2\_OUTLINE\_Intro\_Jud\_Course---COMPARE

Сесија за информирање на учесниците за напорите на Советот на Европа во градењето капацитети за сајбер-криминал преку неколку нивни проекти, како што е iPROCEEDS-2.

3\_1.4 Computer & Internet Basics---COMPARE

(онлајн верзија)

Шема на компонентите на компјутерски систем

Куќиште, напојување, процесор, RAM-меморија, графичка картичка, хард-диск, мрежна картичка, податочни кабли за податоци и други поврзувања

Од кое од наведеното е најверојатно да очекуваме да повратиме корисни електронски докази создадени од осомничен?

Мрежна картичка во лаптоп

Процесор во мобилен уред

Хард-диск во лаптоп

Графичка картичка во десктоп компјутер

Точен одговор е В.

Хард-дискот е главниот уред за складирање на датотеки во компјутер или лаптоп и затоа е најверојатно да содржи електронски докази.

Мрежните картички, процесори и графички картички веројатно нема да дадат нешто што е корисно.

Проверка на знаење

Интернетот е пример за каков тип на мрежа?

Мрежа со комутирани струјни кола (circuit-switched network)

Надземна транспортна мрежа

Друштвена мрежа

Мрежа со комутирање на пакети (packet-switched network)

Точен одговор е Г.

Интернетот е мрежа со комутирање на пакети каде податоците се делат на пакети и истите можат да одат по различни патеки до крајната дестинација.

Мрежа со комутирање на струјни кола бара континуиран проток на податоци

Што би бил најдобриот опис

за вашиот лаптоп кога се приклучува на мрежа во вашиот дом?

Приватна IP адреса

Фиксна IP адреса

Динамичка IP адреса

Јавна IP адреса

Точен одговор е А.

Домашна мрежа нормално се контролира од рутер кој доделува IP адреси од приватен опсег.

Рутерот ќе има јавна IP адреса што сите внатрешни уреди ќе ја користат за пристап на интернет.

Фиксна и динамична се поими што важат за јавните IP адреси.

Проверка на знаење

HTML се користи за структурирање на веб-страници што можат да се прегледуваат преку веб-прегледувач (пребарувач).

Што значи HTML?

Hidden Text Meaning Language

Hypertext Mark-up Language

Hi-speed Transfer Metadata Language

Hardware Transportation Media Language

Точен одговор е Б.

Hyper Text Markup Language овозможува да се создадат структурирани делови, текстуални пасус, заглавја и линкови за веб-страница што потоа веб-прегледувач може да ја прочита и прикаже.

Проверка на знаење

Која од овие апликации ќе ви овозможи да пребарувате датотеки (files) што другите мрежни корисници ги споделуваат, како и да ги симнете?

Peer-to-Peer мрежа

Voice over IP мрежа

Internet Relay Chat

Апликација за онлајн игри

Точен одговор е А.

Peer-to-Peer мрежите им овозможуваат на корисниците да понудат датотеки за споделување и корисниците можат да ги пребаруваат датотеките по име, тип, уметник или автор.

Многу илегални датотеки се присутни на мрежата.

Истото може да важи и за IRC, но во многу помал степен.

Проверка на знаење

Што од наведеното би било точно кога се опишува криптовалута?

Глобална е - нема граници

Децентрализирана е - не е контролирано од влада

Непостојана е - вредноста може да варира во голема мера

Сѐ од горенаведеното

Точен одговор е Г.

Криптовалутите може да ги преминуваат меѓународните граници, што ги прави корисни за криминалците во движење, кои кријат пари.

Ниту една банка или влада не управува со валутата.

Нејзината вредност може да се менува брзо и со голема нестабилност.

5\_1.5 Cybercrime Basics---COMPARE

Сајбер-криминал и студии на случај

Давање вовед за претставниците за информатичкото општество и сајбер-криминалот, како и идентификување на меѓународните организации и нивните напори за справување со овој модерен вид на криминал

Давање основни дефиниции за сајбер-криминал, разгледување на Конвенцијата од Будимпешта на Советот на Европа и дефинирање на современи форми на сајбер-криминал

Проблемот со сите овие?

