МИНИСТЕРСТВО НА ОБРАЗОВАНИЕТО И НАУКАТА

Проект

Н А Р Е Д Б А

№ …….

за придобиване на квалификация по професията

„КИБЕРСИГУРНОСТ“

Раздел I
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. С тази наредба се определя държавният образователен стандарт (ДОС) за придобиването на квалификация по професията 103202 „Киберсигурност“ от област на образование „Сигурност и отбрана“ и професионално направление 1032 „Национална и лична сигурност и защита на имуществото“ съгласно Списъка на професиите за професионално образование и обучение по чл. 6, ал. 1 от Закона за професионалното образование и обучение.

Чл. 2. Държавният образователен стандарт за придобиването на квалификация по професията 103202 „Киберсигурност“, съгласно приложението към тази наредба, определя изискванията за придобиването на трета и четвърта степен на професионална квалификация по професията, за придобиване на квалификация по част от професията, както и за достигане на отделни единици резултати от ученето.

Чл. 3. Въз основа на ДОС по чл. 1 и рамковите програми по чл. 10, ал. 3, т. 3 от Закона за професионалното образование и обучение се разработват типови учебни планове и учебни програми за ученици. Въз основа на рамковите програми по чл. 10, ал. 3, т. 2, 4, 5 и 6 се разработват учебни планове и учебни програми за лица, навършили 16 години.

ПРОЕКТ

Раздел II

СЪДЪРЖАНИЕ НА ДЪРЖАВНИЯ ОБРАЗОВАТЕЛЕН СТАНДАРТ

Чл. 4. (1) Държавният образователен стандарт по чл. 1 определя изискванията към кандидатите, описанието на професията, единиците резултати от учене за придобиване на трета и четвърта степен на професионална квалификация по професията, критериите и средствата за оценяване на всяка единица резултат от учене, съвкупността от единици резултати от ученето, които формират придобиването на квалификация по част от професия, изискванията към материалната база и изискванията към обучаващите.

(2) Държавният образователен стандарт за придобиване на квалификация по професията включва общата, отрасловата и специфичната професионална подготовка с необходимите професионални компетентности, които гарантират на обучаемия възможността за упражняване на професията след завършване на обучението.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Учебните планове и учебните програми по чл. 3, разработени въз основа на тази наредба, започват да се прилагат от учебната 2026 – 2027 г. за учениците, които постъпват в VIII клас в училищното професионално образование и обучение, а за лица, навършили 16 години – от 1 януари 2026 г.

§ 2. Тази наредба се издава на основание чл. 22, ал. 6, във връзка с ал. 2, т. 6 от Закона за предучилищното и училищното образование.

КРАСИМИР ВЪЛЧЕВ

Министър на образованието и науката

ПРОЕКТ

Приложение към чл. 2

ДЪРЖАВЕН ОБРАЗОВАТЕЛЕН СТАНДАРТ
ЗА ПРИДОБИВАНЕ НА КВАЛИФИКАЦИЯ ПО ПРОФЕСИЯТА
„КИБЕРСИГУРНОСТ“

Професионално направление					
Код: 1032	**Национална и лична сигурност и защита на имуществото**				
Професия					
Код: 103202	**Киберсигурност**				
Степени на професионална квалификация		**-**	**-**	**III**	**IV**
Ниво по Национална квалификационна рамка (НКР)		**-**	**-**	**4**	**5**
Ниво по Европейска квалификационна рамка (ЕКР)		**-**	**-**	**4**	**5**

ПРОЕКТ

1. Изисквания към кандидатите

1.1. Изисквания към кандидатите за входящо минимално образователно и/или входящо квалификационно равнище за придобиване на степени на професионална квалификация съгласно Закона за професионалното образование и обучение

За придобиване на трета и четвърта степен на професионална квалификация по професията „Киберсигурност“ от Списъка на професиите за професионално образование и обучение, утвърден от министъра на образованието и науката със Заповед № РД09-2230 от 09.08.2024 г., изискванията за входящото минимално образователно равнище към кандидатите са:

1.1.1. За придобиване на трета степен на професионална квалификация

- за ученици – завършено основно образование;
- за лица, навършили 16 години – придобито право за явяване на държавни зрелостни изпити или завършено средно образование.

1.1.2. За придобиване на четвърта степен на професионална квалификация

- завършено средно образование.

Изискването за входящо квалификационно равнище при продължаващо професионално обучение за придобиване на четвърта степен на професионална квалификация е придобита трета степен на професионална квалификация по професията, съответно по част от професията.

1.2. Здравословното състояние на кандидата се удостоверява с медицински документ, доказващ, че професията, по която желае да се обучава, не му е противопоказна.

2. Описание на професията

2.1. Трета степен на професионална квалификация по професията

Придобилият трета степен на професионална квалификация по професия „Киберсигурност“ ще има професионални знания, умения и компетентности да извършва дейности с комплексен характер по защита на информационни системи, мрежи и данни при изменящи се условия, както и да поема отговорности за подпомагане на работата на други лица в рамките на екипи за киберсигурност.

Придобилите трета степен на професионална квалификация по професията „Киберсигурност“ участват активно в оперативни дейности по наблюдение, защита и реагиране в рамките на екипи, ръководени от специалисти с по-висока квалификация, отговорни за сигурността на информационните системи и цифровите активи в организацията. Те са пряко ангажирани с техническото изпълнение на ежедневните задачи съгласно утвърдени процедури, свързани с идентифициране на рискове, мониторинг на мрежовия

ПРОЕКТ

трафик, събиране и анализ на данни от системни логове, както и предприемане на начален отговор при киберинциденти.

Техният труд включва инсталиране, конфигуриране и поддържане на системи за защита – защитни стени, антивирусен софтуер, инструменти за криптиране на данни и средства за откриване на злонамерена дейност. Те подпомагат прилагането и тестването на утвърдени процедури за реагиране при инциденти, участват в симулации и обучения за повишаване на осведомеността на служителите и поддържат базова документация, свързана с политики за защита на информацията.

Работната среда изисква високо ниво на съсредоточеност, работа с компютърни системи в продължителни интервали от време, включително на смени. Нерядко се налага бърза реакция в кризисни ситуации, което предполага устойчивост на стрес и умения за работа под напрежение.

Личностните качества, които имат ключово значение за успешната реализация в професията, включват висока степен на дисциплинираност, внимание към детайлите, емоционална устойчивост и постоянен стремеж към усъвършенстване. От особена важност са също така уменията за ефективна работа в екип, добрата комуникация и стриктната лоялност при боравене с чувствителна и поверителна информация.,

2.2. Четвърта степен на професионална квалификация по професията

Придобилият четвърта степен на професионална квалификация по професия „Киберсигурност“ ще има професионални знания, умения и компетентности за извършване на широк кръг дейности с комплексен характер в областта на информационната, мрежовата и цифровата сигурност, при изменящи се условия, както и поемане на управленски отговорности за работата на други лица и за разпределяне на ресурси при упражняване на професията.

Придобилите четвърта степен на професионална квалификация по професията „Киберсигурност“ изпълняват както технически, така и управленски и стратегически функции. Те отговарят за координация и надзор на дейностите по информационна и мрежова сигурност, ръководят екипи, управляват ресурси и участват в изготвянето и прилагането на политики на организационно и междуинституционално ниво.

Те извършват анализ и оценка на рисковете, разработват и прилагат планове за реагиране при инциденти, ръководят обучения и симулации, както и създават стратегии за защита на информационните ресурси. В ролята си те поддържат активно взаимодействие с организационни ръководства, външни партньори и държавни и международни органи, представят състоянието на сигурността, оценяват заплахи и участват във вземането на стратегически решения.

ПРОЕКТ

Те отговарят за прилагането и контрола на международни стандарти за сигурност, участват в процеси по сертифициране и администрират системи за управление на информационната сигурност (например ISO/IEC 27001). Освен това внедряват иновативни технологични решения, като автоматизация на процеси, машинно обучение и интелигентни системи за защита.

Специалистът с четвърта степен на професионална квалификация носи отговорност както за оперативната сигурност, така и за изграждането и поддържането на култура на сигурност в организацията. Той организира обучения, ръководи инициативи за повишаване на осведомеността и насърчава отговорното цифрово поведение сред служителите.

Работната среда изисква висока степен на ангажираност, способност за бързо и адекватно реагиране при инциденти, както и ефективна комуникация с различни екипи, включително в условия на напрежение. Специалистите обикновено работят в технологично обезпечени офиси, но могат да извършват дейности и дистанционно или в извънредни ситуации.

Успешното упражняване на професията на това ниво изисква задълбочена професионална експертиза, стратегическо и аналитично мислене, лидерски качества и способност за вземане на самостоятелни решения, основани на данни и реалистична оценка на риска. От специалистите се очаква непрекъснато професионално развитие и проактивно следене на международните тенденции, нововъзникващи заплахи и регулаторни изисквания.

3. Единици резултати от ученето (ЕРУ) за придобиване на трета и четвърта степен на професионална квалификация по професията

Степен на професионална квалификация	Ниво по НКР/ ЕКР	Номер на ЕРУ и вид професионална подготовка (ПП)																			
		ЕРУ 1	ЕРУ 2	ЕРУ 3	ЕРУ 4	ЕРУ 5	ЕРУ 6	ЕРУ 7	ЕРУ 8	ЕРУ 9	ЕРУ 10	ЕРУ 11	ЕРУ 12	ЕРУ 13	ЕРУ 14	ЕРУ 15	ЕРУ 16	ЕРУ 17	ЕРУ 18	ЕРУ 19	ЕРУ 20
		Обща ПП		Отраслова ПП		Специфична ПП															
III	4	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x					
IV	5	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

3.1. Списък на Единиците резултати от ученето по видове професионална подготовка

ЕРУ по обща професионална подготовка – единна за всички професионални направления от Списъка на професиите за професионално образование и обучение

ЕРУ 1. Здравословни и безопасни условия на труд и опазване на околната среда

ЕРУ 2. Икономика и предприемачество

ЕРУ по отраслова професионална подготовка – единна за професиите от

ПРОЕКТ

професионално направление „Национална и лична сигурност и защита на имуществото“
ЕРУ 3. Комуникативни умения и професионална етика
ЕРУ 4. Организация, функции и координация в системата за национална сигурност

ЕРУ по специфична професионална подготовка по професията „Киберсигурност“

ЕРУ 5. Правна подготовка по професията
ЕРУ 6. Основи на дигиталните технологии и киберсредата
ЕРУ 7. Информационна сигурност и етични стандарти
ЕРУ 8. Управление на идентичност и достъп
ЕРУ 9. Приложение на защитни технологии
ЕРУ 10. Мониторинг и откриване на инциденти
ЕРУ 11. Реакция при инциденти и възстановяване
ЕРУ 12. Основи на криптографията
ЕРУ 13. Защита срещу социално инженерство
ЕРУ 14. Документиране и докладване на инциденти
ЕРУ 15. Прилагане на политики и стандарти за сигурност
ЕРУ 16. Стратегическо управление на киберсигурността
ЕРУ 17. Ръководство и развитие на екипи по киберсигурност
ЕРУ 18. Тактическа реакция и управление при киберинциденти
ЕРУ 19. Регулаторна и етична отговорност в киберсигурността
ЕРУ 20. Технологична архитектура и иновации в киберсигурността

3.2. Описание на единиците резултати от ученето за професията „Киберсигурност“

3.2.1. Обща професионална подготовка по професията

ЕРУ 1	**Здравословни и безопасни условия на труд и опазване на околната среда**
Резултат от учене 1.1	Спазва хигиенните норми и здравословните и безопасните условия на труд (ЗБУТ) на работното място
Знания	• Познава основните нормативни актове за здравословни и безопасни условия на труд • Обяснява възможните професионални и здравни рискове на работното място и причините за тяхното възникване • Разяснява основните правила при оказването на първа помощ при трудови злополуки • Изброява основните видове лични предпазни средства и техните функции • Познава видовете защитни приспособления и средства за сигнализация и маркировка за осигуряване на ЗБУТ • Изброява правилата за работа при аварии и аварийни ситуации
Умения	• Прилага мерки за безопасност на работното място • Спазва хигиенните норми на работното място • Прилага инструкции за безопасна работа • Реагира правилно при аварийни ситуации
Компетентности	• Спазва стриктно мерките за безопасност при изпълнение на различните трудови дейности
Резултат от учене 1.2	Осъществява превантивна дейност за опазване на околната среда

ПРОЕКТ

Знания	• Познава нормативни актове, свързани с опазването на околната среда, и ЗБУТ • Познава трудовоправните норми, свързани със ЗБУТ • Разяснява общите изисквания за осигуряване на ЗБУТ съобразно спецификата на провежданата дейност и изискванията на техническото, технологичното и социалното развитие с цел защита на живота, здравето и работоспособността на работещите
Умения	• Търси информация за устойчиви практики, приложими в конкретната професионална дейност • Изпълнява дейности по събиране и съхраняване на опасни продукти, излезли от употреба уреди и консумативи съобразно правилата за рециклиране • Използва технологии и материали, щадящи околната среда • Спазва практики за пестене на вода, енергия и други ресурси на работното място
Компетентности	• Правилно обработва отпадъците на работното място съобразно изискванията за сортиране • Вярно и точно разпознава замърсяващи фактори на работното място и съдейства за ограничаване на въздействието им • Способен е стриктно да следва утвърдените правила и изисквания за опазване на околната среда
Критерии за оценяване на ЕРУ	Част по теория на професията: Владее теоретични знания за: • хигиенните норми • здравословните и безопасните условия на труд на работното място • овладяването на аварийни ситуации и оказването на първа помощ • превантивната дейност за опазване на околната среда Част по практика на професията: • Избира своевременно най-адекватния тип поведение при зададената рискова ситуация • Вярно и точно определя необходимите действия за оказване на първа помощ
Средства за оценяване	Част по теория на професията: • Писмен изпит Част по практика на професията: • Изпълнение на практическа задача по индивидуално задание по практика
ЕРУ 2	**Икономика и предприемачество**
Резултат от учене 2.1	Познава основите на пазарната икономика
Знания	• Познава основни икономически понятия – търсене, предлагане, пазар, конкуренция, цена • Познава ролята на държавата в икономиката – данъци, бюджет, регулации

