Національний університет цивільного захисту України
Кафедра організації та технічного забезпечення аварійно-рятувальних робіт

Методичні вказівки до виконання розрахункової роботи
з дисципліни «Інформаційна безпека у сфері професійної діяльності»

АНАЛІЗ ТА ПРОГНОЗ СТАНУ БЕЗПЕКИ ОБ'ЄКТУ ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

для здобувачів вищої освіти денної та
заочної форми навчання;
освітньо-кваліфікаційного рівня «магістр»
за спеціальністю 261 «Пожежна безпека»,
спеціалізацією «Управління пожежною безпекою»

Укладачі: Борисова Л.В., Собина В.О.

Черкаси, 2024

1. Розрахункове завдання «Аналіз та прогноз стану безпеки об'єкту обчислювальної техніки в умовах надзвичайних ситуацій»

Зміст

Введення

У методичному посібнику надано вказівки до виконання розрахункової роботи з дисципліни «Інформаційна безпека у сфері професійної діяльності».

У роботі передбачається проведення аналізу об'єкту критичної інфраструктури, оцінки ризику для об'єкту, та (або) системи, які підпадають під небезпеку.

Методичні вказівки містять визначення мети роботи та перелік завдань, що розв'язуються, опис завдань на послідовно виконуваних етапах підготовчої самостійної роботи та вимоги до змісту звіту по контрольній роботі.

Методичні вказівки містять:

контрольні питання для самоперевірки;

список рекомендованої літератури по тематиках виконуваних робіт.

Мета роботи та питання, що досліджуються

Мета роботи: аналізу ризиків внаслідок надзвичайних ситуацій для об'єктів обчислювальної техніки з урахуванням динаміки зміни небезпечних подій у часі.

1. Питання, що досліджуються:

1.1. Аналіз та прогноз стану безпеки об'єкту обчислювальної техніки в умовах надзвичайних ситуацій.

1.2. Прогноз стану безпеки об'єкту обчислювальної техніки в умовах надзвичайних ситуацій з урахуванням динаміки зміни небезпечних подій у часі.

2. Рекомендований план виконання розрахункової роботи

2.1. Аналіз об’єкту критичної інфраструктури (за вибором здобувача вищої освіти), формування переліку вихідних даних та вимог.

2.2. Обчислити часткові ризики від подій кожного виду небезпеки.

2.3. Обчислити комбінований ризик.

2.3. Визначити часткові та сумарні функції безпеки та ризику

2.4. Підсумки роботи з оцінкою результатів виконання завдання.

3. Підготовка до розрахункової роботи

Вивчити теоретичний матеріал з рекомендованої літератури з питань, що розглядаються у розрахунковій роботі.

1. Проаналізувати схему нарахування загального ризику (рис.2) відповідно до вибраного об’єкту критичної інфраструктури.
2. Виділити небезпечні події з ймовірними показниками.
3. Проаналізувати і обчислити часткові ризики від подій кожного виду.
4. Обчислити комбінований ризик.
5. Проаналізувати і обчислити динаміку зміни небезпечних подій у часі.
6. Приклад оформлення курсової роботи (по тексту теоретично матеріалу).

4. Вимоги до змісту звіту

1. Завдання на розрахункову роботу (Додаток 1).
2. Опис і результати розрахунків часткових ризиків від подій кожного виду; обчислення комбінованого ризику.
3. Опис і результати розрахунків динаміки зміни небезпечних подій у часі.

4. Контрольні питання для самоперевірки

1. Як називається кількісна характеристика оцінки ступеня небезпеки?
2. Що таке кількісна оцінка ризику?
3. Як поділяються ризики?
4. Яким ефектом супроводжується ризик?
5. Що є показником уразливості об’єкта?
6. Що необхідно з’ясувати для оцінювання ступеня ризику?
7. Як визначаються виправдані ризики?
8. Які рівні ризику є не допустимими?
9. На яких принципах ґрунтується прийняття рішень за результатами аналізу небезпеки й оцінки ризику?

6. Література

1. Качинський А.Б. Засади системного аналізу безпеки складнихсистем / А.Б. Качинський. – К. : ДП «НВЦ «Євроатлантикінформ», 2006. – 336 с.
2. Гавриш О.А., Кавун В.А. Критичний аналіз нормативних засад управління проектними ризиками. Економічний вісник НТУУ «КПІ». 2017. № 14. С. 216–222.