Сајбер-војна - меѓународната трка во вооружување сега се одвива повеќе онлајн отколку офлајн.

Сајбер-војната е употреба на технологија за напад врз одредена нација, предизвикувајќи штета што може да се спореди со вистинска војна.

Постојат многу поими што се користат кога се зборува за сајбер-криминал:

Компјутерски криминал, сајбер-криминал, хај-тек или високотехнолошки криминал, интернет криминал, ИТ криминал, технолошки криминал

тоа збунува и може погрешно да ве наведе!

Во животот на полициските и обвинителските служби

Меѓународните јавни организации и приватните компании имаат сѐ поголема загриженост во однос на последиците од незаконските и штетни дела извршени со помош на комуникациските мрежи или во рамките на тие мрежи.

Проверка на знаење

Што од наведеното може да се вклучи во описот на сајбер-криминал?

Кога технологијата содржи податоци поврзани со кривично дело

Каде што комуникацијата преку е-пошта се користи во кривичното дело

Кога еден компјутерот е нападнат од друг компјутер

Сѐ од горенаведеното

Точен одговор е Г.

Иако е тешко да се најде вистинска дефиниција за сајбер-криминалот, сите описи може да се искористат како дел од сајбер-криминал - заедно со можеби помагање на кривично дело или сведочење на исто.

Пристап на Советот на Европа

Конвенцијата од Будимпешта за сајбер-криминал и поврзаните стандарди

В. Рамка и заштитни мерки за постојните практики за проширување на прекуграничните претреси

Контактните точки се активни посредници со задача да ја олеснат правосудната соработка помеѓу земјите членки

Обучувачот треба да го посети сајтот пред презентација за да добие чувство за оваа организација

Обучувачот треба да го посети сајтот пред презентацијата за да добие чувство за оваа организација

Истата вклучува

Борба против сајбер-криминалот

Другите даватели на содржини вообичаено го користат.

Пробивање во веб-сервер

Самостојна замена на хостиран веб-сајт

Придвижување од т.н. *fiat*-валути како целни кон криптовалути и оние со големи средства во криптовалути

Проверка на знаење

Ако на вашиот компјутер имало штетен софтвер (malware) и истиот ги енкриптирал сите ваши датотеки - може да се де-енкриптираат само со плаќање на одредена сума пари - како би го опишале она што го имате на компјутерот?

Trojan (тројанец)

Ransomware (софтвер за откуп)

Ботнет

Лоша среќа

Точен одговор е Б.

Ransomware-от, кога е присутен ги енкриптира датотеките, а клучот за деенкриптирање може да се добие со плаќање ‘откуп (ransom)’ во криптовалута.

www.coe.int/cybercrime

Изработка и дистрибуција на видеа и слики

Малолетните лице активни на друштвените мрежи укажуваат на поголем број потенцијални жртви

Помага сѐ поголемата јавна свест

Генерално се јавува на обичниот (отворениот) веб, друштвените мрежи и онлајн игрите

Откако ќе се оствари контакт, дејството се движи

кон енкриптирани пораки преку интернет

Споделувањето може да се изврши:

(Може да се прошири и на други што води до принуда или изнуда)

Закани со постоен материјали за да се добие нов

Сексуална експлоатација на деца - иднината

Многу закани се веќе доста втемелени и стабилни

Импликации при докажување на автентичноста за органите за спроведување на законот

Иако технологијата е сè уште релативно нова, истата брзо се подобрува и станува подостапна и полесна за употреба.

Можеби е прашање на време кога ќе се појават првите *deepfakes* (високо квалитетни лажни слики/видеа) што прикажуваат онлајн CSE, што пак ќе резултира во генерирање на нов „персонализиран“ CSEM.