ПРОЕКТ

	• Обяснява дейността на организацията в контекста на основни икономически принципи и понятия • Разяснява основни понятия във финансите – приходи, разходи, печалба, инвестиции • Разбира значението на социалната и екологичната отговорност при ръководене на бизнес
Умения	• Използва основни икономически понятия, като търсене, предлагане, пазар, конкуренция и цена при изпълнение на професионалните си задачи • Отчита значението на основните финансови показатели, като приходи, разходи, печалба и инвестиции
Компетентности	• Прилага правилата и изискванията, свързани с ролята на държавата в икономиката, включително данъци, бюджет и регулации, в рамките на работната среда и своите професионални ангажименти
Резултат от учене 2.2	Познава основите на предприемачеството
Знания	• Познава същността и ролята на предприемачеството в икономиката • Изрежда основните стъпки при стартиране на бизнес, включително генериране на идея, пазарно проучване, изготвяне на бизнес план • Изброява видовете фирми и организационно-правни форми на стопанска дейност
Умения	• Разграничава видовете фирми и организационно-правните форми на стопанска дейност • Прилага знания за предприемачеството в работната си среда
Компетентности	• Идентифицира успешни практически примери за управление на бизнес начинания • Предлага решения за подобряване на дейността в съответствие с технологичните и организационните изисквания • При необходимост представя идеи и предложения пред клиенти, инвеститори или партньори, като аргументира решенията си
Критерии за оценяване на ЕРУ	Част по теория на професията: • Владее основните теоретични знания и понятия в областта на икономиката • Владее основните теоретични постановки в областта на предприемачество Част по практика на професията: • Вярно, точно и мотивирано определя действията за разрешаване на описания проблем в зададения казус • Участва в разработването на бизнес план на фирмата според изискванията на предварително дефинираното задание
Средства за оценяване	Част по теория на професията: • Писмен изпит Част по практика на професията: • Изпълнение на практическа задача по индивидуално задание по практика

ПРОЕКТ

3.2.2. Отраслова професионална подготовка по професията

ЕРУ 3	**Комуникативни умения и професионална етика**
Резултат от учене 3.1	Общува ефективно с членовете на работния екип при изпълнение на служебни дейности
Знания	• Изброява основните длъжности в екипа и обяснява тяхната роля • Разяснява как функционира екипът и какви са типовете взаимодействие между членовете му • Описва каналите за комуникация вътре в организацията (например доклади, съобщения, електронна поща)
Умения	• Общува ясно и разбираемо с колеги и преки ръководители при изпълнение на задачи • Използва подходящ тон, изказ и поведение съгласно професионалния етикет • Работи съвместно с екипа при разпределяне на задачи, смени и служебни задължения • Прилага основни правила при комуникация в дигитална среда (електронна поща, платформи, месинджъри)
Компетентности	• Поддържа професионален стил на общуване, съобразен с организационните правила • Разпознава ситуация, в която трябва да се обърне към ръководител или да съобщи информация • Работи в екип, като спазва правилата на делово поведение и професионална отговорност
Резултат от учене 3.2	Приложимо използва комуникационни умения при конфликти, инциденти и нестандартни ситуации
Знания	• Изброява основни етични правила при комуникация на работното място • Описва разликите между вербална и невербална комуникация • Обяснява основни причини за възникване на конфликти и методи за тяхното избягване
Умения	• Прилага техники за спокойно и уважително поведение при напрежение и спорове • Участва в ролеви игри или симулации за поведение в кризисни ситуации (например аварии, технически проблеми, спешни случаи) • Провежда устен инструктаж или дава кратко писмено съобщение (доклад, бележка, имейл)
Компетентности	• Избира подходящ начин на общуване спрямо ситуацията и човека, с когото комуникира • Демонстрира самоконтрол и адекватност в напрегнати ситуации • Спазва професионални и етични стандарти в писмената и устната комуникация
Критерии за оценяване на ЕРУ	Част по теория на професията: • Дефинира основни понятия, правила и етични норми в професионалната комуникация • Описва структурата на работния екип и каналите за вътрешна комуникация

ПРОЕКТ

	• Обяснява подходящо поведение и комуникация при конфликти, инциденти и кризисни ситуации Част по практика на професията: • Демонстрира ефективно устно и писмено общуване в симулирани професионални ситуации • Участва адекватно в екипна комуникация и при провеждане на инструктаж или доклад • Избира подходящи комуникационни стратегии в условия на напрежение или конфликт
Средства за оценяване	Част по теория на професията: • Писмен изпит Част по практика на професията: • Изпълнение на практическа задача по индивидуално задание по практика
ЕРУ 4	**Организация, функции и координация в системата за национална сигурност**
Резултат от учене 4.1	Разбира структурата, функциите и елементите на системата за национална сигурност на държавата
Знания	• Дефинира понятието „национална сигурност“ и нейната мисия в обществото • Изброява основните цели и функции на системата за национална сигурност • Разграничава основните компоненти: органи, институции, сили, ресурси • Познава видовете заплахи за сигурността – природни, техногенни, социални, икономически, информационни • Разбира ролята на взаимодействието между различните сфери на сигурността (вътрешна, външна, икономическа, екологична и др.)
Умения	• Представя с примери какво включва дейността по осигуряване на сигурността на държавата и населението • Илюстрира с конкретни случаи заплахи или кризи, засягащи повече от един елемент на сигурността • Обяснява защо координацията между институциите е ключова в ситуации на заплаха • Описва последици от отслабване или нарушаване на даден елемент от системата за сигурност
Компетентности	• Анализира връзките между елементите на системата за национална сигурност • Разсъждава върху необходимостта от цялостен подход и превенция • Аргументира ролята на всеки гражданин и професионалист в изграждането на устойчива система за сигурност
Резултат от учене 4.2	Разпознава институциите и службите, имащи роля в сигурността и обществения ред, и обяснява тяхното взаимодействие
Знания	• Изброява основните държавни структури, които работят за сигурността и обществения ред • Разграничава институции с различен фокус: вътрешна сигурност, обществен ред, опазване на населението, защита при бедствия и др.

ПРОЕКТ

	• Познава принципите на координация и обмен на информация между тези институции • Идентифицира примери за съвместни действия при инциденти, кризи или рутинни дейности
Умения	• Дава примери за взаимодействие между служби в реални или симулирани ситуации • Обяснява как протича координацията при сигнали за инциденти, природни бедствия, заплахи за обществения ред • Създава схематично представяне на комуникация между институции при сценарий • Описва процеса на вземане на решения и предаване на информация при служебни действия
Компетентности	• Анализира ползите от съгласуваната работа между различни звена на сигурността • Демонстрира разбиране за необходимостта от баланс между институционални отговорности и колективна реакция • Разглежда сигурността като система от взаимосвързани компоненти, в която взаимодействието е ключово
Критерии за оценяване на ЕРУ	Част по теория на професията: • Дефинира основни понятия (сигурност, функции, компоненти) • Изброява институциите и описва техните основни задачи • Обяснява логиката на взаимосвързаност между видовете сигурност и звената в системата Част по практика на професията: • Анализира примерна ситуация, застрашаваща националната сигурност или обществения ред • Представя схема за взаимодействие между институции при възникване на инцидент • Изказва аргументирано мнение за нуждата от съгласувана работа и превенция
Средства за оценяване	Част по теория на професията: • Писмен изпит Част по практика на професията: • Изпълнение на практическа задача по индивидуално задание по практика

3.2.3. Специфична професионална подготовка по професията

ЕРУ 5	**Правна подготовка по професията**
Резултат от учене 5.1	Познава същността на правната рамка за информационна и киберсигурност
Знания	• Дефинира правото на защита на личната информация и комуникация като конституционно гарантирано право • Изброява основните принципи и норми на Закон за киберсигурност (ЗКС), Наказателен кодекс (НК), GDPR, ЗЗЛД и свързаните европейски регламенти • Описва основни положения от наказателното право, свързано с престъпления в киберпространството

ПРОЕКТ

	• Познава задълженията на администратори и оператори на лични данни • Изброява основните права и задължения на служителите в звена по информационна сигурност • Представя процедурите за защита на чувствителна и класифицирана информация • Посочва приложението на административна и наказателна отговорност при нарушения в цифрова среда
Умения	• Обяснява правото на защита на личната информация в цифрова среда • Различава ролите на администратор, оператор и длъжностно лице по сигурността по отношение на защитата на личната информация • Интерпретира понятия, като „неправомерен достъп“, „нарушение на целостта на данни“, „изтичане на информация“ • Дава примери за правни последствия от действия в киберпространството (фишинг, зловреден софтуер, нерегламентиран достъп) • Описва процедури за уведомяване при инциденти съгласно нормативната уредба • Обобщава практики за работа с класифицирана информация • Интерпретира съответствието с международни стандарти за сигурност (ISO/IEC 27001, NIST)
Компетентности	• Демонстрира разбиране на основите на правото в областта на сигурността на информацията • Извършва служебни дейности при спазване на законовите и вътрешнофирмените правила за защита на данни и сигурност • Предприема действия при нарушения в съответствие с нормативните изисквания
Резултат от учене 5.2	Разпознава престъпления и нарушения в областта на киберсигурността и информационните технологии
Знания	• Изброява основни престъпления срещу цифровата идентичност (нерегламентиран достъп, саботаж, измами и др.) • Описва цифрови престъпления – фишинг, измама с лични данни, разпространение на зловреден софтуер • Дефинира понятието „кибертероризъм“ и „инцидент с критична инфраструктура“ • Посочва обстоятелства, изключващи обществената опасност на деянието • Представя понятието „цифрово доказателство“ и правния статут на логове, метаданни и системни записи • Познава основните изисквания при разследване на киберпрестъпления • Посочва процедурите за взаимодействие с правоприлагащи органи в случай на цифрово престъпление
Умения	• Разпознава наказуеми деяния в сферата на киберсигурността • Разграничава законни и незаконни действия с ИТ системи • Обяснява приложението на принципите за неизбежна отбрана в дигитален контекст

ПРОЕКТ

	• Сравнява действия, които са престъпление или административно нарушение при достъп и манипулация на данни • Анализира сценарии на престъпления – например атака срещу сървър, вирусна инвазия, изтичане на данни • Дефинира подходяща реакция при инцидент съгласно правната рамка • Обяснява стъпки за съхранение и предаване на цифрови доказателства • Съдейства на компетентните органи при сигнализиране и докладване на инцидент
Компетентности	• Демонстрира правна информираност за престъпления в дигитална среда • Реагира адекватно при установяване на нарушения, като спазва законоустановените процедури • Участва в процес по доказване и докладване на киберинциденти съгласно законовите изисквания
Критерии за оценяване на ЕРУ	Част по теория на професията: • Разглежда и разграничава правната рамка за сигурността на информацията и киберпрестъпления • Описва престъпления, специфични за цифровата среда и технологичната инфраструктура • Посочва съответните нормативни източници и процедури • Представя права и задължения на служители по сигурността в ИТ сектора Част по практика на професията: • Решава казуси, свързани с правни проблеми при инциденти • Използва адекватно правна терминология при описване на цифрови нарушения • Описва мерки за ограничаване и докладване на нарушения
Средства за оценяване	Част по теория на професията: • Писмен изпит Част по практика на професията: • Изпълнение на практическа задача по индивидуално практическо задание
ЕРУ 6	**Основи на дигиталните технологии и киберсредата**
Резултат от учене 6.1	Разпознава и използва основни компютърни компоненти и операционни системи
Знания	• Познава основните компоненти на компютърната система (процесор, памет, хранилище, периферия) • Изброява характеристиките и функциите на различни операционни системи (Windows, Linux) • Обяснява структурата на файлова система • Описва ролята на BIOS/UEFI, boot процеса и основни системни услуги • Посочва начина на организиране и достъп до данни в цифрова среда • Дефинира понятия, като драйвер, процес, услуга, виртуализация • Изброява стандартни инструменти за системна диагностика и наблюдение

ПРОЕКТ

Умения	• Стартира и използва операционна система (Windows/Linux) за изпълнение на базови задачи • Организира файлове и директории по зададена логика • Използва команди от терминал (cmd/powershelll/bash) за основни действия • Използва вградени инструменти за наблюдение на системата (Task Manager, top, htop, event viewer и др.) • Извършва базова конфигурация на локален потребител • Инсталира и деинсталира стандартен софтуер • Използва основни административни функции – shutdown, restart, device info, logs
Компетентности	• Самостоятелно използва компютърна система в професионална ИТ среда • Демонстрира увереност при работа с различни операционни системи • Разпознава системни аномалии, които изискват ескалация
Резултат от учене 6.2	Извършва основна мрежова настройка и диагностика
Знания	• Обяснява архитектурата на TCP/IP и основни мрежови модели • Дефинира понятията „IP адрес“, „подмрежа“, „шлюз“, DNS • Познава ролята на DHCP, NAT, маршрутизиране • Изброява основни мрежови услуги – HTTP, FTP, SSH, DNS, SMTP • Разграничава частни и публични IP мрежи • Познава начина на функциониране на локална мрежа (LAN) • Описва основите на Wi-Fi и Ethernet свързаност
Умения	• Конфигурира базови IP настройки (ръчно и чрез DHCP) • Използва команди, като ping, ipconfig, tracert, netstat, nslookup за диагностика • Свързва устройство към локална и безжична мрежа • Проверява свързаност и достъпност на услуги • Идентифицира основни проблеми в мрежовата свързаност • Обновява DNS и променя конфигурации при нужда • Работи с графични и текстови интерфейси за мрежова настройка
Компетентности	• Демонстрира умения за първоначално конфигуриране и диагностика на мрежа • Поддържа основна мрежова свързаност в среда с ниска сложност • Докладва установени отклонения или подозрителна активност
Резултат от учене 6.3	Използва основни комуникационни и технически термини на чужд език при работа с операционни системи, софтуер и цифрови среди
Знания	• Разпознава често използвани чуждоезични термини в софтуерни интерфейси и системни съобщения • Познава основни думи и изрази в контекста на компютърна и мрежова работа (например save, settings, network, security) • Разбира същността на инструкции, предупреждения и системни указания на чужд език
Умения	• Навигира в интерфейс на чужд език при операционни системи и приложения • Разбира и следва технически инструкции, ръководства и помощни съобщения на чужд език