3. Визначення ризику як міри небезпеки потенційно небезпечних об’єктів / В.В. Бєгун // Актуальні проблеми цивільного захисту. Тези VI Всеукраїнської науково-практичної конференції рятувальників. – К., 2004. – С. 23-25.
4. Собина В.О. Аналіз та прогноз стану безпеки об’єкту обчислювальної техніки в умовах надзвичайних ситуацій / В.О. Собина, Л.В. Борисова, О.В. Єлізаров // Проблеми надзвичайних ситуацій: зб. наук. пр. – Вип. 21. – Х. : НУЦЗУ, 2015. – С. 89-96.

Основний текст

Вступ

Загрози інформаційній безпеці розглядаються в органічному зв’язку з питаннями захисту об’єктів критичної інфраструктури, до якої в більшості країн світу відносять інформаційні системи та комп’ютерні мережі системи надзвичайних ситуацій. Процес управління ризиками відповідає міжнародній практиці, основним принципом якої є дотримання життєвого циклу «план – виконання – перевірка – дія» та застосування визнаних галузевих стандартів таких, як BS 25999-1:2006 (Управління безперервністю бізнесом) та ISO/IEC 27001:2005 (Вимоги до системи управління інформаційною безпекою). Одним із найбільш ефективних факторів

Зниження виникнення надзвичайних ситуацій є створення і запровадження нових інформаційних технологій контролю за критичними параметрами технологічних процесів на об’єктах з небезпечною діяльністю на основі широкого використання автоматизованих і комп’ютерних засобів.

Інформація, інформаційний фонд за умов надзвичайної ситуації стає основним ресурсом ефективного прийняття рішень, спрямованих на ліквідацію надзвичайної ситуації.

Кожний конкретний об’єкт є індивідуальним набором параметрів та інформаційних додаткових даних. Ступінь впливу параметрів один на одного різний і визначає швидкість наростання аварійного процесу.

Найбільш уразливим об’єктами забезпечення інформаційної безпеки є системи збору і обробки інформації про можливе виникнення надзвичайних ситуацій і прийняття рішень щодо оперативних дій, пов’язаних із розвитком таких ситуацій і ходом ліквідації їх наслідків.

Кожний параметр в інформаційній базі має:

своє критичне значення, вище якого він переходить в передаварійну область;

свій поріг аварійності;

усі параметри інформаційної бази взаємозалежні, впливаючи один на одного тою чи іншою мірою.

Аналіз ризику здійснюється за схемою: ідентифікація небезпек, моніторинг навколишнього середовища – аналіз (оцінка й прогноз) загрози – аналіз уразливості територій – аналіз ризику надзвичайної ситуації на території – аналіз індивідуального ризику для населення.

З точки зору аналізу ризиків і управління безпекою розрізняють:

індивідуальний ризик,

потенційний територіальний ризик,

соціальний ризик,

колективний ризик (число загиблих і потерпілих у результаті можливих надзвичайних ситуацій),

прийнятний ризик (рівень ризику, з яким суспільство готове примиритися),

неприйнятний ризик,

ризик-рівень індивідуального ризику (не викликає занепокоєння й не приводить до погіршення якості життя населення), яким можна знехтувати.