Главни приоритети на истражителите при измама

Трансакциите преку интернет еволуираат и растат

Потекнуваат од компромитирање на податоците, повреди поврзани со податоците од трети страни, текстуални пораки за *phishing* и измама

Информациите за чип-картичката се копираат

Картичката со магнетна лента е создадена од информацијата

Се користи во продавници кои сè уште ја користат таа технологија

Го експлоатира начинот на кој компаниите ги вршат деловните активности

Останува клучна област за трговијата со криминални производи и услуги

Валутата на Dark Web останува виртуелна

Ширење низ повеќе јурисдикции (судски надлежности)

Вклучувајќи форуми, страници за споделување датотеки, *pastebins* (веб-сајтови за чување текст), страници за пренос на видеa, услуги за скратување на URL-називите, блогови, апликации за испраќање пораки, платформи за пренос во живо, веб-страници на друштвените мрежи, услуги за хостирање

Проверка на знаење

Која криптовалута е најраспространета во рамки на DarkWeb?

Monero

Dash

Bitcoin

Zcoi

Точен одговор е В.

Биткоинот е сè уште најраспространет, но сигурно не е единствениот.

Многу други сега се развиваат и ќе продолжат да се користат предизвикувајќи проблеми за органите за спроведување на законот во истрагите на кривични дела и дистрибуцијата на парични средства.

6\_1.6 Lesson Plan (Online)---COMPARE

(Преглед - онлајн верзија)

* Пристап до софтверот/платформата за онлајн конференции.
* Прожектор и платно.
* Пристап до интернет.
* Бележници и пенкала за учесниците

Се препорачува покрај овој план за лекции и слајдовите, обучувачот да го проучи и извештајот за T-CY, [**Конвенцијата од Будимпешта за сајбер-криминал: практични придобивки и влијаниe**](https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac), бидејќи е важен дел од оваа сесија. Доколку има дополнителен интерес за тоа како земјите имаат корист од Конвенцијата од Будимпешта, обучувачот може да сподели кој било релевантен дел од извештајот со претставниците за време на сесијата за прашања и одговори.

Важни слајдови

7\_1.6 The Budapest Convention---COMPARE

Опфат (делокруг)

Меѓународна соработка:

Екстрадиција

ЗПП/MLA

Спонтано информирање

Експедитивно барање за зачувување

Експедитивно откривање на податочен сообраќај

ЗПП за пристап

Прекуграничен пристап

ЗПП за податочен сообраќај во реално време (RT TD)

ЗПП за следење

247 контакт точки

Опфат (делокруг)

Меѓународна соработка:

Екстрадиција

ЗПП/MLA

Спонтано информирање

Експедитивно барање за зачувување

Експедитивно откривање на податочен сообраќај

ЗПП за пристап

Прекуграничен пристап

ЗПП за податочен сообраќај во реално време (RT TD)

ЗПП за следење

247

Мрежа 247

Пристап на Советот на Европа

Конвенцијата од Будимпешта за сајбер-криминал и поврзаните стандарди

GLACY+ - EUCOE Заеднички проект за глобална акција против сајбер-криминалот -

CyberEast – EUCOE Источно партнерство -

iPROCEEDS-2 – EUCOE Борба против приносите од кривични дела остварени преку Интернет -

CyberSouth – EUCOE Заеднички проект за сајбер-криминал и електронски докази -

Области на земјите учеснички

Специјализирани услуги, како и меѓу-агенциска и јавно-приватна соработка

Модели на ITU (ICT4PACSADCHIPCAR модели на закони)

Основи на

Договорот за сајбер-криминал

Овластувања (процесни истражни мерки во врска со сајбер-криминалот)

Заштита на граѓанските слободи и човековите права (процесни услови и заштитни мерки)

Оперативна [247 контакт точка]

Модел закон на Комонвелтот

и инструментот за соработка од Хараре

Слајдот покажува дека инструментот за соработка од Хараре содржи кривични дела и процесни истражни мерки во врска со сајбер-криминалот

Слајдот покажува дека инструментот за соработка од Хараре содржи кривични дела и процесни истражни мерки во врска со сајбер-криминалот

Меѓународна димензија

на сајбер-криминалот

Точен одговор е ѓ) Сѐ од горенаведеното

Меѓународна димензија

на сајбер-криминалот

Точен одговор е б) Сајбер-безбедност и г) Национална безбедност

https:\\www.coe.int\en\webcybercrime-the-budapest-convention-on-cybercrime-in-operation-new-t-cy-report