DRAFT

	• Използва чуждоезични термини при търсене на решения и при работа със системни инструменти
Компетентности	• Демонстрира увереност при работа с цифрови системи и платформи с чуждоезичен интерфейс • Прилага знания за термини и инструкции на чужд език в реални професионални задачи • Спазва указания и процедури, базирани на чуждоезично цифрово съдържание
Критерии за оценяване на ЕРУ	Част по теория на професията • Поставените задачи са изпълнени самостоятелно и в рамките на предварително зададеното за това време Част по практика на професията • Демонстрирани са знания, умения и компетентности, свързани с използването на дигиталните технологии
Средства за оценяване	Част по теория на професията: • Писмен изпит Част по практика на професията: • Изпълнение на практическа задача по индивидуално практическо задание
ЕРУ 7	**Информационна сигурност и етични стандарти**
Резултат от учене 7.1	Разпознава основните принципи на управление на идентичност и контрол на достъп в ИТ системи
Знания	• Дефинира основните принципи на информационната сигурност – конфиденциалност, цялостност, наличност • Описва понятието „информационен актив“ и видовете чувствителна информация • Изброява категориите заплахи за сигурността на информацията (технологични, организационни, човешки фактор) • Разпознава основните цели на организационната политика по информационна сигурност • Посочва методи за защита на данни при съхранение и предаване • Обяснява ролята на пароли, криптиране, многофакторна автентикация • Изброява добри практики за сигурно поведение при работа с информационни системи
Умения	• Разграничава видовете заплахи за информацията – вътрешни, външни, случайни, злонамерени • Идентифицира признаци на нарушение в информационната сигурност • Обяснява действията си при открит риск или инцидент • Използва базови средства за защита на лични и служебни данни • Оценява ситуации, в които поверителна информация е застрашена • Поддържа сигурна работна среда – заключване на екрана, контрол на достъп • Прилага елементарни процедури за защита на данни при ежедневна работа
Компетентности	• Демонстрира съобразено поведение при работа с информационни системи

ПРОЕКТ

	• Изпълнява служебните си задължения с внимание към защитата на чувствителна информация • Осъзнава собствената си отговорност при боравене с информационни активи
Резултат от учене 7.2	Прилага етични норми и професионално поведение при работа с информационни ресурси
Знания	• Описва значението на етичния кодекс в сферата на информационните технологии • Изрежда основните принципи на професионалната етика: добросъвестност, отговорност, поверителност • Познава видовете неправомерно поведение – шпионаж, умишлено изтичане на информация, неоторизиран достъп • Дефинира термини, като „вътрешна заплаха“, „злоупотреба със служебен достъп“ • Описва последствията от етични нарушения – дисциплинарни, административни, наказателни • Знае кога и как следва да сигнализира за нарушение • Разпознава поведението, което застрашава интегритета на системата или екипа
Умения	• Спазва вътрешни правила за етично поведение и защита на информацията • Разграничава допустими и недопустими действия при достъп до данни • Демонстрира етично поведение при комуникация с колеги, клиенти, външни лица • Използва служебни ресурси само по предназначение • Обяснява действията си при наблюдение на неетично или рисково поведение • Докладва по установен ред за съмнения за нарушения • Предприема отговорни действия за предотвратяване на етични и информационни нарушения
Компетентности	• Изпълнява служебните си функции с висока степен на лична и професионална отговорност • Участва в изграждането на култура на доверие, сигурност и етика в работния екип • Поддържа лична и организационна репутация чрез добросъвестна работа
Резултат от учене 7.3	Прилага вътрешните политики за сигурност и поведение при работа с информационни активи
Знания	• Познава структурата и съдържанието на вътрешните политики за информационна сигурност • Изброява ключови организационни документи: политика за пароли, правила за достъп, процедури при инциденти • Описва понятието „клас на чувствителност на информацията“ и как се обозначава • Разпознава правила за работа с носители на информация – USB, външни дискове, споделени устройства • Познава стъпките за докладване на нарушение • Обяснява ролята на служителите по сигурността (CISO, DPO)

ПРОЕКТ

	• Различава стандартни процедури при onboarding и offboarding на служители
Умения	• Следва процедурите за защита на активи според установените правила • Спазва ограниченията за използване на лични/външни устройства в защитена среда • Попълва и съхранява регистрационни формуляри, свързани с достъп и сигурност • Прилага добра практика при обмен на информация вътре и извън организацията • Използва правилно системи за служебна комуникация (включително криптирани канали, VPN) • Реагира съгласно указанията при съмнение за пробив или неоторизиран достъп • Докладва своевременно инцидент чрез утвърдения канал
Компетентности	• Действа отговорно и съобразено с вътрешната политика за сигурност на организацията • Поддържа съответствие с изискванията на длъжността, свързани с поверителност и защита на данни • Съдейства за изграждане на култура на спазване на сигурността в екипа
Критерии за оценяване на ЕРУ	Част по теория на професията: • Дефинира основните принципи на информационната сигурност – конфиденциалност, цялостност, наличност • Представя етичните норми и поведението, очаквано при работа с цифрова информация • Обяснява ролята на вътрешните политики за сигурност • Разграничава служебно и неетично поведение при боравене с информация • Идентифицира основни правила за работа с класифицирана или чувствителна информация • Познава процеса на докладване на инцидент и правните последствия от нарушение Част по практика на професията: • Оценява реална или симулирана ситуация и идентифицира потенциален риск за информационната сигурност • Прилага правилно модел на поведение при контакт с чувствителни данни • Избира подходящ начин за реакция при неетично поведение в работна среда • Демонстрира изпълнение на действия съгласно вътрешна процедура при инцидент – попълване на доклад, комуникация с отговорно лице • Използва защитени методи за споделяне или предаване на информация • Следва организационна политика при работа с преносими носители и лични устройства
Средства за оценяване	Част по теория на професията: • Писмен изпит Част по практика на професията:

ПРОЕКТ

	• Изпълнение на практическа задача по индивидуално задание по практика
ЕРУ 8	**Управление на идентичност и достъп**
Резултат от учене 8.1	Разпознава основните принципи на управление на идентичност и контрол на достъп в ИТ системи
Знания	• Дефинира понятията „идентификация“, „автентикация“, „авторизация“ • Изброява основните видове потребителски идентичности и роли • Обяснява принципа на „минимални права“ (least privilege) • Описва ролеви модели за достъп (RBAC, ABAC) • Посочва разликата между локален и централен контрол на достъп • Назовава основни технологии за идентификация и достъп – потребител/парола, PIN, токен, карта, биометрия • Разграничава типовете потребители – администратори, обикновени гости и служебни акаунти
Умения	• Различава нива на достъп според роли и отговорности • Сравнява методи за автентикация • Избира подходяща автентикационна техника спрямо контекста • Обяснява процеса на заявка, одобрение и активиране на достъп • Води списък с потребители и достъпни ресурси • Разграничава потенциални слабости в контрола на достъп • Докладва несъответствие в правата или неоторизиран достъп
Компетентности	• Спазва правилата за достъп и защита на ИТ ресурси • Приложимо използва идентификационни системи при работа с информационни активи • Поддържа поверителността и целостта на личните си идентификационни данни
Резултат от учене 8.2	Използва технологии за автентикация и многослойна защита на достъп
Знания	• Описва принципа на многофакторна автентикация (MFA) • Изброява факторите на автентикация: знание, притежание, биометрия • Обяснява приложението на токени, смарт карти, OTP кодове • Разпознава възможности и ограничения на биометрични системи • Познава основни рискове при незащитен достъп • Посочва въздействието на незащитена автентикация върху сигурността • Разграничава автентикация в локална мрежа и в облачна услуга
Умения	• Активира MFA за даден акаунт • Настройва базови параметри за вход (парола, резервен достъп) • Използва автентикационни приложения • Използва криптирани канали при вход в системи (VPN, SSH, HTTPS) • Различава легитимен от съмнителен опит за вход • Променя и управлява паролите си според вътрешни правила • Прилага организационна политика за сигурна идентичност
Компетентности	• Демонстрира способност да управлява достъпа си в рамките на организацията

ПРОЕКТ

	• Изпълнява действия с повишено внимание при автентикация • Поддържа техническа и етична хигиена при вход в системи
Резултат от учене 8.3	Документира и прилага правила за управление на потребители и идентичности
Знания	• Изброява организационни процедури за регистрация и дерегистрация на потребители • Описва типичния жизнен цикъл на потребителски акаунт • Познава принципите на достъпа по заявка и одобрение • Различава основни категории на чувствителна информация • Маркира задълженията на потребителите по вътрешни политики • Обяснява ролята на администраторите по достъпа • Познава изискванията за одит и проследимост
Умения	• Попълва заявка за създаване/промяна на потребителски достъп • Създава и актуализира регистрационни форми или справки за достъп • Сравнява списък на реални и регистрирани потребители • Открива акаунти без валиден собственик или нужда от деактивиране • Документира инцидент, свързан с неправомерен достъп • Използва шаблони и формуляри съгласно вътрешните правила • Съдейства за вътрешни одити по достъп
Компетентности	• Спазва установената процедура за администриране на достъп • Гарантира отчетност и прозрачност при работа с потребителски права • Работи в екип със системни администратори и специалисти по сигурността
Резултат от учене 8.4	Прилага организация и контрол на физическия достъп до информационни ресурси
Знания	• Обяснява значението на физическата защита на сървърни и комуникационни зони • Изброява средствата за контрол на физически достъп – карти, пинове, биометрия • Познава рискове от неконтролиран достъп до технически помещения • Маркира политиката за достъп до помещения с ограничен достъп • Разграничава типове зони според критичност (свободен, контролиран, защитен достъп) • Познава техниките за регистриране и логване на достъпи • Изброява действията при засичане на неоторизиран достъп
Умения	• Различава нива на физически достъп по длъжност и разрешение • Използва средства за легитимация в контролирани зони • Следва протокол при въвеждане на посетител или външна проверка • Попълва запис в дневник за достъп • Докладва съмнителна активност в чувствителна зона • Съблюдава пропускателния режим според вътрешни правила • Прилага указания при аварии, пожари или инциденти с физически достъп

ПРОЕКТ

Компетентности	• Прилага контролирана и отчетна практика при физическия достъп до ИТ активи • Участва в поддържането на сигурна среда в зоните с ограничен достъп • Реагира адекватно при инцидент или нарушение на физическата сигурност
Критерии за оценяване на ЕРУ	Част по теория на професията: • Дефинира понятието за управление на идентичност, достъп и автентикация • Използва типове системи и технологии за удостоверяване • Представя процедурите за регистриране, одит и контрол на потребителски достъп • Обяснява принципите за контрол на физическия достъп до чувствителни ресурси Част по практика на професията: • Конфигурира профил и определя роля в ИТ среда • Демонстрира използване на токен/многофакторна автентикация • Попълва документ за създаване/прекратяване на достъп • Следва правила за физически достъп и попълва регистрационен журнал
Средства за оценяване	Част по теория на професията: • Писмен изпит Част по практика на професията: • Изпълнение на практическа задача по индивидуално задание по пррактика
ЕРУ 9	**Приложение на защитни технологии**
Резултат от учене 9.1	Разпознава основните защитни технологии за информационна сигурност
Знания	• Изброява основните класове защитни технологии: антивируси, защитни стени, IDS/IPS, прокси сървъри, филтри за съдържание • Описва функциите на антивирусна система и подходите за откриване на зловреден код • Дефинира понятието „файъруол“ и видовете правила за трафик • Разграничава мрежово-базирана и хост-базирана защита • Обяснява понятията „бял“ и „черен списък“ • Представя ролята на прокси сървъри и уебфилтрация • Познава принципите на поведенчески и сигнатурен анализ
Умения	• Разпознава защитните технологии в дадена среда • Описва действието на всяка технология спрямо заплахи • Прилага защитни технологии в подходяща ситуация спрямо конкретните заплахи • Интерпретира взаимодействието между различни слоеве на защита • Извлича основна информация за състоянието на системата от защитен софтуер • Сравнява характеристики на алтернативни решения • Обяснява как комбинация от защитни технологии създава слоеста защита
Компетентности	• Демонстрира разбиране за основната архитектура на системите за защита на информацията