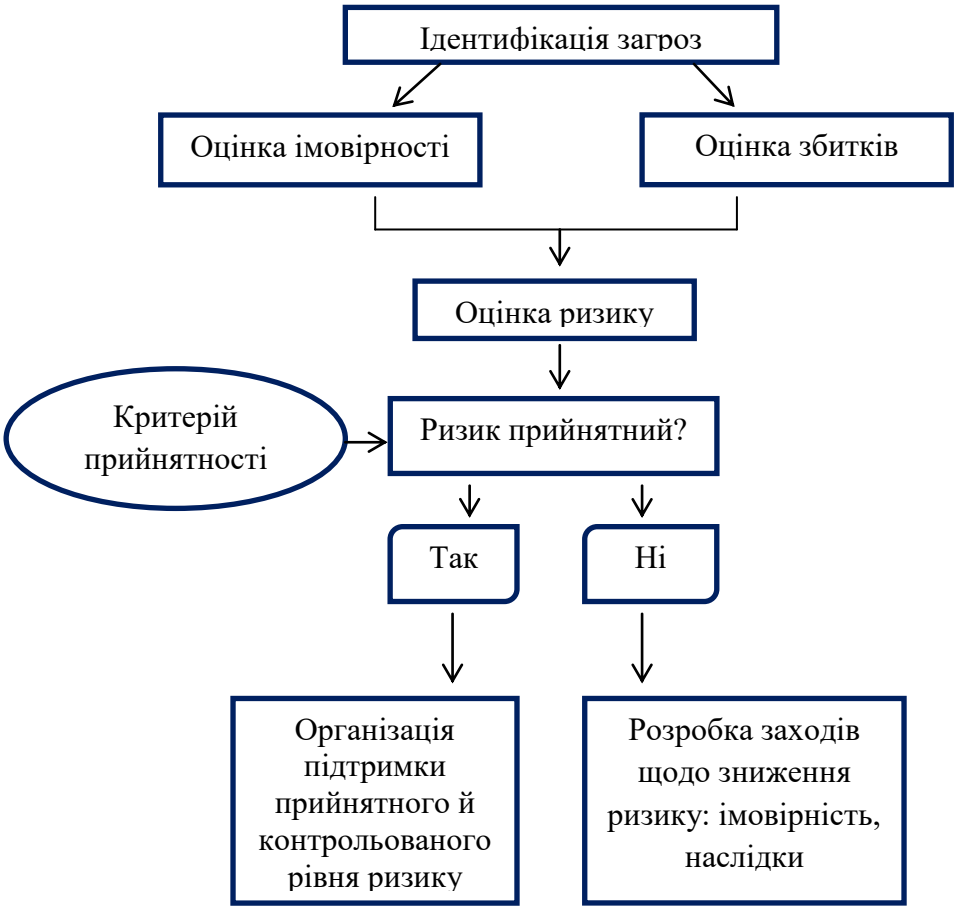

Рисунок 1 – Блок-схема аналізу ризику

Найважливішим елементом аналізу ризику є оцінка ймовірностей і повторюваності несприятливих подій. Для прогнозування НС застосовуються закони розподілу ймовірності Пуассона й статечні розподіли.

Приймемо раніше розроблені методичні апарати аналізу ризиків для обґрунтування рішень і дій посадових осіб за збереження всіх основних якостей інформації – конфіденційності, цілісності та доступності. Модель оцінки

ризику припускає, що за певний проміжок часу середній ризик, спричинений подією *A*, можна визначити за допомогою виразу (1)

$$R(A) = P(A)Y(A)\,, \qquad (1)$$

де $P(A) -$ частота події *A*, що має розмірність, обернену до часу; $Y(A)$ – можливий одноразовий збиток, спричинений подією *A*, що має розмірність втрат.

Частота у формулі (1) чисельно дорівнює статистичній імовірності події *A* і виражається числом негативних подій за одиницю часу (відмов/міс., аварій/рік тощо), до якої можна застосувати основні теореми теорії ймовірності. Вважаємо, що ймовірність негативних подій – безрозмірна величина, і згідно з формулою значення повинні мати розмірність збитків. Такий ризик є комбінованим або зведеним (до одиниці часу).

Статична ймовірність події *A* (ризик, що трапився під час події) дорівнює

$$P(A) = \frac{\nu(t)}{T}\,, \qquad (2)$$

де $\nu(t) -$ кількість проявів події *A* за час *t;*

T – період спостереження.

Тоді формула (1) набуває вигляду, визначаючи зміст показника $R(A)$ як кількість підданих ризику протягом періоду спостереження елементів:

$$R(A) = \frac{\nu(t)}{T}\ Y(A)\,, \qquad (1')$$

Ризик, що трапився під час події, є однією з характеристик небезпеки негативної події і є показником уразливості об'єкта. Скористаємося показником ступеня уразливості $C_y(A)$ (або $R(A)$), який є відношенням уражених об'єктів (елементів) $M_{\text{вр.ел.}}$ до їхньої загальної кількості $M_{\text{заг.}}$ (число загальних елементів – кількість елементів ООТ, які опинилися в зоні ураження), зафіксований для події певної інтенсивності:

$$C_y(A) = \frac{M_{вр.ел.}}{M_{заг.}}\,, \qquad (3)$$

Збиток у формулі (1) пов'язаний зі ступенем уразливості співвідношенням

$$Y(A) = C_y(A)Y_n(A)\,, \qquad (4)$$

де $Y_n(A)$ – умовний повний збиток унаслідок реалізації події *A*, який чисельно дорівнює кількості або вартості всіх елементів ООТ або кількості або вартості тих елементів ООТ, що опинилися в зоні ураження.