Подобрување на домашните законодавства

Конвенцијата од Будимпешта имаше значително влијание врз усогласување на законодавството

Ова влијание се чувствува и кај страните потписнички и кај останатите

Другите држави со закони/нацрт-закони во голема мера се во согласност со Конвенцијата од Будимпешта = 20

Од 30 јуни

2020

Подобрување на домашните законодавства

Донесените домашни одредби одговараат на одредбите од материјалното право во Конвенцијата од Будимпешта

Донесените домашни одредби одговараат на одредбите од процесното право во Конвенцијата од Будимпешта

Постои зголемување на вкупниот број истраги за сајбер-криминал што ги спроведуваат страните

Ова првенствено се должи на

Подобрувањето на домашните законодавства

Достапност на функционална

меѓународна соработка

Влијанија

Обемно користење на 247 мрежите

Градење на капацитети

Советот на Европа обезбедува техничка помош за подобрување на законодавството во многу земји

Канцеларијата за програма за сајбер-криминал (C-PROC) има поддржано повеќе од 1000 активности

6 тековни проекти

Промовирање на јавно-приватната соработка

Области на земјите учеснички

Специјализирани услуги, како и меѓу-агенциска и јавно-приватна соработка

http:\\www.coe.intt\cy

http:\\www.coe.int\en\webcybercrime-stagingglacy

Меѓународна димензија

на сајбер-криминалот

Точен одговор е б) Конвенцијата од Будимпешта има 65 страни.

Обучувачот може да објасни дека Конвенцијата од Будимпешта имала влијание врз повеќе од 150 земји - бидејќи служи како упатство за законодавството во многу земји.

Меѓународна димензија

на сајбер-криминалот

Точен одговор е б) Конвенцијата од Будимпешта има 65 страни.

Обучувачот може да објасни дека Конвенцијата од Будимпешта имала влијание врз повеќе од 150 земји - бидејќи служи како упатство за законодавството во многу земји.

РЕАЛНОСТА Е КАКО ШТО СЛЕДИ

Заканите за корисниците на Интернет, техничките легални алатки за истраги и гонење на сајбер-криминал се идентични во сите земји

Конвенцијата од Будимпешта ги фаворизира земјите со инфраструктура

Конвенцијата од Будимпешта обезбедува поголема придобивка за земјите во развој и им дава можност на овие земји да упатуваат правно обврзувачки барања до земјите со развиена инфраструктура (кои во најголем дел се сите членки на Конвенцијата од Будимпешта).

Предрасуди налог јавност

Компјутерски системи

Ботнет мрежи

Прекуграничен пристап

Кражба на идентитет

DDOS напади

Напади на критичната инфраструктура

Штетен софтвер (malware)

Спам

Манипулација на изборниот процес

Налози за генерирање информации за претплатници

Тероризам

Компјутерски системи

Ботнет мрежи

Прекуграничен пристап

Кражба на идентитет

DDOS напади

Напади на критичната инфраструктура

Штетен софтвер (malware)

Спам

Манипулација на изборниот процес

Налози за генерирање информации за претплатници

Тероризам

Меѓународна димензија

на сајбер-криминалот

Точен одговор е ѓ) Сѐ од горенаведеното

Меѓународна димензија

на сајбер-криминалот

Точен одговор е ѓ) Сѐ од горенаведеното

9\_2.1 Digital & Electronic Evidence---COMPARE

Генерирани од корисник - документи, фотографии, итн.

Генерирани од уред - истории, логови

10\_Session 2.2 Lesson Plan Online)---VOMPARE

(онлајн верзија)

* Пристап до софтверот/платформата за онлајн конференции.
* Пристап до интернет.
* Бележници и пенкала за учесниците

Пред презентирањето на оваа сесија, се препорачува обучувачот да ги разгледа ставовите 22 – 78 од Извештајот за објаснување на конвенцијата за сајбер-криминал.

Овој дел завршува со две анкетни прашања.