ПРОЕКТ

	• Може да участва в поддържане на многослойна защитна инфраструктура
Резултат от учене 9.2	Конфигурира и използва базови антивирусни и мрежови защитни системи
Знания	• Посочва функциите и модулите на антивирусна програма • Дефинира разлика между сканиране на файлове, памет, стартиращи процеси и уебактивност • Описва настройките на персонален файъруол • Разграничава разрешен/забранен трафик • Изброява действията при засечена заплаха • Познава типовете логове, които генерират защитните системи • Обяснява как се настройват автоматични актуализации на базите със сигнатури
Умения	• Инсталира и конфигурира антивирусен софтуер • Извършва пълно и частично сканиране • Настройва автоматично поведение при откриване на заплаха • Конфигурира базови правила във файъруол • Разрешава/забранява програми или портове • Извлича логове и ги анализира за инциденти • Извършва рутинни проверки и обновления
Компетентности	• Спазва утвърдените правила за техническа сигурност • Самостоятелно поддържа защитните средства в своя и мрежова работна среда • Докладва навреме при съмнение за отклонение или заплаха
Резултат от учене 9.3	Работи със системи за филтриране и контрол на уебдостъп
Знания	• Дефинира понятията „прокси сървър“, „филтрация на съдържание“, „блокиране на уебсайтове“ • Описва въздействието на филтри върху сигурността и производителността • Изброява подходите за категоризация на сайтове • Обяснява какво е DNS филтриране • Познава инструментите за родителски/корпоративен контрол • Описва базови настройки на URL филтър • Разграничава ползването на защитени и незащитени връзки (HTTP/HTTPS)
Умения	• Конфигурира филтриране на съдържание чрез антивирус/прокси • Създава списъци с блокирани/разрешени адреси • Използва административен панел за мониторинг на трафик • Проверява DNS филтър за засечени рискови дестинации • Наблюдава поведението на потребители чрез наличните инструменти • Променя правила при необходимост и по зададени критерии • Обобщава резултати от блокирани достъпи
Компетентности	• Поддържа основни механизми за уебзащита в потребителска или учебна ИТ среда • Съдейства за ограничаване на зловреден достъп до интернет съдържание • Докладва блокирани/рискови активности, установени чрез филтрираща система

ПРОЕКТ

Резултат от учене 9.4	Прилага защитни технологии за физическа сигурност в контекста на киберсигурността
Знания	• Дефинира ролята на физическата сигурност като част от цялостната информационна сигурност • Изброява защитни технологии за физически достъп: електронни ключове, RFID, биометрични скенери, видеонаблюдение, алармени системи • Описва рискове от неоторизиран физически достъп до мрежови и сървърни ресурси • Разграничава зони с различно ниво на достъп и тяхното технологично обезпечаване • Обяснява принципа на „контролна точка за достъп“ (Access Control Point) • Представя взаимодействието между ИТ системи и физическа охрана (например SIEM + системи за достъп) • Познава принципите на логване и проследимост при физически достъп
Умения	• Работи с технологии за контрол на физически достъп до чувствителни зони • Използва електронни идентификатори (карти, токени, пинове) при контролирано преминаване • Реагира при алармен сигнал или неоторизиран физически опит за достъп • Поддържа запис за физически достъп до помещения и устройства • Обяснява правилата за комбинирана защита (физическа+ логическа) в ИТ среда • Проверява и отчита състоянието на устройствата за физическа защита (електрически заключвания, сензори, видеокамери) • Докладва инциденти или съмнения за заобикаляне на физически защити
Компетентности	• Прилага процедури за контрол на физическия достъп до информационни и технически ресурси • Работи съвместно с екипи по охрана, техническа поддръжка и киберсигурност при осигуряване на защита • Осигурява проследимост и отговорност при работа в контролирана зона • Поддържа култура на внимание и отчетност при работа в помещения с критични ИТ активи
Критерии за оценяване на ЕРУ	Част по теория на професията: • Дефинира основните класове защитни технологии и принципите им на работа в киберсреда • Обяснява ролята на многослойната защита и принципите за уебфилтрация и контрол на съдържанието • Представя взаимодействието между логическа и физическа сигурност при защита на информационни ресурси Част по практика на професията: • Конфигурира антивирусен софтуер или защитна стена с основни настройки за сигурност • Извлича и интерпретира данни от логове или системи за контрол на достъп

ПРОЕКТ

	• Прилага технологични средства за защита в симулирана ситуация, включително при инцидент с физически достъп
Средства за оценяване:	Част по теория на професията: • Писмен изпит Част по практика на професията: • Изпълнение на практическа задача по индивидуално задание по практика
ЕРУ 10	**Мониторинг и откриване на инциденти**
Резултат от учене 10.1	Разпознава основни източници на информация за състоянието на мрежи и системи
Знания	• Изброява основните източници на данни за наблюдение – лог файлове, системни съобщения, аларми • Описва функцията на SIEM, IDS/IPS и мониторингови конзоли • Обяснява понятията „събитие“ и „инцидент“ в контекста на информационната сигурност • Разграничава нива на критичност на аларми и известия • Познава основни параметри на нормално поведение на система/мрежа • Маркира ключови индикатори за нарушение (Indicators of Compromise – IoC) • Разпознава логически атаки спрямо автентикация, услуги или мрежова комуникация
Умения	• Чете лог файлове и идентифицира основни параметри (дата, източник, събитие) • Навигира административен панел на SIEM или IDS • Проверява статуса на аларма и я сравнява с нормалните стойности • Разграничава фалшиви положителни от реални аларми • Филтрира и сортира събития по време, устройство, IP или потребител • Обяснява сигнал от системата спрямо контекста • Използва основни IoC като критерии за анализ
Компетентности	• Демонстрира осъзнато поведение при наблюдение на информационна инфраструктура • Поддържа точност и последователност при работа с инструменти за мониторинг • Съдейства за навременно откриване на подозрителна активност
Резултат от учене 10.2	Прилага процедури за анализ и първоначална оценка на инцидент
Знания	• Обяснява последователността при оценка на инцидент – идентификация, анализ, категоризация • Познава понятията „време за реакция“, „ескалация“, „бързо ограничаване“ • Изброява изискванията за документация и докладване при инцидент • Описва критериите за оценка на въздействието от инцидент • Познава стандартни сценарии за мрежови атаки (brute-force, scanning, DoS и др.) • Посочва значение на своевременното сигнализиране • Разграничава инцидент от операционен проблем или потребителска грешка

ПРОЕКТ

Умения	• Анализира съдържание на аларма и формулира хипотеза за събитието • Съпоставя няколко събития за откриване на обща причина • Попълва формуляр за инцидент (дата, засегнати системи, описание) • Етикетира инцидента според критичност и въздействие • Решава дали инцидентът подлежи на ескалация • Докладва своевременно към отговорното лице или екип • Участва в първично ограничаване на достъпа или изолиране на системата
Компетентности	• Подпомага навременно идентифициране и ограничаване на инциденти • Работи съгласно организационните процедури за сигурност • Гарантира точност и последователност в анализите и докладите
Резултат от учене 10.3	Поддържа отчетност и комуникация при наблюдение и сигнализиране
Знания	• Изброява видовете документи и записи при инцидент – логове, формуляри, дневници • Познава структурата на инцидентен доклад • Обяснява значението на навременна и точна комуникация • Разпознава комуникационни канали (вътрешен тикетинг, e-mail, конзолни известия) • Описва правилата за предаване на чувствителна информация • Посочва отговорните роли при инцидентна комуникация (SOC, CIRT, CISO) • Познава процедурите за съхранение на доказателства
Умения	• Попълва дневник за наблюдение и действия • Изготвя кратък доклад за открит инцидент • Съобщава по зададен канал (вътрешен тикет, устно, e-mail) • Предава ясно и конкретно информацията – какво, кога, къде, как • Съхранява събраните доказателства според правилата • Работи в екип с останалите участници в инцидентния отговор • Проследява следващи стъпки след сигнализиране
Компетентности	• Осигурява отчетност и проследимост при наблюдение на ИТ системи • Съдейства ефективно в процеса на инцидентен отговор • Поддържа комуникация в условия на повишено напрежение и риск
Критерии за оценяване на ЕРУ	Част по теория на професията: • Дефинира понятието „информационен инцидент“ и обяснява разликата между събитие и инцидент • Изрежда основните източници за наблюдение – логове, аларми, сигнали от IDS/IPS и SIEM системи • Описва процедурите за анализ, оценка, документиране и ескалиране на инцидент Част по практика на професията: • Разпознава потенциален инцидент в симулирана работна среда (например аларма в SIEM панел) • Попълва формуляр за инцидент с точна информация (дата, системи, описание, действия)

ПРОЕКТ

	• Извършва първична реакция – сигнализиране, изолиране, маркиране на събития, според организационни указания
Средства за оценяване	Част по теория на професията: • Писмен изпит Част по практика на професията: • Изпълнение на практическа задача по индивидуално задание по практика
ЕРУ 11	**Реакция при инциденти и възстановяване**
Резултат от учене 11.1	Разпознава видовете инциденти и предприема първични действия при киберинцидент
Знания	• Дефинира понятието „киберинцидент“ и различните му типове (malware, phishing, DDoS, неоторизиран достъп и др.) • Обяснява основните фази на жизнения цикъл на инцидента: идентификация, реакция, възстановяване • Разглежда видовете въздействие от инцидент – по системи, услуги, данни и потребители • Познава концепцията за „време за реакция“ и „време за възстановяване“ • Изброява видовете системи и инструменти, използвани за откриване и управление на инциденти • Описва критични индикатори за пробив (IoC) и поведение, различаващо се от нормалното • Обяснява рисковете от неадекватна или забавена реакция при инцидент
Умения	• Разграничава инцидент от нормално събитие или грешка при работа • Реагира при аларма, като я анализира и предприема предварителни действия • Участва в активното идентифициране на засегнатата система или потребител • Докладва инцидента чрез съответния канал за ескалация • Попълва формуляр с основни параметри на инцидента • Сравнява текущия случай със стандартен сценарий на често срещани атаки • Описва предприетите действия и състоянието на засегнатите системи
Компетентности	• Действа в съответствие с вътрешната процедура за реакция при инциденти • Прилага навременна и обоснована първична реакция при инциденти в рамките на правомощията си • Съдейства за ограничаване на щетите от инцидента
Резултат от учене 11.2	Изолира засегнати системи и съдейства при ограничаване на инцидента
Знания	• Изброява стандартните методи за изолиране на засегнати устройства от мрежата • Познава командите и административните средства за ограничаване на достъпа (локално и мрежово) • Разграничава пълна и частична изолация

ПРОЕКТ

	• Описва основни подходи за блокиране на трафик, IP адреси, потребителски профили • Обяснява понятието „съдържателна изолация“ при корпоративни услуги (например e-mail filtering, file blocking) • Познава критериите за определяне на приоритет при инцидент • Описва организацията на комуникацията между отдели при инцидент (SOC, ИТ, ръководство)
Умения	• Прекъсва мрежовата връзка на засегната система при нужда (логически или физически) • Използва интерфейс на SIEM, IDS или друг инструмент за временно блокиране на комуникации • Преустановява активни потребителски сесии • Дава предложение за временно ограничение на достъпа до услуга • Документира извършените действия по изолиране • Комуникира с екипа по сигурност при необходимост от допълнителни мерки • Участва в сесии за оценка на предприетите ограничителни действия
Компетентности	• Действа самостоятелно при изпълнение на задачи по изолиране на системи • Спазва тактическата последователност и координация при работа с критични инциденти • Работи екипно и ефективно в динамична ситуация
Резултат от учене 11.3	Подпомага възстановяването и докладва резултатите от инцидент
Знания	• Обяснява основните принципи на възстановяване на системи след инцидент • Познава типовете бекъп – пълен, инкрементален, диференциален • Изброява методи за проверка на целостта след възстановяване • Описва съдържанието на финален инцидентен доклад • Обяснява какво представлява процеса на анализ след инцидент • Познава основите на Root Cause Analysis (RCA) или анализа на първопричините • Обяснява съображенията за повторно въвеждане в експлоатация на засегната система
Умения	• Подпомага възстановителния екип чрез предоставяне на информация от логове и събития • Участва в проверка на нормалната функционалност след възстановяване • Документира времето и действията по възстановяване • Съдейства за идентифициране на първопричината на инцидента • Изготвя кратък отчет за предприети действия, срокове и резултати • Подпомага процеса на тестване на мерките за възстановяване • Съдейства при актуализиране на процедури за бъдещо предотвратяване
Компетентности	• Действа с внимание към устойчивостта на системите и целостта на информацията

ПРОЕКТ

	• Участва в процеса на учене от инциденти и подобряване на сигурността • Осигурява прозрачност и отчетност на предприетите действия в етапа след реакция на инцидент
Критерии за оценяване на ЕРУ	Част по теория на професията: • Описва дейността по идентифициране, ограничаване и възстановяване след киберинцидент, включително оценка на въздействието и създаване на инцидентен доклад • Дефинира правилата, указанията и етапите на реакция при инцидент в съответствие с вътрешна процедура, ръководство или национален/международен стандарт (например NIST, ISO/IEC 27035) • Подчертава примерни тактически указания за действия при различни типове инциденти – неоторизиран достъп, зловреден софтуер, DDoS, фишинг и др. Част по практика на професията: • Обяснява дейността по първично идентифициране и документиране на киберинцидент, включително събиране на доказателства и комуникация с отговорни лица • Различава правилата, указанията и изискванията за ограничаване на инцидент чрез изолиране на система, блокиране на потребител/трафик и подкрепа при възстановяване • Дава примери за тактически указания за действия при различни инциденти, включително докладване, логическо ограничаване на въздействието, възстановяване от резервни копия и отчетност за предприетите действия след инцидента
Средства за оценяване	Част по теория на професията: • Писмен изпит Част по практика на професията: • Изпълнение на практическа задача по индивидуално задание по практика
ЕРУ 12	**Основи на криптографията**
Резултат от учене 12.1	Разпознава основните криптографски концепции и тяхното приложение
Знания	• Дефинира понятията „криптиране“, „декриптиране“, „хеширане“, „цифров подпис“ • Разграничава симетрична и асиметрична криптография • Описва ролята на публичния и частния ключ в криптирането • Познава основите на PKI (инфраструктура с публичен ключ) • Изброява алгоритми за криптиране и хеширане (AES, RSA, SHA-256 и др.) • Обяснява предназначението на цифрови сертификати • Описва функциите на удостоверяващите органи (CA)
Умения	• Разпознава криптиран и некриптиран трафик (например HTTP vs HTTPS) • Демонстрира използване на инструмент за хеширане на файлове • Използва базова криптографска програма за криптиране/ декриптиране на данни (например VeraCrypt, GPG) • Проверява валидността на цифров сертификат в уеббраузър