З урахуванням виразу (2) і (4), формула (1) набуде наступного вигляду:

$$R(A) = \frac{\nu(t)}{T} \quad C_y(A)Y_n(A), \qquad (5)$$

Ця формула є загальною для обчислення ризику. При її практичному використанні в кожному конкретному випадку необхідно вносити уточнення. При розгляді частних ризиків, притаманних саме для певного типу елементів ООТ, які підпали під вплив небезпечної події, до формули (5) вводяться необхідні уточнення. Тоді ризик розраховується за наступною модифікованою формулою:

$$R_ч(A) = \frac{\nu(t)}{T} \; P(H)C_{yч}(A)H\,, \qquad (6)$$

де $R_ч(A)$ – частний ризик;

$P(H)$ – ймовірність перебування елементів певного типу в зоні ураження;

$C_{yч}(A)$ – ступінь уражаємості цієї групи елементів;

H – кількість елементів, що відповідає умовному повному збитку $Y_n(A)$ згідно з формулою (5).

Рисунок 2 – Схема нарахування загального ризику

Розглянемо *приклад нарахування загального ризику*.

Дано.

Нехай унаслідок декомпозиції до І рівня (рис.1) об'єкту ООТ із *10 комплектами ООТ* виділено небезпечні події з такими ймовірними показниками:

І. ймовірність виникнення проблеми з технікою $P_{\text{I}}(A) = 0{,}7$;

ІІ. ймовірність перехоплення інформації або НСД через допоміжне обладнання $P_{\text{II}}(A) = 0{,}6$;

ІІІ. ймовірність лихого задуму $P_{\text{III}}(A) = 0{,}25$;

IV. ймовірність виникнення реальної техногенної або стихійної загрози ззовні $P_{IV}(A) = 0{,}06$.

Для спрощення вважаємо, що:

ймовірності виникнення означених подій вже обчислені за формулою (2);

повний умовний збиток дорівнює кількості всіх комплектів ООТ $Y(A) = 10$;

усі події вважаємо незалежними одна від одної.

Потрібно: обчислити часткові ризики від подій кожного виду; обчислити комбінований ризик.

1. За формулою (1) середні ризики становлять:

– від подій І виду (відмови в ООТ): $R_{\text{I}}(A) = 0{,}7 \cdot 10 = 7$;

– від подій ІІ виду (перехоплення через допоміжне обладнання): $R_{\text{II}}(A) = 0{,}6 \cdot 10 = 6$;

– від подій ІІІ виду (злий задум персоналу): $R_{\text{III}}(A) = 0{,}25 \cdot 10 = 2{,}5$;

– від подій IV виду (негативний вплив середовища): $R_{IV}(A) = 0{,}06 \cdot 10 = 0{,}6$.

2. Обчислимо відповідні ступені ураженості елементів об'єкту за формулою (3) з урахуванням фізичного змісту формули (1):

3.

$$C_{\text{I}} = \frac{7}{10}\ ;\ C_{\text{II}} = \frac{6}{10}\ ;\ C_{\text{III}} = \frac{2{,}5}{10};\ C_{IV} = \frac{0{,}6}{10}.$$

4. Можливі одномоментні збитки від тих же подій відповідно до (5) становитимуть:

$$R_{\text{Iодн.}}(A) = 0{,}7 \cdot \frac{7}{10} \cdot 10 = 4{,}9; \quad R_{\text{IIодн.}}(A) = 0{,}6 \cdot \frac{6}{10} \cdot 10 = 3{,}6;$$

$$R_{\text{IIIодн.}}(A) = 0{,}25 \cdot \frac{2{,}5}{10} \cdot 10 = 0{,}625;$$

$$R_{IV\text{одн.}}(A) = 0{,}06 \cdot \frac{6}{100} \cdot 10 = 0{,}36.$$

Комбінований одномоментний збиток дорівнює:

$$R_{\text{К.одн.}}(A) = 4{,}9 + 3{,}6 + 0{,}625 + 0{,}625 + 0{,}036 = 9{,}16.$$

5. Комбінований середній збиток дорівнює:

$$R_{\text{К.сер.}}\ (A) = 7+6 + 2{,}5 + 0{,}6 = 16{,}1.$$

6. Припустимо, що на кожному з 10-ти комплектів ООТ встановлено 5 комплектів програмного забезпечення. У разі виникнення події I-го виду в зоні ураження може опинитися приблизно чверть наявних ООТ із своїм програмним забезпеченням, 2,5 комплекти апаратури і 12,5 комплектів програмного забезпечення відповідно. Часткові ступені уражаємості дорівнюють:

