Т Е С Т И
з навчальної дисципліни
«Запобігання кіберзлочинам»

1. Об’єктами кібербезпеки є:

а) конституційні права і свободи людини і громадянина;

б) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

в) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

г) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

д) всі відповіді вірні.

2. Застосування законодавства у сфері кібербезпеки та прийняття суб'єктами владних повноважень рішень на виконання норм Закону здійснюються з додержанням принципів:

а) мінімально необхідного регулювання, згідно з яким рішення (заходи) суб'єктів владних повноважень повинні бути необхідними і мінімально достатніми для досягнення мети і завдань, визначених цим Законом;

б) об'єктивності та правової визначеності, максимально можливого застосування національного та міжнародного права щодо повноважень і обов'язків державних органів, підприємств, установ, організацій, громадян у сфері кібербезпеки;

в) забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, та/або послуг із захисту інформації, кіберзахисту, у тому числі прав щодо невтручання у приватне життя і захисту персональних даних;

г) всі відповіді вірні.

3. Застосування законодавства у сфері кібербезпеки та прийняття суб'єктами владних повноважень рішень на виконання норм цього Закону здійснюються з додержанням принципів:

а) прозорості, згідно з яким рішення (заходи) суб'єктів владних повноважень мають бути належним чином обґрунтовані та повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності (їх застосування);

б) збалансованості вимог та відповідальності, згідно з яким має бути забезпечено баланс між встановленням відповідальності за невиконання вимог кібербезпеки та кіберзахисту, а також за запровадження надмірних вимог та обмежень;

в) еквівалентності вимог до забезпечення кібербезпеки об'єктів критичної інфраструктури, згідно з яким застосування правових норм повинно бути якомога більш рівнозначним щодо кіберзахисту комунікаційних та технологічних систем об'єктів критичної інфраструктури, що належать до одного сектору економіки та/або які здійснюють аналогічні функції.

г) всі відповіді вірні.

4. Індикатори кіберзагроз – це:

а) показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;

б) показники що використовуються для знешкодження кіберзагрози;

в) показники (статистичні дані), що використовуються для обчислення видатків на загрози;

г) показники, що використовуються для обрання мережевого обладнання;

5. Відповідно до чинного законодавства КІБЕРІНЦИДЕНТ це:

а) подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

б) кіберзлочин;

в) віктимна поведінка користувача віртуального простору;

г) адміністративне правопорушення;

6. Відповідно до чинного законодавства КІБЕРЗЛОЧИН (комп'ютерний злочин) це:

а) суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

б) винне діяння у кіберпросторі, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

в) суспільно небезпечне винне діяння з його використанням кіберпростору, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

г) суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена виключно міжнародними договорами України;

7. **Відповідно до чинного законодавства КІБЕРПРОСТІР це:**

а) середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;

б) середовище, яке надає можливості для здійснення комунікацій, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем;

в) середовище (віртуальний простір), утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет;

г) віртуальний простір мережа Інтернет або інша глобальна мережа передачі даних;

8. Яке з наведених визначень найбільш повно відображає властивості понятт КІБЕРРОЗВІДКА визначені чинним закондавством:

а) діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням;

б) діяльність, що здійснюється правоохоронними органами у кіберпросторі або з його використанням;

в) діяльність, що здійснюється органами прокуратури у кіберпросторі або з його використанням;

г) діяльність, що здійснюється хакерами у кіберпросторі або з його використанням;

9. Захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі, це:

а) кібербезпека;

б) кіберзахищенність;

в) захищенність;

г) всі відповіді вірні;

10. Сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії, це:

а) кібероборона;

б) кіберзахищенність;

в) кібербезпека;

г) всі відповіді вірні;

11**. Систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними**

інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів, це:

а) національні електронні інформаційні ресурси (далі - національні інформаційні ресурси);

б) Національна телекомунікаційна мережа;

в) критично важливі об'єкти інфраструктури;

г) система управління технологічними процесами;

12. Подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів, це:

а) інцидент кібербезпеки;

б) кіберзлочин;

в) кібератака;

г) кибершахрайство

13. Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:

а) міністерства та інші центральні органи виконавчої влади;

б) місцеві державні адміністрації;

в) органи місцевого самоврядування;

г) всі відповіді вірні

14. Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, НЕ є:

а) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

б) Збройні Сили України, інші військові формування, утворені відповідно до закону;

в) Національний банк України;

г) Постачальники комунікаційних послуг;

15. Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:

а) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;

б) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

в) органи місцевого самоврядування;

г) всі відповіді вірні;

16. Суб'єкти забезпечення кібербезпеки у межах своєї компетенції є:

а) здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

б) здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

в) здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

г) всі відповіді вірні;

17. Суб'єкти забезпечення кібербезпеки у межах своєї компетенції є:

а) розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

б) забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління;

в) здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.

г) всі відповіді вірні;

18. До об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які:

а) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

б) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я;

в) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;

г) всі відповіді вірні;

19. До об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які:

а) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

б) є об'єктами потенційно небезпечних технологій і виробництв;

в) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;

г) всі відповіді вірні;

20. Забезпечення кібербезпеки в Україні НЕ ґрунтується на принципах:

а) верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;

б) забезпечення національних інтересів України;

в) відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;

г) гуманізму;

21. Забезпечення кібербезпеки в Україні ґрунтується на принципах:

а) державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері;

б) пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;

в) пріоритетності запобіжних заходів;

г) всі відповіді вірні;

22. Забезпечення кібербезпеки в Україні ґрунтується на принципах:

а) верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;

б) невідворотності покарання за вчинення кіберзлочинів;

в) пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

г) всі відповіді вірні;

23. Забезпечення кібербезпеки в Україні ґрунтується на принципах:

а) міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях;

б) забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки.

в) пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;

г) всі відповіді вірні;

24. Функціонування національної системи кібербезпеки забезпечується шляхом:

а) вироблення і оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО;

б) створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО;

в) встановлення обов'язкових вимог інформаційної безпеки об'єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об'єкти критичної інформаційної інфраструктури;

г) всі відповіді вірні

25. Функціонування національної системи кібербезпеки забезпечується шляхом:

а) формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту;

б) залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;

в) проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі;

г) всі відповіді вірні.