ПРОЕКТ

	• Идентифицира несъответствия в криптирана комуникация (например сертификат с изтекъл срок) • Използва хеш за проверка на целостта на файл • Работи с инструменти за генериране и съхранение на ключове
Компетентности	• Прилага основни криптографски средства за защита на данни при пренос или съхранение • Участва в процеса на проверка на цифрова идентичност и валидност на комуникация • Изпълнява задачи с повишено внимание към конфиденциалността и целостта на информацията
Резултат от учене 12.2	Използва сигурни канали за електронна комуникация
Знания	• Познава методите за защита на комуникацията – VPN, SSL/TLS, SSH • Обяснява понятието „криптографски протокол“ • Разграничава сигурна и несигурна комуникация в локални и интернет среди • Изброява рискове от използване на отворени и незащитени мрежи • Описва процедурите за създаване на защитена сесия • Познава термини, като „шифрован тунел“, „криптирана връзка“, „автентикация на канал“ • Изброява базови приложения и протоколи с вградена криптография (HTTPS, FTPS, SFTP, SSH)
Умения	• Установява VPN връзка чрез клиентска програма • Свързва се към отдалечен сървър чрез SSH клиент • Разпознава криптирани имейли и съобщения (PGP, S/MIME) • Проверява сигурността на уебсайт чрез преглед на сертификат • Използва криптирани облачни услуги при споделяне на файлове • Работи с криптирани чат/комуникационни платформи (например Signal) • Следва правилата за сигурна комуникация в организационен контекст
Компетентности	• Гарантира сигурността на комуникационните канали в рамките на служебните задължения • Работи отговорно с чувствителна информация в цифрова среда • Поддържа конфиденциалност при вътрешна и външна електронна кореспонденция
Резултат от учене 12.3	Прилага политики и добри практики за криптографска защита на данни
Знания	• Изброява организационни изисквания за криптиране на данни и защита на носители • Познава политики за сигурност, свързани с криптографски ключове • Описва рискове при неправилно управление на ключове или сертификати • Познава стандарти за криптографска сигурност (например NIST SP 800-57, ISO/IEC 27001) • Разграничава роли в процеса по управление на ключове – създател, разпространител, потребител • Дефинира „жизнен цикъл на криптографски ключ“

ПРОЕКТ

	• Познава процедурите за унищожаване на чувствителни данни
Умения	• Прилага организационни инструкции за използване на криптирани носители (USB, HDD) • Използва криптиране на устройство (BitLocker, LUKS и др.) • Документира използване или предаване на криптографски материал • Следва указания за съхранение и архивиране на ключове • Оценява рисковете при използване на външни облачни услуги без криптиране • Прилага мерки за защита при работа с преносими устройства • Спазва срокове за подновяване или отнемане на сертификати
Компетентности	• Спазва добри практики за криптографска защита съгласно вътрешните политики • Работи съгласувано с администраторски и технически екип по сигурността • Съдейства за предотвратяване на инциденти, свързани с компрометиране на криптирана информация
Критерии за оценяване на ЕРУ	Част по теория на професията: • Описва дейността по криптографска защита на данните чрез симетрично и асиметрично криптиране, хеширане и използване на цифрови подписи • Дефинира правилата, указанията и изискванията за създаване на сигурни комуникационни канали с помощта на криптографски протоколи (SSL/TLS, VPN, SSH) • Подчертава примерни тактически указания за използване на криптографски решения в различни ситуации – при съхранение на данни, при комуникация и при работа с чувствителна информация Част по практика на професията: • Обяснява дейността по защита на данните чрез използване на криптирани файлове, хеш функции и сигурни канали за комуникация • Различава правилата, указанията и изискванията за работа с криптирани носители, криптирана електронна поща и обмен на чувствителни данни • Дава примери за използване на базови криптографски инструменти (например GPG, BitLocker, сертификати, VPN клиент) при изпълнение на служебни задачи
Средства за оценяване	Част по теория на професията: • Писмен изпит Част по практика на професията:

ПРОЕКТ

	• Изпълнение на практическа задача по индивидуално задание по практика
ЕРУ 13	**Защита срещу социално инженерство**
Резултат от учене 13.1	Разпознава социалните техники за измама и техните характеристики
Знания	• Дефинира понятието „социално инженерство“ в контекста на информационната сигурност • Изброява основните видове атаки чрез социално инженерство – фишинг, спиър-фишинг, вишинг, бейтинг, pretexting и др. • Обяснява психологическите механизми, използвани при социално инженерство (страх, авторитет, любопитство, спешност и др.) • Разграничава таргетирани от масови атаки • Познава признаци на фалшива комуникация (e-mail, SMS, обаждане) • Изброява сценарии, при които най-често се използва социално инженерство – инцидентни доклади, подкана за спешна смяна на парола, фалшиви фактури • Описва последствията от успешна атака (достъп до системи, измама, кражба на данни)
Умения	• Разпознава съобщения, съдържащи индикатори за фишинг • Анализира елементи на фалшива комуникация – подправен подател, неправилен домейн, необичаен стил • Съпоставя шаблонни атаки с реални казуси • Докладва съмнително съобщение чрез зададен служебен канал • Проверява автентичността на източници чрез обратна комуникация • Споделя примери за срещани атаки и действия, които са предотвратили щетите • Работи съобразено с правилата за отваряне на прикачени файлове и следване на линкове
Компетентности	• Демонстрира осъзнато поведение в среда, изложена на социални заплахи • Прилага предпазни мерки при електронна комуникация • Предприема действия при съмнение за манипулация чрез социални канали
Резултат от учене 13.2	Реагира при опит за социално инженерство
Знания	• Описва стъпките за реакция при установяване на фишинг съобщение или опит за манипулация • Познава вътрешните процедури за докладване на инцидент от човешки произход • Изброява организационни роли, които участват в реакцията – служител по сигурността, ИТ екип, ръководство • Дефинира понятието „инцидент с човешка манипулация“ • Обяснява рисковете от несподеляне или прикриване на опит за измама • Разграничава инцидент, възникнал от човешка грешка, от умишлена атака • Познава елементите на формуляра за съобщаване на инцидент

ПРОЕКТ

Умения	• Извършва първична проверка на съобщението, без да го отваря или изпълнява • Попълва инцидентен формуляр със съмнение за фишинг или измама • Уведомява прекия ръководител и звеното по сигурност • Съдейства при изолирането на съмнителната комуникация (например чрез маркиране в системата) • Следи официалната реакция и предупреждение към други потребители • Участва в кратко устно/писмено докладване на инцидента • Прилага указания за временно поведение след инцидент (например въздържане от комуникация с определен подател)
Компетентности	• Реагира отговорно и съгласувано при социално инженерна атака • Поддържа професионално поведение при съмнение за човешка манипулация • Гарантира точност и отчетност в докладите, свързани със социални атаки
Резултат от учене 13.3	Участва в дейности за повишаване на осведомеността относно социалното инженерство
Знания	• Описва ролята на осведомеността в превенцията срещу социални атаки • Познава форми на вътрешни кампании и обучения (електронни бюлетини, плакати, демонстрации, игри) • Разграничава подходи за обучение на различни групи служители – ИТ персонал, администрация, външни изпълнители • Изброява често срещани грешки при реакция на фишинг • Обяснява стойността на симулирани тестове (фишинг кампании, проверка на реакция) • Познава понятия, като „психологическа устойчивост“, „информационна хигиена“, „култура на сигурност“ • Дефинира поведенчески индикатори, които подсказват за излагане на риск
Умения	• Участва в кратко вътрешно обучение или инструктаж по сигурност • Разпространява съобщения или материали, свързани с кампания по осведоменост • Събира обратна връзка от потребители за подозрителни случаи • Подготвя базова информация за примерни атаки и превантивни мерки • Съдейства при организацията на симулационен фишинг тест • Подпомага служители с по-малка ИТ грамотност при идентифициране на рискови съобщения • Препраща материали или ресурси за обучение
Компетентности	• Участва в изграждането на осъзнато и отговорно поведение в организацията • Подкрепя вътрешните инициативи по сигурност, свързани с човешки фактор • Служи като комуникационна връзка между технически и нетехнически служители при рискови ситуации

ПРОЕКТ

Критерии за оценяване на ЕРУ	Част по теория на професията: • Описва дейността по разпознаване и предотвратяване на социални атаки чрез електронна и междуперсонална комуникация, включително фишинг, спиър-фишинг, вишинг и други форми на манипулация • Дефинира правилата, указанията и изискванията за реакция при установяване на опит за социално инженерство и поведението на служителя при комуникация с неизвестен или съмнителен източник • Подчертава примерни тактически указания за действия при възникване на социално-инженерен инцидент, включително докладване, изолиране и повишаване на осведомеността сред колеги Част по практика на професията: • Обяснява дейността по идентифициране на признаци за фалшиви имейли, съобщения или обаждания и демонстрира поведение при съмнение за измама • Различава правилата и добрите практики за комуникация с външни лица, включително използването на служебни канали и ограничения при споделяне на информация • Дава примери за участие в дейности по осведоменост, симулирани фишинг тестове и обучение на потребители, свързани с човешкия фактор в сигурността
Средства за оценяване	Част по теория на професията: • Писмен изпит Част по практика на професията: • Изпълнение на практическа задача по индивидуално задание по практика
ЕРУ 14	**Документиране и докладване на инциденти**
Резултат от учене 14.1	Описва дейността по охрана на селскостопанско имущество
Знания	• Изброява видовете документация, свързана с инциденти – формуляр за инцидент, журнал за събития, лог файл, дневник на реакцията • Познава структурата и задължителните елементи на инцидентен доклад (време, тип, засегнати системи, описание, действия, отговорници) • Описва разликата между оперативен журнал, формален доклад за инцидент и анализ на причините и последствията след инцидента • Дефинира понятието „проследимост“ в контекста на информационната сигурност • Познава вътрешните правила за документиране в организацията • Изброява задълженията на персонала по отношение на отчетност при сигурност • Обяснява значението на ясното, обективното и краткото изразяване в служебната документация
Умения	• Разпознава подходящия документ според вида на инцидента • Съпоставя елементи от различни доклади и извежда общата структура

ПРОЕКТ

	• Описва последователността на събитията от наличните данни (например от лог файл) • Идентифицира липсваща информация в непълен доклад • Попълва формуляр по образец с примерни данни • Съхранява документация в съответствие с изискванията за достъп и конфиденциалност • Работи с електронни шаблони и платформи за инцидентна отчетност
Компетентности	• Поддържа точна и пълна документация за събития, свързани с киберинциденти • Осигурява проследимост на действията и комуникацията по време на инцидента • Следва вътрешноустановените изисквания за отчетност
Резултат от учене 14.2	Съставя доклад и докладва за инцидент на работно ниво
Знания	• Познава формата и стила на служебен доклад и инцидентна бележка • Изброява езиковите и административните правила при съставяне на официален текст (обективност, хронология, без предположения) • Описва ролята на отчета като юридически и одитен документ • Познава примерни сценарии на технически инциденти, изискващи доклад • Разграничава докладване по вътрешен канал (тикет, e-mail, платформа) от външно уведомяване (например към Комисията за защита на личните данни, КЗЛД, Национална агенция за приходите – НАП, Комисия за регулиране на съобщенията – КРС, както и към определените специфични органи по компетенция) • Изброява лицата и длъжностите, до които се адресира докладът според критичността • Описва формата на обратната връзка след подаден доклад
Умения	• Съставя кратък доклад за инцидент по зададен шаблон • Използва точен език, последователност и пълнота при описание на инцидента • Прилага стандартни формати и формулировки за сигурност • Проверява доклада за пропуски и неясноти • Обобщава информация от няколко източника (логове, свидетелства, съобщения) • Придържа се към зададен обем и ниво на поверителност • Попълва техническа част от доклада с подкрепа от старши специалист, ако е необходимо
Компетентности	• Съставя точни и полезни документи в рамките на собствената си компетентност • Поддържа комуникационна отчетност с колеги и ръководство • Допринася за анализа и подобряването на мерките по сигурността чрез документиране
Резултат от учене 14.3	Извършва анализ на инциденти и прилага високотехнологични решения за обработка на информация
Знания	• Обяснява какво представлява анализа след възникнал инцидент и значението на „научени уроци“ (lessons learned)

ПРОЕКТ

	• Познава структурата и предназначението на финален/ аналитичен доклад • Изброява приложенията на дигитални инструменти, включително ИИ, за обобщение, класифициране и визуализиране на инцидентна информация • Обяснява правилата за човешка проверка и валидиране на резултатите, генерирани от ИИ • Разграничава допустимите от недопустимите автоматизирани действия при обработка на служебна документация • Описва принципите за защита на лични и чувствителни данни при работа с ИИ и други автоматизирани средства
Умения	• Извлича релевантна информация от доклади, логове и формуляри за инциденти, самостоятелно или с помощта на ИИ инструмент • Съставя и структурира основна част от аналитичен текст или таблица с ключови моменти с или без използване на автоматизирани средства • Прилага указания за редактиране, коригиране и валидиране на предложен текст от ИИ при подготовка на отчет • Включва идентифицирани пропуски или препоръки към организационните процедури, като анализира информацията директно или с подкрепяща автоматизация • Представя последователно хронология на събитията чрез прости средства – таблици, списъци, времеви линии, въз основа на логическо разсъждение и/или ИИ обработка • Съдейства при подготовка на финална презентация или обобщение на инцидента, включително визуални средства, създадени със софтуерна помощ
Компетентности	• Способен е да участва в анализа и докладването на инциденти, като използва дигитални инструменти самостоятелно или с помощта на ИИ, според зададените процедури • Спазва стандартите за качество, достоверност и поверителност при документиране независимо от използваната технология • Поддържа отчетност и допринася за организационното учене чрез смесено прилагане на човешки преценки и технологични средства
Критерии за оценяване на ЕРУ	Част по теория на професията: • Описва дейността по документиране и докладване на инциденти чрез попълване на формуляри, водене на дневници, съставяне на служебни доклади и участие в анализа на причините и последствията след инцидента • Дефинира правилата, указанията и изискванията за съставяне на инцидентни документи, включително възможността за използване на дигитални инструменти и изкуствен интелект при спазване на стандартите за точност и поверителност • Подчертава примерни тактически указания за създаване на отчети и формуляри за инциденти, както и мерки за подобряване на процеса чрез анализ на предходни събития Част по практика на професията:

ПРОЕКТ

	• Обяснява дейността по съставяне на инцидентен доклад, включително събиране, структуриране и представяне на информация за настъпило събитие, с или без помощта на ИИ • Различава правилата, указанията и изискванията при работа с документи за инциденти – вътрешни формуляри, финални отчети, доклади за анализ, включително автоматизирани шаблони • Дава примери за прилагане на документиране на реални или симулирани инциденти, включително участие в обобщаване чрез ИИ платформи или електронни системи за сигурност
Средства за оценяване	Част по теория на професията: • Писмен изпит Част по практика на професията: • Изпълнение на практическа задача по индивидуално задание по практика
ЕРУ 15	**Прилагане на политики и стандарти за сигурност**
Резултат от учене 15.1	Познава приложимите политики, законови и стандартни изисквания в киберсигурността
Знания	• Изброява основните нормативни документи и стандарти: Закон за киберсигурност (ЗКС), Регламент (ЕС) 2016/679 (GDPR), ISO/IEC 27001, както и всички актуални регламенти на ЕС в сферата на киберсигурността • Дефинира понятието „политика за сигурност“ и нейните компоненти: цели, обхват, роли, мерки, отчетност • Разграничава нива на сигурност и поверителност според типа данни (обикновени, чувствителни, класифицирани и др.) • Познава правата и задълженията на служителите при работа с лични данни • Обяснява ролята на длъжности, като DPO (отговорник по защита на данните), CISO (отговорник по информационна сигурност) • Изброява санкции при неспазване на изискванията за защита на данни • Познава термини, като „съответствие“, „инцидент с лични данни“, „регулаторен одит“, „отчетност“
Умения	• Разпознава политики и процедури за сигурност, приложими в своята организация • Идентифицира кои данни подлежат на защита по Общия регламент относно защита на данните/ General Data Protection Regulation– GDPR, както и може да етикетира видовете информация • Спазва правила за събиране, съхранение и предаване на лични данни • Разграничава правилното и неправилното поведение спрямо вътрешната политика • Работи със служебни документи и софтуерни платформи според зададени инструкции за поверителност • Съблюдава условията за достъп до различни информационни ресурси според класификацията • Следи срокове за отчетност, архивиране или унищожаване на документи

ПРОЕКТ

Компетентности	• Работи в съответствие с приетите в организацията стандарти, регулации и вътрешни правила • Изпълнява задълженията си в съответствие с принципа на законосъобразността • Поддържа поведение, гарантиращо защита на поверителността и сигурността на информацията
Резултат от учене 15.2	Прилага политики за информационна сигурност при изпълнение на конкретни задачи
Знания	• Изброява типични елементи на вътрешна политика по сигурността: контрол на достъп, работа с преносими носители, криптиране, докладване на инциденти • Познава процедурите при приемане и напускане на служител (nbarding/ffbarding), аспектите, свързани с киберсигурността • Описва практики за сигурно поведение – заключване на екрана, смяна на пароли, забрана за споделяне на акаунти • Разграничава нивата на санкциониране при нарушаване на вътрешните политики • Дефинира термини, като „минимален достъп“, „декларация за поверителност“, „задължение за съобщаване“ • Познава политиките за отдалечена работа и защита при използване на лични устройства (BYOD) • Изброява основни мерки за физическа сигурност на работното място
Умения	• Спазва процедурите за оторизиран достъп до системи и помещения • Докладва при установено отклонение от политиката – загуба на носител, нарушен достъп, неразрешен обмен • Прилага инструкции за поведение при обработка на служебна информация • Използва защита на екран, парола, двуфакторна автентикация • Използва правилно шифровани носители и преносими устройства • Следи за неоторизирана активност и я докладва • Участва във вътрешни проверки и обучения по сигурността
Компетентности	• Прилага на практика изискванията от вътрешните политики по сигурността • Поддържа отчетност за достъпа и обработката на чувствителна информация • Демонстрира отговорно поведение, съответстващо на ролята му в организационната структура
Резултат от учене 15.3	Подпомага процеса по поддържане на съответствие и участие в одити и проверки
Знания	• Обяснява какво е „съответствие със стандарт“ и ролята му за организационната сигурност • Изброява действията, които подлежат на проверка при вътрешен или външен одит (достъп, документи, докладване) • Дефинира понятията „регистър на обработванията“, „лог файл“, „одитна следа“ • Познава основните моменти в политиката за запазване на данни

ПРОЕКТ

	• Изброява права и задължения на служителя при вътрешна проверка • Познава етапите на подготовка за сертификация по стандарт (IS/IEC 27001) и как той може да бъде приложен при внедряване на рамки за киберсигурност • Обяснява необходимостта от обучение и периодично преглеждане на политики
Умения	• Поддържа точна и пълна документация за действия, които извършва в системи или при достъп до данни • Съдейства на проверяващ екип, предоставяйки информация по заявка • Участва в попълване на регистри и формуляри, свързани със сигурността • Събира и структурира доказателства при одит – отчети, e-mail, журнали • Работи с шаблони за самооценка на съответствие • Спазва срокове и инструкции при подготвителни дейности за проверка • Допринася с предложения за подобрение, установени чрез реална практика
Компетентности	• Осигурява проследимост на действията си в контекста на изискванията за съответствие • Подпомага екипа по сигурността чрез точна, навременна и проверима информация • Поддържа нагласа за подобряване на вътрешните процеси и култура на съответствие
Критерии за оценяване на ЕРУ	Част по теория на професията: • Обяснява целта и структурата на политиките за сигурност в организационен контекст • Разграничава основни нормативни и стандартни изисквания в киберсигурността • Дефинира ключови понятия, като „съответствие“, „инцидент с лични данни“, „одитна следа“ Част по практика на професията: • Прилага правила за защита на лични и чувствителни данни при изпълнение на конкретна задача • Докладва инцидент или отклонение от вътрешна политика чрез зададена процедура • Съдейства в симулирана проверка или одит, като попълва и представя необходимата документация
Средства за оценяване	Част по теория на професията: • Писмен изпит Част по практика на професията: • Изпълнение на практическа задача по индивидуално практическо задание
ЕРУ 16	**Стратегическо управление на киберсигурността**
Резултат от учене 16.1	Разработва стратегия за киберсигурност, базирана на анализ на вътрешната и външната среда

ПРОЕКТ

Знания	• Обяснява какво представлява стратегическото управление и каква е неговата роля за ефективната защита на информационните активи на една организация • Познава съдържанието и основните принципи на международните стандарти, като ISO/IEC 27001 (стандарт за управление на информационната сигурност) и NIST Cybersecurity Framework (рамка, използвана за идентифициране и управление на рисковете) • Разяснява как се извършва стратегически анализ на средата чрез инструменти, като SWOT анализ (идентифициране на силни и слаби страни, възможности и заплахи) и PESTLE анализ (оценка на политически, икономически, социални, технологични, правни и екологични фактори) • Може да дефинира кои активи в една организация са критични за нейната сигурност – например сървъри, клиентски бази данни или електронни комуникации
Умения	• Провежда SWOT и PESTLE анализи, като събира и анализира информация за външни и вътрешни фактори, влияещи върху сигурността • Формулира стратегически цели, които са в съответствие с мисията и приоритетите на организацията • Идентифицира и анализира заинтересованите страни (ръководство, служители, клиенти, регулатори) и техните очаквания спрямо сигурността • Използва графики, диаграми и логически карти, за да визуализира елементите на стратегията
Компетентности	• Способен е самостоятелно да предложи структура на стратегически документ за киберсигурност • Разполага с умения да адаптира стратегията към спецификите на организацията • Работи ефективно с други отдели за интегриране на стратегическите цели в цялостната дейност на институцията
Резултат от учене 16.2	Определя показатели и измерва ефективността на стратегията за сигурност
Знания	• Обяснява значението на ключови индикатори за изпълнение (KPIs – Key Performance Indicators) – това са измерими стойности, които показват до каква степен се постигат поставените цели • Познава ключовите индикатори за риск (KRIs – Key Risk Indicators) – те дават информация за потенциални заплахи и възможност за тяхното ранно идентифициране • Знае какво включва цикълът на стратегическо управление – планиране, изпълнение, мониторинг и подобрение
Умения	• Определя показатели (KPIs и KRIs), които са приложими към конкретна ситуация или тип организация • Създава формат (шаблон) за отчет, чрез който да се следи напредъка по изпълнение на стратегията • Прилага принципа SMART при формулиране на цели – т.е. целите трябва да бъдат конкретни, измерими, постижими, релевантни и времево обвързани

ПРОЕКТ

Компетентности	• Способен е да наблюдава изпълнението на стратегията чрез измерими данни • Разпознава отклонения от очакваното и предлага конкретни мерки за корекция • Подготвя периодични отчети, които представя пред ръководството или заинтересовани страни
Резултат от учене 16.3	Разработва план за непрекъсваемост на дейността и възстановяване след инциденти
Знания	• Обяснява какво представляват план за непрекъсваемост на бизнеса (BCP – Business Continuity Plan) и план за възстановяване след инцидент (DRP – Disaster Recovery Plan) • Знае как се прави анализ на въздействието върху бизнеса (BIA – Business Impact Analysis) – анализ, който определя кои процеси са критични и какво ще струва тяхното прекъсване • Разграничава два ключови параметъра: • Целено време за възстановяване RTO (Recovery Time Objective) – максималният допустим период (максималното време), за който даден процес, система или услуга трябва да бъдат възстановени след инцидент, за да се избегнат значителни загуби • Целева точка за възстановяване RPO (Recovery Point Objective) – максималният допустим период, за който данни могат да бъдат загубени поради инцидент, без да се компрометират критичните бизнес процеси
Умения	• Провежда BIA (Анализ за въздействие върху бизнеса), като оценява кои процеси са най-критични за организацията • Определя разумни граници за възстановяване (RTO, RPO) в зависимост от риска и възможностите на организацията • Създава и тества планове за действия при аварийни ситуации • Използва сценарии и симулации за проверка на ефективността на плановете
Компетентности	• Участва в изготвяне и поддържане на реални BCP/DRP документи • Интегрира плановете в стратегическата рамка на организацията • Осигурява практическа готовност за възстановяване след срив или инцидент
Критерии за оценяване на ЕРУ	Част по теория на професията: • Обяснява връзката между стратегия, показатели и устойчивост • Дефинира и прилага понятия, като KPI, KRI, BIA, RTO, RPO • Разпознава приложимостта на международни стандарти и аналитични модели Част по практика на професията: • Изготвя примерна стратегия за информационна сигурност • Извършва SWOT анализ по зададен казус • Разработва бизнес план за възстановяване при зададен инцидент • Представя индикатори за мониторинг и оценка на изпълнение на стратегия

ПРОЕКТ

Средства за оценяване	Част по теория на професията: • Писмен изпит Част по практика на професията: • Изпълнение на практическа задача по индивидуално задание по практика
ЕРУ 17	**Ръководство и развитие на екипи по киберсигурност**
Резултат от учене 17.1	Анализира ролевите профили и необходимите компетенции в екипи по киберсигурност
Знания	• Познава основните ролеви профили, определени в Европейската рамка за умения в областта на киберсигурността (ECSF) – например анализатор в SOC, специалист по реагиране при инциденти, ръководител на екип, специалист по риск • Разграничава технически, поведенчески и управленски компетенции, необходими за различните роли • Познава принципите на компетентностния модел и как той се използва при изграждане на организационна структура
Умения	• Идентифицира конкретни компетенции и квалификации за различни длъжности в екипа • Изготвя профили на длъжности и описания на роли, базирани на реални организационни нужди • Използва рамки за съответствие между изискванията на длъжност и профила на кандидата
Компетентности	• Самостоятелно анализира нуждите от човешки ресурс и препоръчва конкретни мерки за попълване на екипа • Оценява пригодността на кандидатите спрямо нуждите на екипа по сигурност
Резултат от учене 17.2	Организира процеса по подбор и въвеждане на персонал
Знания	• Познава различни методи за подбор: интервюта, технически тестове, казуси, поведенчески интервюта (STAR методика) • Анализира етичните и регулаторните изисквания при подбор на персонала, включително свързани със защита на лични данни и поверителност • Познава логиката и структурата на процеса на въвеждане на нови служители
Умения	• Подготвя и провежда интервюта с фокус върху техническа, поведенческа и културна пригодност • Изготвя критерии за оценка на кандидатите, съобразени с нуждите на организацията • Организира въвеждащи обучения и наставничество за нови членове на екипа
Компетентности	• Ръководи процеса по набиране и адаптация на нови служители по сигурността • Осигурява плавен преход от кандидатстване към ефективна работа в екипа
Резултат от учене 17.3	Прилага мотивационни и лидерски подходи в работата на екипа
Знания	• Познава различни мотивационни теории (например Маслоу, Херцберг, Deci & Ryan) и тяхното значение в ИТ екипи • Различава стилове на ръководство – авторитарен, демократичен, коучинг, ситуационен и тяхната приложимост