для апаратури

$$C_{ЧI}^{(HARD)}(A) = \frac{0{,}7 \cdot 2{,}5}{10} = 0{,}175\ ;$$

для програмного забезпечення

$$C_{ЧI}^{(SOFT)}(A) = \frac{0{,}7 \cdot 12{,}5}{50} = 0{,}175\ .$$

Частні ризики від події I-го виду за формулою (6) становитимуть відповідно:

для апаратури

$$R_I^{(HARD)}(A) = 0{,}7 \cdot 0{,}25 \cdot 10 \cdot 0{,}175 = 0{,}31\ ;$$

для програмного забезпечення

$$R_I^{(SOFT)}(A) = 0{,}7 \cdot 0{,}25 \cdot 50 \cdot 0{,}175 = 1{,}53\ .$$

У разі виникнення події II-го виду в зоні ураження може опинитися приблизно половина наявних ООТ зі своїм програмним забезпеченням, тобто 5 комплектів апаратури і 25 комплектів програмного забезпечення відповідно. Звідси:

для апаратури

$$C_{\text{ЧII}}^{(HARD)}(A) = \frac{0{,}6 \cdot 5}{10} = 0{,}3\ ;$$

для програмного забезпечення

$$C_{ЧII}^{(SOFT)}(A) = \frac{0{,}6 \cdot 25}{50} = 0{,}3\ ;$$

Тоді частні ризики від події II-го виду за формулою (6) відповідно становитимуть:

для апаратури

$$\mathrm{R}_{\mathrm{II}}^{(\mathrm{HARD})}(\mathrm{A}) = 0{,}6 \cdot 0{,}5 \cdot 10 \cdot 0{,}3 = 0{,}9;$$

для програмного забезпечення

$$R_{II}^{(SOFT)}(A) = 0{,}6 \cdot 0{,}5 \cdot 50 \cdot 0{,}3 = 4{,}5$$

У разі виникнення події III-го і IV-го виду у зоні ураження опиняться всі наявні ЕОМ із своїм програмним забезпеченням. Звідси

для апаратури

$$\mathrm{C}_{\text{ЧIII}}^{(\mathrm{HARD})}(\mathrm{A}) = \frac{0{,}25 \cdot 10}{10} = 0{,}25\ ;$$

$$C_{ЧIV}^{(HARD)}(A) = \frac{0{,}06 \cdot 10}{10} = 0{,}06\ ;$$

для програмного забезпечення

$$C_{ЧIII}^{(SOFT)}(A) = \frac{0{,}06 \cdot 10}{10} = 0{,}25;$$

$$C_{ЧIV}^{(SOFT)}(A) = \frac{0{,}06 \cdot 50}{50} = 0{,}06.$$

Тоді частні ризики від події III-го виду за формулою (6) становитимуть:

для апаратури

$$R_{III}^{(HARD)}(A) = 0{,}25 \cdot 1{,}0 \cdot 10 \cdot 0{,}25 = 0{,}625;$$

для програмного забезпечення

$$R_{III}^{(SOFT)}(A) = 0{,}25 \cdot 1{,}0 \cdot 0{,}25 \cdot 50 = 3{,}125.$$

Відповідно, частні ризики від події IV-го виду становитимуть:

для апаратури

$$R_{IV}^{(HARD)}(A) = 0{,}06 \cdot 1{,}0 \cdot 10 \cdot 0{,}06 = 0{,}036;$$

для програмного забезпечення

$$R_{IV}^{(SOFT)}(A) = 0{,}06 \cdot 1{,}0 \cdot 0{,}06 \cdot 50 = 0{,}18$$

7. Повний ризик для даного об’єкта:

$$R_{\text{пов.}}(A) = 0{,}31 + 1{,}53 + 0{,}9 + 4{,}5 + 0{,}625 + 3{,}125 + 0{,}036 + 0{,}18 = 8{,}206$$

Безпека – це комплексний критерій оцінки якості будь-якої сучасної системи, яка характеризує як динаміку системи, так і її технічне втілення.