14 до 26

Задолжителни слајдови

11\_2.2 Substantive Provisions of BC---COMPARE

Сесија 2.2

Оваа сесија трае 90 минути

„компјутерски систем“ значи кој било уред или група меѓусебно поврзани или сродни уреди, од кои еден или повеќе, согласно одредена програма, врши автоматска обработка на податоците;

„компјутерски податоци“ значи какво било презентирање на факти, информации или концепти во форма соодветна за обработка во компјутерски систем, вклучувајќи и програма соодветна да причини компјутерски систем да извршува одредена функција;

Да

комуникација или поврзани услуги за обработка на податоци (на пр. даватели на услуги за хостинг и кеширање)

приватни и јавни субјекти

бесплатни или платени услуги

одредба за затворена група или јавноста

Не

даватели на услуги за содржини

Анкетно прашање

Што од наведеното НЕ е вклучено во податочниот сообраќај:

Време

Времетраење

Содржина

Наслов на предметот

Обем на комуникацијата

Точните одговори се В и Г.

Точен одговор е: в) содржина и г) наслов на предметот (ова се содржински податоци)

Анкетно прашање

Што од наведеното НЕ е вклучено во информации за претплатникот:

Адреса

Содржина

E-mail адреса

Информации за кредитни картички

Број на мобилен телефон

Точен одговор е Б

Точен одговор е: б) содржина (ова се содржински податоци)

Пред да преминеме на интернет, треба да дадеме малку перспектива за тоа што е мрежа и што ја сочинува истата - што е важно за да се обезбеди разбирање за тоа како функционира интернетот

Анкетно прашање

Ако вработен е овластен да пристапува до банкарски податоци, дали може да биде обвинет за илегален пристап доколку вработениот пристапи до податоците за да помогне во извршување на кривично дело?

ДА

НЕ

Точен одговор е А

Точен одговор е: а) Да.

Ова е затоа што овластувањето кое обично му се дава на вработен не дозволува пристап со цел извршување на кривично дело.

Вработениот на тој начин би постапил над овластувањето, пристапувајќи до компјутерот за да изврши кривично дело.

Илегално следење („следење (interception)“)

Секоја страна ќе донесе такви законски и други мерки што се потребни за утврдување на кривични дела според сопственото домашно законодавство, кога е намерно сторено следење без право на тоа, со помош на технички средства, на пренос на компјутерски податоци недостапен за јавноста до, од или во рамките на компјутерски систем, вклучувајќи електромагнетни емисии од компјутерски систем што носи такви компјутерски податоци.

Страната може да побара делото да биде извршено со нечесна намера или во врска со компјутерски систем што е поврзан со друг компјутерски систем.

Секоја страна ќе донесе такви законски и други мерки што се потребни за утврдување на кривични дела според сопственото домашно законодавство, кога е намерно сторено следење без право на тоа, со помош на технички средства, на пренос на компјутерски податоци недостапен за јавноста до, од или во рамките на компјутерски систем, вклучувајќи електромагнетни емисии од компјутерски систем што носи такви компјутерски податоци.

Страната може да побара делото да биде извршено со нечесна намера или во врска со компјутерски систем што е поврзан со друг компјутерски систем.

На левата страна, овој слајд го покажува текстот на член 3 од Конвенцијата од Будимпешта со еден нагласен елемент („до, од или во рамките на компјутерски систем“).

На десната страна, овој слајд дава објаснување за нагласениот елемент.

Следењето на преноси до, од или во рамки на компјутерски систем е криминализирано.

Овој слајд дава примери кои го објаснуваат опфатот на член 3 во врска со ова, како и разликата помеѓу овие три елементи.

Илегално следење („електромагнетни емисии“)

Страната може да го задржи правото да бара однесувањето опишано во став 1 да резултира во сериозна штета.

Оштетувањето и влошувањето се акти кои се преклопуваат по значење

Истите се однесуваат на негативната промена на интегритетот или информациската содржина на податоците и програмите

Секоја страна ќе донесе такви законодавни и други мерки што може да бидат потребни за да се утврди како кривично дело според сопственото домашно законодавство, кога е намерно сторено: оштетување, бришење, влошување, промена или потиснување на компјутерски податоци без право на тоа.

