на мрежата, защитна стена, защитен обмен на електронни съобщения, защита на DNS, DDos/Botnets защита, защита на Web приложения;
- основните методи за реализиране на заплахите и за защита на информацията и средствата за реализирането им.

2. Умения за:

- проектиране, изграждане и използване методите и техническите средства за осигуряване на компютърна сигурност;

3. Компетентности за:

- разбиране на същността на информационната сигурност;
- решаване на задачи, свързани с избор на ефективни средства за защита на компютърни системи и мрежи.

V. АВТОРСКИ ЕКИП

Учебната програма е разработена от авторски екип, сформирани по проект BG05M2OP001-2.014-0001 „Подкрепа за дуалната система на обучение“, финансиран от Оперативна програма „Наука и образование за интелигентен растеж“ 2014 – 2020 г., съфинансирана от Европейския съюз чрез Европейските структурни и инвестиционни фондове:

- инж. Иванка Янкова – ПГ по механоелектротехника и електроника – гр. Бургас;
- инж. Ивайло Драгнев – ПГ по електротехника и електроника – гр. Пловдив;
- инж. Любомира Вълкова – ПГ по електротехника и електроника – гр. Пловдив.

Учебната програма е съгласувана с външните експерти:

- гл. ас. д-р. инж. Ангел Данев – Университет по хранителни технологии, гр. Пловдив;
- Регина Узунова – „Кауфланд България ЕООД енд Ко КД“.