Особливе значення для нормального функціонування зазначених об'єктів має *забезпечення безпеки інформаційної інфраструктури країни при аваріях, катастрофах і стихійних лихах*.

Широке використання систем ПЕОМ і розробка різного плану інформаційних систем підвищують ефективність прийняття групових рішень, алгоритмічні та програмні засоби яких є елементами моделювання деревовидних структур рішень аналізу ризику, прогнозування, містять засоби зв'язку та системи управлянні даними із загальним і індивідуальним доступом, стандартні засоби аналізу даних і управління інформацією.

З урахуванням адаптації раніше розроблених методичних апаратів аналізу ризиків внаслідок надзвичайних ситуацій для об'єктів обчислювальної техніки, показано, що при управлінні безпекою ООТ слід в оцінку ризику вводити весь спектр небезпек, можливих для досліджуваного ООТ при його роботі.

Висновки. Інформаційні потоки сприймаються як різні відомості про стан елементів НС та оточуючого середовища, про впливи на інші дані, що необхідні для досягнення мети.

При управлінні безпекою ООТ слід керуватися наступним:

в оцінку ризику вводити весь спектр небезпек, можливих для досліджуваного ООТ при його роботі;

заходи щодо зниження ризику приймаються на найбільш несприятливих напрямках (рис.1). При виборі засобів захисту перевагу надавати таким, які при однакових витратах забезпечують найбільше зниження ризику.

Проаналізуємо *динаміку зміни небезпечних подій у часі*. Якщо розуміти під безпекою ООТ відсутність неприпустимого ризику враження об'єкта при виникненні небезпечних ситуацій, то для її оцінки вводиться функція S_i.

Сукупність характеристик небезпечних подій, «зважених» з ймовірностями їх виникнення визначимо як функцію ризику H_i.

Для спрощення «потік» небезпечних подій будемо наближено вважати пуассонівським. Тоді для j-ї компоненти досліджуваного об'єкта можна записати:

$$S_i(t) = exp\left\{-t \sum_{i}^{n} \lambda_i \rho_{ij}\right\} \qquad (1)$$

$$H_i(t) = 1 - exp\left\{-t \sum_{i=1}^{n} \lambda_i \rho_{ij}\right\} \qquad (2)$$

де λ_i – інтенсивність небезпечних подій *i*-го порядку;

ρ_{ij} – ймовірність враження подією *i*-го виду *j*-ї компоненти досліджуваного

$$\lambda_i\,(t) = \frac{a_i\,(t)}{T}$$

де $a_i\,(t)$ – математичне очікування числа подій *i*-го типу за період спостереження *T*;

T – період спостереження.

Наближено можна вважати, що

$$\rho_{ij} = \frac{n_{ij}}{n_i}$$

де n_{ij} – число небезпечних подій *i*-го виду, які призвели до враження *j*-ї компоненти;

n_i – загальне число небезпечних подій і-го виду;

n – число джерел небезпеки для даного ООТ.

Тоді сумарні функції безпеки та ризику для всіх компонентів об'єкту будуть такими

$$S_\Sigma = \prod_{j=1}^{k} S_i\,(t) = exp\left\{-\mathrm{t}\sum_{j=1}^{k}\Lambda_j\right\}$$

$$H_\Sigma(\,t) = \prod_{j=1}^{k} H_i\,(t) = 1 - \,exp\left\{-\mathrm{t}\sum_{j=1}^{k}\Lambda_j\right\}$$

$$\Lambda_j = \sum_{i=1}^{N}\lambda_i\;\rho_{ij}$$

Проаналізуємо застосування на практиці наведених формул.

Дано.

Для того ж об'єкта обчислювальної техніки (*K* = 2, п.6 прикладу 1) за результатами спостережень обчислені наступні інтенсивності небезпечних подій:

I. ймовірність виникнення проблеми із технікою $\rho_I\,(A)$ = 2,74;

II. ймовірність перехоплення інформації або НСД через допоміжне обладнання $\rho_{II}\,(A)$ = 1,37;

III. ймовірність лихого задуму $\rho_{III}\,(A)$ = 0,8;

IV. ймовірність виникнення реальної техногенної або стихійної загрози ззовні $\rho_{IV}\,(A)$ = 0,5.

Число джерел небезпеки для даного об'єкта *n* = 10.