Страната може да го задржи правото да бара однесувањето опишано во став 1 да резултира во сериозна штета.

Страната може да го задржи правото да бара однесувањето опишано во став 1 да резултира во сериозна штета.

Промената се однесува на модификација на постојните податоци

Вклучува внесување на штетен код, како што се вируси и тројанци и резултат е модификација на податоците

Манипулација со податоците („потиснување“)

Анкетно прашање

Ако вработен е овластен да пристапува до банкарски податоци и ако вработениот пристапи до податоците за да помогне при извршување на кривично дело со пренесување на податоците до неговиот соучесник, за кое дело(а) ќе биде обвинет вработениот?

Илегален пристап

Илегално следење

Манипулација со податоците

Точни одговори се А и В

Точен одговор е: а) илегален пристап и в) манипулација со податоците.

Ова е затоа што вработениот мора да пристапи до податоците што е над овластувањето - што пак претставува кривично дело илегален пристап, а потоа да ги внесе податоците во компјутерскиот систем на соучесникот без овластување - што претставува кривично дело манипулација со податоците.

Попречувањето е акција што го попречува правилното функционирање на компјутерскиот систем

Попречувањето мора да се одвива преку:

Внесување

Пренесување

Оштетување

Бришење

Изменување

Потиснување

на компјутерските податоци

Анкетно прашање

Одредено лице набавува за употреба уред за тестирање на пенетрација, проектиран да овозможи пристап до компјутер без овластување.

Лицето има намера да го искористи за да спроведе овластено тестирање на компјутерски систем.

Дали ова е кривично дело според член 6 од Конвенцијата од Будимпешта?

ДА

НЕ

Точен одговор е Б

Точен одговор е: б) Не. Набавката на уред што е проектиран да овозможи пристап до компјутер без овластување е кривично дело само ако се набави со намера да се изврши кривично дело според Конвенцијата од Будимпешта.

Во овој случај, лицето го набавува уредот заради овластено тестирање на компјутерски систем, а не со намера да го користи за извршување на кривично дело.

Оттаму, ова не е кривично дело според член 6 од Конвенцијата од Будимпешта.

12\_Session 2.3 Lesson Plan (Online)---COMPARE

(онлајн верзија)

* Персонален компјутер/лаптоп опремен со софтверски верзии компатибилни со подготвените материјали
* Пристап до софтверот/платформата за онлајн конференции.
* Пристап до интернет.
* Бележници и пенкала за учесниците

Пред презентирањето на оваа сесија, се препорачува обучувачот да ги разгледа ставовите 79 – 127 од Извештајот за објаснување на конвенцијата за сајбер-криминал.

Овој дел завршува со едно анкетно прашање.

13\_2.3 Substantive Provisions of BC 1---COMPARE

Анкетно прашање

Точен одговор е: б) Не. Ова е затоа што член 8 од Конвенцијата од Будимпешта бара конкретна измама или нечесна намера за да се оствари економска корист за себе.

Анкетно прашање

Точен одговор е: б) Не. Ова е затоа што член 8 од Конвенцијата од Будимпешта бара конкретна измама или нечесна намера за да се оствари економска корист за себе.

Анкетно прашање

Точен одговор е: б) Не, ова е затоа што член 9 од Конвенцијата од Будимпешта опфаќа само визуелни прикази.

Анкетно прашање

Точен одговор е: б) Не, ова е затоа што член 9 од Конвенцијата од Будимпешта опфаќа само визуелни прикази.

14\_Session 2.4 Lesson Plan (Online)---COMPARE

* Интернет пристап (доколку е достапен)
* PowerPoint или друг софтвер за презентации

Пред презентирањето на оваа сесија, се препорачува обучувачот да ги разгледа ставовите 131 – 183 од **Извештајот за објаснување на конвенцијата за сајбер-криминал**. Овој дел завршува со две анкетни прашања.

48 до 49

Важни слајдови

15\_2.4 Procedural Powers under the BC---COMPARE

Анкетно прашање

Точен одговор е: а) Да - ако се вклучени електронски докази.