ПРОЕКТ

	• Разбира факторите, водещи до професионално изтощение (burnout), и механизмите за превенция
Умения	• Използва подходящ лидерски стил според ситуацията, характеристиките на екипа и контекста • Прилага методи за подкрепа на служители при стрес или високо натоварване • Организира индивидуални и екипни срещи за обратна връзка и насърчаване на ангажираност
Компетентности	• Създава положителна екипна култура, насърчаваща сътрудничество, доверие и откритост • Прилага стратегии за задържане на кадри и устойчиво развитие на екипа
Критерии за оценяване на ЕРУ	Част по теория на професията: • Обяснява значението на ролевите профили и как те подпомагат управлението на човешките ресурси • Дефинира лидерски стилове, мотивационни подходи и рискове за изтощение • Познава стъпките за организиране на вътрешно обучение Част по практика на професията: • Изготвя длъжностна характеристика на роля в киберсигурността • Провежда интервю по сценарий и оценява кандидат • Създава мини план за обучение по тема от сферата на сигурността • Анализира казус с демотивация в екипа и предлага коригиращи действия
Средства за оценяване	Част по теория на професията: • Писмен изпит Част по практика на професията: • Изпълнение на практическа задача по индивидуално задание по практика
ЕРУ 18	**Тактическа реакция и управление при киберинциденти**
Резултат от учене 18.1	Анализира заплахи и избира тактически подходи за реагиране при киберинциденти
Знания	• Обяснява фазите на жизнения цикъл на реагиране при инциденти – включително идентификация, изолация, ограничаване, елиминиране, възстановяване и последващ анализ – като прилага рамки и стандарти • Познава различните типове киберинциденти – включително атаки чрез фишинг, зловреден софтуер, отказ от услуга (DDoS), пробиви в бази данни и вътрешни заплахи – и тяхното въздействие върху сигурността на организацията • Разграничава тактически подходи според нивото на критичност на инцидента и чувствителността на засегнатите активи, включително сценарии за „бързо ограничаване“ (containment) и стратегическо изолиране на системи

ПРОЕКТ

Умения	• Извършва първоначална оценка на ситуацията по ключови индикатори за инцидент (Indicators of Compromise – IoCs), включително анализ на логове, алармени сигнали и подозрителна мрежова активност • Прилага подходящ модел за реагиране според типа инцидент и наличните ресурси, като взема предвид приоритизирането на бизнес процеси и критични активи • Документира последователността на действията и проследимостта на събитията в хронологичен и аналитичен формат, подходящ за вътрешен анализ и външен одит
Компетентности	• Способен е да избира, прилага и адаптира тактически модели за реагиране на базата на конкретната оперативна среда и наличната информация, като гарантира минимално въздействие върху бизнес процесите • Демонстрира аналитична устойчивост при работа под напрежение и взема решения, съобразени с правната рамка, вътрешните политики и принципите на защита на данните • Владее способността да комуникира тактическите стъпки и рисковете, свързани с инцидента, както към технически екипи, така и към управленски и нетехнически аудитории
Резултат от учене 18.2	Инструктира и координира действията на екипа по време на инцидент
Знания	• Определя структурата и ролите в екипи за реагиране на инциденти (CSIRT/SOC) – включително оператори от първо ниво, анализатори, координатори и външни участници • Разбира процедурите за активиране на предварително разработени сценарии за реагиране (playbooks), както и алгоритмите за ескалация на инциденти при промяна в степента на критичност • Познава добри практики за оперативна комуникация, включително използване на тикетинг системи, сигурни комуникационни канали и разпределение на роли по време на инцидент
Умения	• Провежда брифинг и инструктаж за членовете на екипа с ясно дефинирани задачи и стъпки за действие • Осигурява координация между различни екипи и отдели (например ИТ, право, комуникации), участващи в инцидентния отговор • Поддържа актуален запис на предприетите действия, използваните инструменти и резултатите от реакцията в реално време
Компетентности	• Ръководи ефективно действията на многопрофилен екип при критичен инцидент, като съчетава тактическо мислене, лидерство и прецизност при разпределяне на отговорности • Осигурява съгласуваност на действията със стратегическите цели на организацията, включително запазване на репутацията, в съответствие с нормативната рамка и ограничаване на щетите • Демонстрира способност за ясна и уверена комуникация в реално време с всички участници в процеса – както вътрешни, така и външни, включително регулатори или партньори

ПРОЕКТ

Резултат от учене 18.3	Участва в анализ след инцидента и разработване на коригиращи действия
Знания	• Разбира значението на Post-Incident Analysis (PIA) и етапа „lessons learned“ като ключови за повишаване на организационната устойчивост • Познава шаблони за докладване на инциденти, включително задължителните елементи: описание на събитието, засегнати активи, предприети действия, въздействие, изводи и препоръки • Познава методи за извършване на анализ на коренната причина (root cause analysis – RCA) с цел идентифициране на системни слабости и предложения за ефективни мерки за предотвратяване на бъдещи инциденти
Умения	• Изготвя детайлен доклад за инцидента, в който анализира ефективността на предприетите действия и оценява възможностите за подобрение • Провежда екипна среща за анализ и рефлексия след инцидента, като събира мнения, сравнява версии и установява различия • Идентифицира повтарящи се пропуски или недостатъци в техническата и организационната инфраструктура и ги обвързва с конкретни предложения за оптимизация
Компетентности	• Демонстрира способност да управлява завършения цикъл на инцидента – от реакцията до анализа и прилагането на коригиращи действия, като гарантира затворена обратна връзка в процеса • Предлага адекватни и устойчиви решения за подобряване на процедурите и технологиите, които надграждат реакцията при бъдещи инциденти • Осигурява ангажираност на екипа и ръководството към превенцията чрез стратегически препоръки и култура на учене от реални събития
Критерии за оценяване на ЕРУ	Част по теория на професията: • Обяснява фазите на инцидентния отговор и тяхната логическа връзка • Описва различни типове инциденти и съответните тактически подходи за реагиране • Познава структурата на доклад за инцидент и основните принципи на „lessons learned“ Част по практика на професията: • Избира подходящ тактически подход при симулиран инцидентен сценарий • Ръководи симулация по реагиране – провежда инструктаж, записва действия, подготвя кратък план • Изготвя писмен доклад със SWOT анализ на реално или симулирано инцидентно събитие и препоръки за подобрение
Средства за оценяване	Част по теория на професията: • Писмен изпит Част по практика на професията: • Изпълнение на практическа задача по индивидуално задание по практика
ЕРУ 19	**Регулаторна и етична отговорност в киберсигурността**

ПРОЕКТ

Резултат от учене 19.1	Прилага нормативната рамка за защита на лични и чувствителни данни
Знания	• Обяснява основните принципи и задължения, свързани с Общия регламент относно защита на данните (GDPR), включително понятия като „администратор“, „обработващ данни“, „право на забравяне“ и „преносимост на данни“ • Познава Закона за киберсигурност (ЗКС) в България и неговото съответствие с Директива NIS2 *(директива за сигурност на мрежите и информационните системи2???)* и Регламент (ЕС) 2022/2554 (DORA) относно оперативна устойчивост на цифровите технологии във финансовия сектор, както и други актуални директиви на ЕС или регламенти • Познава стандарта ISO/IEC 27701, който предоставя разширение към ISO/IEC 27001 с фокус върху поверителността и управлението на лични данни.
Умения	• Идентифицира ситуации, в които се обработват лични и чувствителни данни, и прилага адекватни технически и организационни мерки за тяхната защита • Извършва преценка на законовите основания за обработка на данни – например информирано съгласие, договорно задължение, легитимен интерес • Класифицира данни и процедури по ниво на чувствителност и изисквания за защита
Компетентности	• Способен е да приложи точно конкретни нормативни изисквания към различни професионални ситуации, свързани със съхранение, трансфер и обработка на данни • Демонстрира разбиране за баланса между оперативната нужда от данни и правата на субектите на данни, като защитава интересите на организацията и същевременно гарантира съответствие със закона • Прилага етични принципи при работа с лична информация, като демонстрира отговорност, уважение към поверителността и отчетността
Резултат от учене 19.2	Разработва вътрешни политики, процедури и етични кодекси
Знания	• Познава структурата на вътрешни нормативни актове: политика за поверителност, политика за достъп, кодекс за етично поведение, вътрешна процедура за сигнализиране • Разграничава понятието „съответствие“ (compliance) от „етичност“, като обяснява защо и двете са критично важни за устойчивата киберсигурност • Познава международни насоки и добри практики за изграждане на етична култура (например ENISA Guidelines, ISO Code of Ethics)
Умения	• Изготвя вътрешна политика, съобразена с регулации, като GDPR и NIS 2, включително ясно формулирани отговорности, процедури за достъп и права на служителите • Създава инструкции и формуляри за управление на съгласие, проследимост на достъпа и уведомяване при инциденти • Разработва етичен кодекс, валиден за технически и нетехнически роли, с акцент върху интегритет, конфиденциалност и професионализъм

ПРОЕКТ

Компетентности	• Способен е да разработи правилно цялостна вътрешна рамка за етично и правно съответствие, включително документи, процедури и отговорности • Въвежда механизми, чрез които служителите да разбират, прилагат и следват вътрешните политики по етично поведение • Осигурява съгласуваност между етичните стандарти, културата на организацията и конкретните действия на служителите по сигурността
Резултат от учене 19.3	Оценява съответствието и подготвя документация за одити и контрол
Знания	• Познава етапите на вътрешен и външен одит по сигурността – включително планиране, интервюиране, събиране на доказателства, анализ на несъответствия и изготвяне на доклад • Разбира какво представлява оценка на въздействието върху защитата на данните (DPIA) и кога е задължителна според GDPR • Познава механизмите за вътрешен контрол – checklists, одитни дневници, матрици на съответствие, както и принципите на „двойна отчетност“
Умения	• Провежда вътрешна проверка (self-assessment) на съответствие с определен регламент или стандарт • Съставя доклад от одитна дейност, в който посочва открити несъответствия и препоръчва коригиращи мерки • Изготвя матрица за съответствие с GDPR, ISO или вътрешен етичен кодекс, включваща отговорности, срокове и контролни механизми
Компетентности	• Осигурява устойчив процес по самопроверка и корективни действия с цел непрекъснато подобрение на съответствието в организацията • Подготвя документация и представя резултати пред регулаторни органи, като демонстрира професионализъм, прозрачност и ангажираност към спазване на изискванията • Способен е да идентифицира и предотврати етични и правни нарушения, като въвежда ефективни механизми за контрол и сигнализиране
Критерии за оценяване на ЕРУ	Част по теория на професията: • Обяснява основни принципи и задължения по Общия регламент относно защита на данните – GDPR, Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета – Директива МИС2, Регламент (ЕС) 2022/2554 (DORA) относно оперативна устойчивост на цифровите технологии във финансовия сектор – DORA, Закона за киберсигурност – ЗКС • Разграничава понятията „етика“, „съответствие“, „политика“, „процедура“ • Дефинира структурата на вътрешна политика и обосновава нуждата от Оценка на въздействието върху защитата на данните (Data Protection Impact Assessment – DPIA) Част по практика на професията: • Изготвя вътрешна политика по сигурност или поверителност • Съставя формуляр за оценка на въздействието върху защитата на данните или план за етично обучение

ПРОЕКТ

	• Провежда казусно упражнение по откриване и докладване на несъответствие • Подготвя доклад за съответствие или одитна матрица
Средства за оценяване	Част по теория на професията: • Писмен изпит Част по практика на професията: • Изпълнение на практическа задача по индивидуално задание по практика
ЕРУ 20	**Технологична архитектура и иновации в киберсигурността**
Резултат от учене 20.1	Оценява и внедрява нови технологии в контекста на киберсигурността
Знания	• Познава съвременните технологични парадигми, използвани в областта на сигурността, включително Zero Trust Architecture, Security as a Service, XDR (Extended Detection and Response) и SOAR (Security Orchestration, Automation and Response) • Разграничава възможностите и рисковете при използване на изкуствен интелект и машинно самообучение в защитни системи – например при откриване на аномалии, автоматизирана реакция или разпознаване на поведенчески модели • Познава концепцията за „compliance automation“ – т.е. използване на технологии за автоматично проследяване и съответствие със стандарти, като GDPR, ISO 27001 и ЕС МИС
Умения	• Извършва предварителна оценка на риска и въздействието при въвеждане на нова технология в съществуваща ИТ инфраструктура • Интегрира механизми за наблюдение, отчетност и проследимост в нови технологични решения • Използва инструменти за threat intelligence и анализ на сигнали от различни източници (логове, SIEM, UEBA платформи)
Компетентности	• Прилага структуриран подход за избор, внедряване и контрол на технологии с критично значение за информационната сигурност, включително чрез автоматизирани платформи и стандартизирани методологии • Демонстрира информираност и адаптивност към технологичните тенденции, като предлага уместни и устойчиви иновации, съобразени със спецификата на организацията • Взема самостоятелни решения относно пригодността на дадена технология за нуждите на сигурността, балансирайки между ефективност, съвместимост и съответствие
Резултат от учене 20.2	Проектира и управлява архитектури за сигурност на цифрова инфраструктура
Знания	• Разбира принципите на модулна и слоеста архитектура на сигурността – включително логическо разделяне, сегментация на мрежи, защита на периметър и вътрешни зони • Познава методите за управление на идентичност и достъп (IAM), включително политики за минимални привилегии, многофакторна автентикация и самостоятелно администриране

