СТРУКА (назив)	**Електротехника**		
Занимање (назив):	**Техничар информационих технологија**		
Предмет (назив):	**Заштита информационих система**		
Опис (предмета):	**Стручни**		
Модул (наслов):	**Основе криптологије и заштите података**		
Датум: **2023.година**	**Шифра:**		**Редни број: 01**

Сврха

1. Развијање свијести ученика о значају заштите информационих система
2. Упознавање ученика са различитим методама криптографије
3. Упознавање ученика са различитим облицима напада на информационе системе
4. Упознавање ученика са методама заштите оперативних система и рачунарсих мрежа

Специјални захтјеви / Предуслови

- Користити стечена знања из математике и информатике

Циљеви

- Упознавање ученика са криптологијом као научном основом за заштиту информација
- Упознавање ученика са криптографским механизмима и методама криптоанализе
- Упознавање ученика са инфраструктуром јавних кључева и хеш функцијама
- Упознавање ученика са основним принцима мрежне безбједности и са сигурносним аспектима оперативних система
- Упознавање ученика са методама детекције и превенције напада

Теме

1. **Методе криптографије**
2. **Напади на информационе системе**
3. **Заштита оперативних система и рачунарских мрежа**

Тема	**Исходи учења**			**Смјернице за наставнике**
	Знања	**Вјештине**	**Личне компетенције**	
	Ученик је способан да:			

1. Методе криптографије	- објасни значај криптологије, -разумије појмове: податак, информација, шифра, кључ, шифровање, дешифровање; - разумије појмове јавни и приватни кључ, - користи Керкхофове принципе; - објасни симетричну криптографију, - објасни модуларну аритметику; - наведе асиметричну криптографију; - разумије структуру дигиталног сертификата.	- користи транспозиционе шифре, шифре замјене, кодне књиге,one-time pad, Hill-ова шифра, Vigener-ова шифра; - користи блоковске шифре, DES, 3DES, AES, IDEA, BlowFish, TEA; - употребљава криптографију са јавним кључевима (тајност, интегритет, непорецивост); - имплементира дигитални сертификат.	- савјесно, одговорно, уредно и правовремено обавља повјерене послове, -ефикасно планира и организује вријеме, -испољи позитиван однос према значају спровођења прописа и стандарда који су важни за његов рад, -испољи љубазност, комуникативност, ненаметљивост и флексибилност у односу према сарадницима, -одговорно рјешава проблеме у раду, прилагођава се промјенама у раду и изражава спремност на тимски рад, -испољи позитиван однос према професионално-етичким нормама и вриједностима, -испољи иницијативу и предузимљивост, -показује спретност, моторичку координацију, -испољава одличну способност за разумијевање сложених технолошких структура, система, цртежа и информација -развије самосталност у раду.	Наставник ће на почетку теме ученике упознати са циљевима и исходима наставе, односно учења, планом рада и начинима оцјењивања. При реализацији основа криптографије: - ученике треба упознати са основним криптолошким појмовима и њиховом значају и улози у заштити информација; - ученик треба да научи да користи инфраструктуру јавних кључева у циљу заштите информација.
2. Напади на информационе системе	- наведе основне елементе инфраструктуре јавних кључева за заштиту	- дефинише Хеш функције, крипто-хеш функције; - објасни значај инфраструктуре јавних кључева у		- При реализацији цјелине детекција и превенција напада: - ученици треба да се упознају са системом за детекцију напада;

	информационих система; - објасни аутентификацију и методе аутентификације.	заштити информација; - користи инфраструктуру јавних кључева у циљу заштите информација; - објасни значај примјене хеш функција у пракси; - имплементира лозинке, кључеве, биометријску аутентификацију.		- ученици треба да се упознају са превенцијом напада.
3. Заштита оперативних система и рачунарских мрежа	- познаје факторе безбједности рачунарске мреже; - детектује злонамјеран софтвер (тројански коњ, црви, вируси, задња врата, ...).	- реализује контролу приступа ресурсима оперативног система; - објасни факторе ризика по мрежну безбједност; - објасни сигурносне механизме које посједује оперативни систем и начин њихове употребе; - објасни врсте напада на информациони систем; - објасни начине превенције напада		- При реализацији цјелине сигурност оперативних система ученици треба да упознају сигурносне аспекте оперативних и рачунарских система.