Ова е заради опфатот на процесните одредби согласно член 14 од Конвенцијата од Будимпешта го опфаќа собирањето електронски докази за истрага на сите кривични дела.

Анкетно прашање

Точен одговор е: а) Да - ако се вклучени електронски докази.

Ова е заради опфатот на процесните одредби согласно член 14 од Конвенцијата од Будимпешта го опфаќа собирањето електронски докази за истрага на сите кривични дела.

Анкетно прашање

Точен одговор е: а) Да - ако се вклучени електронски докази.

Ова е заради опфатот на процесните одредби согласно член 14 од Конвенцијата од Будимпешта го опфаќа собирањето електронски докази за истрага на сите кривични дела.

Анкетно прашање

Точен одговор е: а) Да - ако се вклучени електронски докази.

Ова е заради опфатот на процесните одредби согласно член 14 од Конвенцијата од Будимпешта го опфаќа собирањето електронски докази за истрага на сите кривични дела.

Анкетно прашање

Точен одговор е: а) Да - ако се вклучени електронски докази.

Ова е заради опфатот на процесните одредби согласно член 14 од Конвенцијата од Будимпешта го опфаќа собирањето електронски докази за истрага на сите кривични дела.

Анкетно прашање

Зачувувањето без одобрение од судија или магистрат е честопати потребно бидејќи ова овластување треба да се користи експедитивно за да се обезбеди зачувување на податоците што се ранливи на загуба или измена и за да се зачува нивниот интегритет.

Анкетно прашање

Точен одговор е: б) Не - Ова е така затоа што Конвенцијата од Будимпешта бара користење на овластувањето според член 18 да се однесува на наведените компјутерски податоци и не може да биде за недефинирани или неодредени компјутерски податоци.

Овластувањата мора да се користат во согласност со начелото на пропорционалност.

Анкетно прашање

Точен одговор е: б) Не - Ова е така затоа што Конвенцијата од Будимпешта бара користење на овластувањето според член 18 да се однесува на наведените компјутерски податоци и не може да биде за недефинирани или неодредени компјутерски податоци.

Овластувањата мора да се користат во согласност со начелото на пропорционалност.

16\_Session 2.5 Lesson Plan (Online)---COMPARE

- онлајн верзија)

* Пристап до софтверот/платформата за онлајн конференции.
* Пристап до интернет.
* Бележници и пенкала за учесниците

Пред презентирањето на оваа сесија, се препорачува обучувачот да ги разгледа ставовите 184 – 239 од **Извештајот за објаснување на конвенцијата за сајбер-криминал**.

Овој дел завршува со две анкетни прашања.

17\_2.5 Procedural Powers under the BC 1---COMPARE

Анкетно прашање

Обвинител бара налог за претрес и заплена по иста основа и праг како што претходно направил за налог за генерирање информации.

Дали налогот треба да се одобри?

ДА

НЕ

Точниот одговор е Б (прагот за претрес и заплена е повисок од налогот за генерирање информации, бидејќи се работи за поинтрузивно овластување)

Точен одговор е: б) Не - прагот за претрес и заплена е повисок од налогот за генерирање информации, бидејќи се работи за поинтрузивно овластување во споредба со налогот за генерирање информации

Анкетно прашање

Обвинител бара налог претрес на сите електронски уреди во сите објекти што ги поседува обвинетиот.

Дали налогот треба да се одобри?

ДА

НЕ

Точен одговор е Б (овластувањето за претрес може да се примени само во однос на определени компјутери)

Точен одговор е: в) Не - овластувањето за претрес може да се примени само во однос на определени компјутери.

Анкетно прашање

Добивате барање за издавање налог за следење за случај поврзан со кражба.

Делото предвидува максимална казна затвор во траење од 6 месеци.

Дали ова би била валидна употреба на овластувањата за следење според Конвенцијата од Будимпешта?

ДА

НЕ

Точен одговор е Б (следењето на содржински податоци може да се примени само во врска со сериозни кривични дела)

Точен одговор е: в) Не - овластувањето за претрес може да се примени само во однос на определени компјутери.