Протягом певного періоду спостережень мали місце (для всіх варіантів):

50 подій I виду, з них 15 призвели до враження апаратури, 20 – до враження програмного забезпечення;

10 подій II виду, з них 3 призвели до враження апаратури, 5 – до враження програмного забезпечення;

5 подій III виду, з них 1 призвела до враження апаратури, 20 – до враження програмного забезпечення;

2 події IV виду, з них 1 призвела до враження апаратури, 1 – до враження програмного забезпечення.

Потрібно.

Визначити частні та сумарні функції безпеки та ризику.

Для спрощення вважаємо, що:

1. інтенсивності відповідних подій вже обчислені за формулою (3);
2. повний умовний збиток дорівнює кількості всіх комплектів ООТ $Y = (A)$;
3. усі події вважаємо незалежними одна від одної;
4. компонент вважається враженим, коли вражено хоча б один із компонентів ООТ або програмне забезпечення.

Потрібно:

обчислити частні ризики від подій кожного виду;

обчислити комбінований ризик.

1. За формулою (4) обчислимо ймовірність враження компонент досліджує мого об’єкту:

для апаратури

$$\rho_I{}^{HARD} = \frac{15}{50} = 0{,}3;\ \rho_{II}{}^{HARD} = \frac{3}{10};\ \rho_{III}{}^{HARD} = \frac{1}{5} = 0{,}2;\ \rho_{IV}{}^{HARD} = \frac{1}{2} = 0{,}5;$$

для програмного забезпечення

$$\rho_I{}^{SOFT} = \frac{15}{50} = 0{,}4;\ \rho_{II}{}^{SOFT} = \frac{2}{10} = 0{,}2;\ \rho_{III}{}^{SOFT} = \frac{5}{5} = 1;$$

$$\rho_{IV}{}^{SOFT} = \frac{1}{2} = 0{,}5;$$

Користуючись формулами (1) і (2) визначимо функції безпеки і ризику для апаратури і програмного забезпечення по кожному із потоку подій:

функції безпеки для апаратного забезпечення

$S^{HARD}(t) = exp\{-t \sum_i^n \lambda_i \rho_{ij}{}^{HARD}\} =$ Завдання на розрахункову роботу

Завдання на розрахункову роботу

$= exp\{-t\,(2{,}74 \cdot 0{,}3 + 1{,}37 \cdot 0{,}3 + 0{,}8 \cdot 0{,}2 + 0{,}5 \cdot 0{,}5)\} = exp\{-1{,}643\,t\}$

функція ризику для апаратного забезпечення

$$H^{HARD}(t) = 1 - S^{HARD}(t) = 1 - exp\left\{-t \sum_{i}^{n} \lambda_i \rho_{ij}{}^{HARD}\right\} =$$
$$= 1 - exp\ \{-1{,}643\ t\}$$

функції безпеки для програмного забезпечення

$$S^{SOFT}(t) = exp\left\{-t \sum_{i}^{n} \lambda_i \rho_{ij}{}^{SOFT}\right\} =$$
$$= exp\ \{-t\ (2{,}74 \cdot 0{,}4 + 1{,}37 \cdot 0{,}2 + 0{,}8 \cdot 1{,}0 + 0{,}5 \cdot 0{,}5)\} = exp\ \{-2{,}42\ t\}$$

функція ризику для програмного забезпечення

$$H^{SOFT}(t) = 1 - S^{SOFT}(t) = 1 - exp\left\{-t \sum_{i}^{n} \lambda_i \rho_{ij}{}^{SOFT}\right\} =$$
$$= 1 - exp\ \{-2{,}42\ t\}$$

1. Сумарні функції безпеки та ризику за формулами (4') ,(5), (6):

$$S_{\sum}(t) = S^{SOFT}(t) \cdot S^{HARD}(t) =$$
$$= exp\left\{-t \sum_{i}^{n} \lambda_i \rho_{ij}{}^{SOFT} + \sum_{i}^{n} \lambda_i \rho_{ij}{}^{HARD}\right\} = \exp\ \{-\ 4{,}063\}$$

$$H_{\sum}(t) = H^{SOFT}(t) \cdot H^{HARD}(t) =$$
$$= 1 - exp\left\{-t \sum_{i}^{n} \lambda_i \rho_{ij}{}^{SOFT} + \sum_{i}^{n} \lambda_i \rho_{ij}{}^{HARD}\right\} = \exp\ \{-\ 4{,}063\}$$