		на информационе системе; - објасни функционисање система за детекцију напада; - објасни функционисање система за превенцију напада.		

Интеграције

- Рачунарске мреже и комуникације
- Интернет технологије и сервиси
- Информациони системи
- Веб програмирање

Извори

- Уџбеници које је одобрило Министарство просвјете и културе Републике Српске;
- Друга стручна и теоријска литература (стручни часописи, приручници, збирке, видео и аудио записи, интернет и сл.).

Оцјењивање

Оцјењивање се врши у складу са Законом о средњем образовању и васпитању и Правилником о оцјењивању ученика у настави и полагању испита у средњој школи. О техникама и критеријима оцјењивања ученике треба упознати на почетку изучавања модула.

СТРУКА (назив)	**Електротехника**		
Занимање (назив):	**Техничар информационих технологија**		
Предмет (назив):	**Заштита информационих система**		
Опис (предмета):	**Стручни**		
Модул (наслов):	**Напредне методе криптологије и заштите података**		
Датум: **2023. година**	**Шифра:**		**Редни број: 02**

Сврха

Да ученици самостално помоћу за то припремњених лабораторијских вјежби провјере стечена теоретска знања.

Специјални захтјеви / Предуслови

- Ученик је обавезан да прије извођења лабораторијске вјежбе да код куће понови потребно теоретско знање, које је потребно за успјешно реализовање одговарајуће лабораторијске вјежбе.

Циљеви

- Да ученици самостално користе алгоритме класичне, симетричне и асиметричне криптографије
- Да ученици самостално провјере стечена теоретска знања
- Упознавање ученика са основним принцима мрежне безбједности и са сигурносним аспектима оперативних система
- Упознавање ученика са методама детекције и превенције напада

Теме

1. **Сигурност криптосистема**
2. **Биометријске методе идентификације и аутентификације**
3. **Напади усмјерени на мрежну инфраструктуру и мјере превенције и заштите**

Тема	**Исходи учења**			**Смјернице за наставнике**
	Знања	**Вјештине**	**Личне компетенције**	
	Ученик је способан да:			

1. Сигурност криптосистема	- објасни појам криптографија, криптоанализа, стеганографија, - наведе основну намјену и сврху DES, 3DES, AES, IDEA, BlowFish, TEA; - објасни појам алгоритма за шифровање јавним кључем (RSA, Diffie-Hellman);	- користи транспозиционе шифре, шифре замјене, кодне књиге, one-time pad, Hill-ова шифра, Vigener-ова шифра, - употреби инфраструктуре јавних кључева за заштиту информационих система; - примјени хеш функције.	- савјесно,одговорно,уредно и правовремено обавља повјерене послове, -ефикасно планира и организује вријеме, -испољи позитиван однос према значају спровођења прописа и стандарда који су важни за његов рад, -испољи љубазност, комуникативност, ненаметљивост и флексибилност у односу према сарадницима, -одговорно рјешава проблеме у раду, прилагођава се промјенама у раду и изражава спремност на тимски рад, -испољи позитиван однос према професионално-етичким нормама и вриједностима, -испољи иницијативу и предузимљивост, -показује добру спретност,моторичку координацију, -испољава одличну способност за разумијевање сложених технолошких структура, система, цртежа и информација	- На почетку теме ученике упознати са циљевима и исходима наставе, односно учења, планом рада и начинима оцјењивања. - Вјежбе у електронској форми треба да омогуће да ученици раде у темпу који је у складу са њиховим индивидуалним могућностима и нивоом предзнања. - Вјежбе треба да буду засноване на примјерима који су ученицима искуствено најближи и у функцији потреба образовног профила. - Треба очувати снажну мотивацију ученика за изучавање предмета. - Пожељно је за демонстрацију криптографских алгоритама користити неки од бесплатних алата(нпр. CrypTool) - Ученике треба упознати са основним криптолошким појмовима и њиховом значају и улози у заштити информација. - Од ученика се може тражити да примијени основне криптографске механизме и криптоаналитичке методе. Ученик треба да научи да користи инфраструктуру јавних кључева у циљу заштите информација.
2. Биометријске методе идентификације и аутентификације	- реализује мрежне баријере(хардвер, софтвер), -објасни нападе усмјерене на мрежну инфраструктуру и	- објасни начин заштите помоћу отиска прста, потпис, препознавање лица,		Од ученика се може тражити да примјени основне криптографске механизме и криптоаналитичке методе. Ученик треба да научи да користи инфраструктуру јавних кључева у циљу заштите информација.