19\_3.x\_Basic Concepts on International Cooperation---COMPARE

Меѓународна димензија

на сајбер-криминалот

За што е основа Меморандумот за разбирање?

Задолжителна соработка?

Доброволна соработка со законски мандат?

Доброволна соработка без законски мандат?

Точен одговор е Б

б.)

Меѓународна димензија

на сајбер-криминалот

Договорот за заемна правна помош се однесува на:

формална соработка помеѓу две или повеќе земји?

формална соработка помеѓу две или повеќе компании?

формална соработка помеѓу два или повеќе органи?

Точен одговор е А

а.)

Меѓународна димензија

на сајбер-криминалот

Во итни околности, барањата може да се направат преку е-пошта.

точно

неточно

Точен одговор е А

а.)

Меѓународна димензија

на сајбер-криминалот

Може ли барањето за зачувување да биде одбиено?

Без никаква причина, бидејќи тоа е дискреционо право на замолената страна.

Само во ограничен број случаи, засновано на конкретни причини.

Точен одговор е Б

б.)

Пристап или налог за испраќање

на содржината од е-поштата од

сервер на ISP (давател на интернет услуги) во земја Б

E–mail акаунт

Содржина на е-пошта на сервер

на ISP во земја Б

Меѓународна димензија

на сајбер-криминалот

Земја А може да пристапи до податоците зачувани во земја Б:

врз основа на надлежноста на органот.

врз основа на меѓународната надмоќ.

врз основа на согласност на сопственикот на податоците.

Точен одговор е В.

в.)

21\_3.x Overview of Cybercrime Investigation---COMPARE

Воведен курс за правосудна обука за сајбер-криминал и електронски докази

Совет на Европа

email

ДД месец ГГГГ

mailto:matteo.lucchetti@coe.int

Содржина на сесијата

Цели на сесијата

Преглед на истрага за сајбер-криминал

Прашање 1: Дали имате органи за сајбер-криминал во вашата земја?

Прашање 2: Дали се специјализирани или редовни?

Прашање 3: Кои се нивните надлежности?

Прашање 4: Кои се нивните капацитети?

Прашање 5: Како соработуваат?

Органи за борба против сајбер-криминал

Специјализирани или редовни

Органи за борба против сајбер-криминал

Надлежности

Капацитети на органите за сајбер-криминал

Во однос на организацијата:

органите за спроведување на законот имаат доволно службеници, помошен персонал и други човечки и технички ресурси?

обвинителството има доволно обвинители, советници и помошници, како и други ресурси?

судската комора/одделение има на располагање доволно судии, помошници и други ресурси?

надлежните државни/владини/правосудни надзорни органи се подготвени да ги поддржат нивните активности?

Меѓународна димензија

на сајбер-криминалот

Дали во вашата земја имате специјализирани органи за сајбер-криминал на сите нивоа?

ДА

НЕ

Соработка

Преглед на истрага за сајбер-криминал

Основни концепти на

истрагата за сајбер-криминал

Основни концепти на

истрагата за сајбер-криминал

Основни концепти на

истрагата за сајбер-криминал

Основни концепти на

истрагата за сајбер-криминал

е подготвено да донесе одлука за неопходните процесни дејствија и, доколку тоа е потребно, со Судот:

Основни концепти на

истрагата за сајбер-криминал

Меѓународна димензија

на сајбер-криминалот

Во истрагата за сајбер-криминал

постапката може да се преземе навремено и без итност.

точно

неточно

Точен одговор е Б

Трет дел

Преглед на истрага за сајбер-криминал

Србија (страна на Конвенцијата)

Неколку меѓународни

искуства

Преглед на истрага за сајбер-криминал

Меѓународна димензија

на сајбер-криминалот

Вметнете анкетни прашања тука:

Вметни опција

Вметни опција

Вметни опција

Вметнете го точниот одговор

Преглед на истрага за сајбер-криминал

Цели на сесијата

Претставниците треба да се запознаат со она што се очекува

да биде постигнато до крајот на сесијата.