ПРОЕКТ

	• Познава техническите средства за физическа сигурност – видеонаблюдение, контрол на физически достъп, защита на сървърни помещения – и тяхната интеграция със системите за информационна сигурност
Умения	• Извършва оценка на съществуваща ИТ архитектура, като идентифицира уязвими точки и липса на интеграция между елементи на сигурността • Проектира архитектура, която комбинира мрежова защита, управление на достъп, мониторинг и отчетност, в съответствие с приетите стандарти • Конфигурира логически и физически контролни механизми (например SIEM системи, контрол на достъпа, защита по дизайн)
Компетентности	• Управлява целия жизнен цикъл на технологичната архитектура по сигурност – от планиране и внедряване до поддръжка и оценка • Координира усилията между различни екипи (ИТ, охрана, ръководство) за изграждане на цялостна система за защита, която обединява хора, технологии и политики • Предлага архитектурни решения, базирани на бизнес нужди, регулаторни изисквания и анализ на технологичен риск, включително за облачна, хибридна или критична инфраструктура
Резултат от учене 20.3	Управлява внедряването и устойчивото развитие на иновации в сигурността
Знания	• Познава фазите на иновационния цикъл – от идентифициране на нужда, пилотно тестване, оценка на ефективността до мащабиране и поддръжка • Обяснява същността на моделите за цифрова зрялост (Digital Maturity Models) и как се използват за планиране на технологична трансформация в организацията • Познава принципите на управление на промяната, включително управление на съпротивата, ангажиране на заинтересовани страни и въвеждане на иновации с минимален риск • Познава стандартите и насоките, свързани с технологично управление, като ISO/IEC 42001 (AI Governance), ENISA препоръки и други
Умения	• Разработва стратегия за внедряване на нова технология, съобразена с нуждите на организацията, наличния капацитет и регулаторните ограничения • Провежда анализ на разходи и ползи (cost-benefit analysis) при избор на иновационно решение в областта на киберсигурността • Планира дейности за наблюдение, поддръжка и усъвършенстване на вече внедрената технология • Организира обучения и комуникационни дейности, свързани с приемането и използването на нови решения в екипа или организацията

ПРОЕКТ

Компетентности	• Способен е да ръководи процеса на технологично обновление в организацията, като осигурява съгласуваност между иновациите, сигурността и бизнес целите • Демонстрира способност да взема обосновани решения за внедряване на иновации, базирани на количествени и качествени анализи • Създава среда на адаптивност и устойчивост чрез систематично развитие на технологичния капацитет на организацията, включително управление на технологични партньори, доставчици и жизнения цикъл на решенията
Критерии за оценяване на ЕРУ	Част по теория на професията: • Обяснява основни принципи и подходи за изграждане на технологични архитектури в киберсигурността с фокус върху структурираност, проследимост и устойчивост • Познава възможностите и ограниченията на съвременни технологии и иновации, използвани за защита на информационни системи и активи • Анализира ролята на архитектурните и технологичните решения за постигане на стратегически цели, свързани със сигурността и съответствието Част по практика на професията: • Извършва цялостна оценка на технологична среда с оглед на сигурността, наличните механизми и потенциални рискове • Проектира концептуална архитектура или предлага конкретно решение за технологично обновление, съобразено с нуждите на организацията • Изготвя план или доклад за внедряване, оценка или подобрение на технологично решение с ясна логика и структура
Средства за оценяване	Част по теория на професията: • Писмен изпит Част по практика на професията: • Изпълнение на практическа задача по индивидуално задание по практика

4. Съвкупност от единици резултати от учене, които формират придобиването на квалификация по част от професията „Киберсигурност“.

Степен на професионална квалификация	Ниво по ЕКР/НКР	ЕРУ № …от списъка по т. 3.1. (мин. 3 броя ЕРУ, поне 1 ЕРУ е от специфичната ПП)
III	4	ЕРУ 6, ЕРУ 9, ЕРУ 10, ЕРУ 3, ЕРУ 4; ЕРУ 6, ЕРУ 8, ЕРУ 15, ЕРУ 5; ЕРУ 10, ЕРУ 11, ЕРУ 13, ЕРУ 3, ЕРУ 5; ЕРУ 5, ЕРУ 7, ЕРУ 10, ЕРУ 14; ЕРУ 6, ЕРУ 9, ЕРУ 12, ЕРУ 3; ЕРУ 3, ЕРУ 5, ЕРУ 6, ЕРУ 4; ЕРУ 4, ЕРУ 5, ЕРУ 15, ЕРУ 3; ЕРУ 5, ЕРУ 7, ЕРУ 14, ЕРУ 15;
IV	5	Неприложимо

5. Изисквания към материалната база

ПРОЕКТ

5.1. Изисквания към кабинетите за обучение по теория на професията – характеристики, обзавеждане, оборудване, софтуер

Обучението по теория на професията „Киберсигурност“ се провежда в учебни кабинети и зали, оборудвани с необходимата електронна, компютърна и мрежова техника, осигуряваща ефективен достъп до учебни ресурси и симулирана среда за обучение.

Учебната среда трябва да предоставя възможност за индивидуална и групова работа, както и за представяне, анализ и визуализация на сложни информационни структури, процеси и архитектури за сигурност.

Основното оборудване и обзавеждане включва:

- учебни маси и столове, съобразени с броя обучаеми;
- бяла дъска или флипчарт за водене на бележки и демонстрации;
- шкафове или стелажи за съхранение на учебни материали и технически средства;
- работно място за всеки обучаван с индивидуален компютър, мишка, клавиатура и слушалки;
- стабилна връзка с интернет с гарантирана скорост и сигурност;
- мултимедийна система (проектор, интерактивна дъска или голям дисплей с аудиовъзпроизвеждане), свързана с преподавателската станция;
- възможност за контролирано споделяне на екрани от преподавателя към учениците и обратно (например чрез локален сървър или специализиран софтуер).

Задължителен софтуер и дигитални ресурси:

- офис пакет (текстообработка, електронни таблици, презентации);
- браузъри и програми за сигурен достъп до интернет;
- обучителни версии на софтуер за киберсигурност, включително:
- Wireshark, Kali Linux, VirtualBox или VMware;
- софтуер за симулация на атаки и защита;
- инструменти за лог анализ и SIEM (например Wazuh, ELK Stack);
- програмни продукти за криптография и дигитална идентичност;
- софтуерни инструменти за управление на политики за достъп и права.

Онагледяване и методическа подкрепа:

- учебни табла, плакати и графични схеми (например OSI модел, структура на SOC, жизнен цикъл на инцидент);
- модулни учебни видеа и демонстрации на реални атаки и защити;

ПРОЕКТ

- интерактивни онлайн ресурси и симулатори;
- локална база с казуси и учебни сценарии.

5.2. Изисквания към учебната база за обучение по практика на професията – характеристики, обзавеждане, оборудване, софтуер

Специализираните учебни бази за провеждане на практическо обучение по професията „Киберсигурност“ включват:

лаборатория по киберсигурност (CyberLab) – учебна зала, предназначена за симулиране на киберзаплахи, инциденти и защита на системи. Лабораторията трябва да разполага със:

- сървъри или виртуални машини за изграждане на контролирана мрежова среда;
- набор от хостове, IDS/IPS, SIEM и защитни стени;
- софтуерни инструменти за мониторинг, анализ, реакция и възстановяване;
- изолирана вътрешна мрежа (sandbox среда), позволяваща безопасно симулиране на атаки;
- техническа възможност за работа с мрежов трафик в реално време и за провеждане на тестове за проникване;
- система за логиране и оценка на действията на обучаемите.

Тренировъчен център за реагиране при инциденти (Cyber Range) – функционално обособено пространство, в което се провеждат практики по сценарии за киберинциденти, включително:

- изградена инфраструктура за симулация на SOC (Security Operations Center);
- обучителна платформа за разпределяне на роли и екипна работа при кризи;
- софтуер за симулации на атаки и защити (например purple team платформи);
- система за проследяване на реакциите на екипите с цел анализ и самооценка.

Партньорски учебни среди в реална или виртуална среда – бази, осигурени чрез сътрудничество с организации от сектора на ИТ и киберсигурността, в които обучаемите могат да прилагат своите знания в практическа обстановка:

- облачни инфраструктури (CloudLabs) за упражняване на сигурност в облачна среда;
- специализирани среди за управление на уязвимости и оценки на риска;
- достъп до тренировъчни платформи, като TryHackMe, Hack The Box и др.

6. Изисквания към обучаващите

Право да преподават по теория и практика на професията имат лица с висше образование и образователно-квалификационна степен „магистър“ или „бакалавър“ по

ПРОЕКТ

специалности от професионални направления „Национална сигурност“ и „Военно дело“ от областта на висше образование „Сигурност и отбрана“, от професионални направления „Право“, „Психология“, „Обществени комуникации и информационни науки“, „Администрация и управление“ от областта на висше образование „Социални, стопански и правни науки“, от професионални направления „Информатика и компютърни науки“ и „Математика“ от областта на висше образование „Природни науки, математика и информатика“, от професионални направления „Електротехника, електроника и автоматика“, „Комуникационна и компютърна техника“, „Транспорт, корабоплаване и авиация“ от областта на висше образование „Технически науки“, както и всички специалности по киберсигурност, информационна сигурност, комуникационна сигурност или сигурност на мрежи и системи, които попадат в посочените направления от Класификатора на областите на висше образование и професионалните направления, приет с Постановление № 125 от 2002 г. на Министерския съвет (ДВ, бр. 64 от 2002 г.), съответстващи на професията.

Учителска длъжност по учебен предмет или модул от професионалната подготовка може да се заема и от лица със завършено висше образование по съответната специалност и без професионална квалификация „учител“.

По учебен предмет или модул от професионалната подготовка, за който няма съответно професионално направление в Класификатора на областите на висше образование и професионалните направления, могат да преподават лица без висше образование и без придобита професионална квалификация „учител“, ако са придобили съответната професионална квалификация при условията и по реда на Закона за професионалното образование и обучение.

Препоръчително е на всеки три години обучаващите да преминават курс за актуализиране на професионалните си знания, умения и компетентности.

Списък на използваните съкращения

I. Съкращения на български език

ДЗИ – Държавни зрелостни изпити

ЕКР – Европейска квалификационна рамка

ЕРУ – Единица резултат от ученето

ЗБУТ – Здравословни и безопасни условия на труд

ЗЗЛД – Закон за защита на личните данни

ЗКС – Закон за киберсигурност

ИИ – Изкуствен интелект

ИТ – Информационни технологии

ПРОЕКТ

КЗЛД – Комисия за защита на личните данни

КРС – Комисия за регулиране на съобщенията

НАП – Национална агенция за приходите

НК – Наказателен кодекс

НКР – Национална квалификационна рамка

ПП – Професионална подготовка

СПК – Степен на професионална квалификация

СППОО – Списък на професиите за професионално образование и обучение

II. Съкращения на английски език

ABAC – Attribute-Based Access Control

AES – Advanced Encryption Standard

AI – Artificial Intelligence

BCP – Business Continuity Plan

BIA – Business Impact Analysis

BIOS – Basic Input/Output System

UEFI – Unified Extensible Firmware Interface

BYOD – Bring Your Own Device

CA – Certificate Authority

CIRT – Computer Incident Response Team

CISO – Chief Information Security Officer

CSIRT – Computer Security Incident Response Team

DDoS – Distributed Denial of Service

DNS – Domain Name System

DORA – Digital Operational Resilience Act

DoS – Denial of Service

DPIA – Data Protection Impact Assessment

DPO – Data Protection Officer

DRP – Disaster Recovery Plan

ECSF – European Cybersecurity Skills Framework

ELK – Elasticsearch, Logstash, Kibana

FTP – File Transfer Protocol

FTPS – File Transfer Protocol Secure

GDPR – General Data Protection Regulation

GPG – GNU Privacy Guard

HDD – Hard Disk Drive

ПРОЕКТ

HTTP – Hypertext Transfer Protocol

HTTPS – Hypertext Transfer Protocol Secure

IAM – Identity and Access Management

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

IEC – International Electrotechnical Commission

IoC – Indicators of Compromise

IoS – Internet of Services

IP – Internet Protocol

ISO – International Organization for Standardization

KPI – Key Performance Indicator

KRI – Key Risk Indicator

LAN – Local Area Network

LUKS – Linux Unified Key Setup

MFA – Multi-Factor Authentication

NAT – Network Address Translation

NIST – National Institute of Standards and Technology

NIST SP – National Institute of Standards and Technology Special Publication

OTP – One Time Password

PESTLE – Political, Economic, Social, Technological, Legal, Environmental

PGP – Pretty Good Privacy

PIA – Post-Incident Analysis

PIN – Personal Identification Number

PKI – Public Key Infrastructure

RBAC – Role-Based Access Control

RCA – Root Cause Analysis

RFID – Radio Frequency Identification

RPO – Recovery Point Objective

RSA – Rivest-Shamir-Adleman

RTO – Recovery Time Objective

S/MIME – Secure/Multipurpose Internet Mail Extensions

SFTP – SSH File Transfer Protocol

SFTP – Secure File Transfer Protocol

SHA – Secure Hash Algorithm

SIEM – Security Information and Event Management

PROJEKT

SMART – Specific, Measurable, Achievable, Relevant, Time-bound

SMS – Short Message Service

SMTP – Simple Mail Transfer Protocol

SOAR – Security Orchestration, Automation and Response

SOC – Security Operations Centre

SSH – Secure Shell

SSL – Secure Sockets Layer

STAR – Situation, Task, Action, Result

SWOT – Strengths, Weaknesses, Opportunities, Threats

TCP – Transmission Control Protocol

TLS – Transport Layer Security

UEBA – User and Entity Behavior Analytics

UEFI – Unified Extensible Firmware Interface

URL – Uniform Resource Locator

USB – Universal Serial Bus

VPN – Virtual Private Network

Wi-Fi – Wireless Fidelity

XDR – Extended Detection and Response

ПРОЕКТ