	примјени мјере превенције и заштите; - реализује заштиту бежичних мрежа; - региструје злонамјеран софтвер.	препознавање говора,... - објасни методе контроле приступа мрежи и имплементира их у пракси објасни различите нападе на инфраструктуру и предложи мјере превенције и заштите објасни нападе на бежичне и мобилне мреже.	-развије самосталност у раду.	При реализацији тематске цјелине контрола приступа инсистирати да ученици објасне методе аутентификације и њихов значај, као и ауторизацију и права приступа. Пожељно је да ученик имплементира, у пракси, методе контроле приступа мрежи. При реализацији тематске цјелине сигурност рачунарских мрежа пожељно је да у лабораторији постоји рутер (или више њих) на коме се може конфигурисати мрежна баријера. На вјежбама демонстрирати подешавања мрежних баријера, као и методе напада на мрежу. Демонстрирати на примјеру бежичних мрежа разбијање WEP кључева (Aircrack ili neki drugi alat) да би ученици схватили све слабости тог вида заштите бежичне мреже. При реализацији тематске цјелине сигурност оперативних система ученици треба да упознају сигурносне аспекте оперативних система. Пожељно је да се ученицима демонстрира контрола приступа ресурсима оперативног система.
3. Напади усмјерени на мрежну инфраструктуру и мјере превенције и заштите	- наведе нападе на апликације и методе превенције, нападе везане за аутентификацију (Brute Force, недовољна аутентификација,спријече недовољну заштиту корисничке лозинке),	- објасни начине превенције напада на информационе системе; - објасни функционисање система за детекцију напада;		При реализацији тематске цјелине сигурност рачунарских мрежа пожељно је да у лабораторији постоји рутер (или више њих) на коме се може конфигурисати мрежна баријера.

	- познаје систем за детекцију напада- архитектура система.	- објасни функционисање система за превенцију напада.		На вјежбама демонстрирати подешавања мрежних баријера, као и методе напада на мрежу. Демонстрирати на примјеру бежичних мрежа разбијање WEP кључева (Aircrack ili neki drugi alat) да би ученици схватили све слабости тог вида заштите бежичне мреже. При реализацији тематске цјелине сигурност оперативних система ученици треба да упознају сигурносне аспекте оперативних система. Пожељно је да се ученицима демонстрира контрола приступа ресурсима оперативног система. При реализацији тематске цјелине сигурност софтвера/апликација/ информационих система демонстрирати на вјежбама изабране врсте напада на апликације и демонстрирати алате за разбијање лозинки (npr. John the Ripper, L0phtCrack) у циљу упознавања ученика са слабостима тог вида заштите. При реализацији тематске цјелине детекција и превенција напада ученици треба да се упознају са системом за детекцију напада и треба да се упознају са превенцијом напада.
Интеграције • Рачунарске мреже и комуникације • Интернет технологије и сервиси • Информациони системи • Веб програмирање				
Извори				

- Уџбеници које је одобрило Министарство просвјете и културе Републике Српске;
- Друга стручна и теоријска литература (стручни часописи, приручници, збирке, видео и аудио записи, интернет и сл.).

Оцјењивање

Оцјењивање се врши у складу са Законом о средњем образовању и васпитању и Правилником о оцјењивању ученика у настави и полагању испита у средњој школи. О техникама и критеријима оцјењивања ученике треба упознати на почетку изучавања модула.