Отже, *ймовірність нештатних ситуацій зростає по експоненті, а стан безпеки ООТ по експоненті спадає.*

При управлінні безпекою ООТ слід керуватися наступним:

в оцінку ризику вводити весь спектр небезпек, можливих для досліджуваного ООТ при його роботі;

заходи щодо зниження ризику приймаються на найбільш несприятливих напрямках (рис.1). При виборі засобів захисту інформації перевагу надавати таким, які при однакових витратах забезпечують найбільше зниження ризику.

Висновки

1. Створення комплексної інформаційної технології у сфері програмно-цільового планування та управління повинно включати розробку, експериментальне і практичне відпрацювання методик синтезу єдиної інформаційної технології для вирішення задач планування та управління роботами із запобігання та ліквідації наслідків надзвичайних ситуацій.

2. Крім виконання інформаційних функцій у межах такої системи повинні бути передбачені можливості моделювання та прогнозування розвитку надзвичайних ситуацій при реалізації альтернативних стратегій управління ними, прогнозу потреби в ресурсах, що необхідні для ліквідації наслідків цих ресурсів.

Додаток 1.

№ варіанту	Ймовірні показники небезпечних подій				Інтенсивності небезпечних подій			
	$P_{\text{I}}(A)$	$P_{\text{II}}(A)$	$P_{\text{III}}(A)$	$P_{IV}(A)$	$\rho_I\ (A)$	$\rho_{II}\ (A)$	$\rho_{III}\ (A)$	$\rho_{IV}\ (A)$
1	0,6	0,8	0,25	0,07	2,68	1,37	0,8	0,4
2	0,5	0,7	0,25	0,05	1,98	1,56	0,7	0,6
3	0,7	0,9	0,25	0,09	2,68	2,04	0,6	0,5
4	0,4	0,5	0,25	0,06	2,66	1,96	0,4	0,2
5	0,5	0,6	0,25	0,04	1,56	1,42	0,7	0,3
6	0,8	0,8	0,25	0,05	2,42	1,22	0,4	0,4
7	0,7	0,7	0,25	0,06	2,46	1,54	0,8	0,2
8	0,4	0,8	0,25	0,07	2,68	1,68	0,2	0,5
9	0,5	0,7	0,25	0,08	2,48	1,84	0,6	0,3
10	0,6	0,4	0,25	0,04	3,02	1,82	0,5	0,6
11	0,7	0,8	0,25	0,08	2,68	1,86	0,8	0,7
12	0,4	0,9	0,25	0,09	3,04	1,48	0,4	0,2
13	0,5	0,5	0,25	0,06	2,86	2,04	0,7	0,4
14	0,7	0,4	0,25	0,05	2,94	1,56	0,4	0,3
15	0,9	0,6	0,25	0,07	2,64	2,04	0,8	0,5
16	0,6	0,7	0,25	0,08	2,88	1,98	0,5	0,2
17	0,7	0,8	0,25	0,05	3,12	1,66	0,3	0,6
18	0,8	0,5	0,25	0,04	2,74	1,78	0,7	0,3
19	0,4	0,9	0,25	0,08	2,64	2,06	0,5	0,5
20	0,6	0,8	0,25	0,04	2,86	2,04	0,4	0,2
21	0,7	0,6	0,25	0,07	2,62	1,44	0,6	0,4
22	0,8	0,7	0,25	0,06	2,84	1,68	0,4	0,3
23	0,6	0,8	0,25	0,08	3,04	1,62	0,8	0,3
24	0,4	0,4	0,25	0,07	2,94	1,88	0,6	0,2
25	0,5	0,5	0,25	0,05	2,62	1,94	0,9	0,6
26	0,6	0,9	0,25	0,06	2,88	1,46	0,7	0,5
27	0,5	0,5	0,25	0,07	2,64	1,58	0,4	0,3
28	0,7	0,7	0,25	0,08	2,46	1,92	0,8	0,4
29	0,9	0,6	0,25	0,05	2,84	1,84	0,7	0,6
30	0,6	0,8	0,25	0,06	2,46	1,64	0,5	0,7
31	0,5	0,5	0,25	0,07	3,12	2,04	0,3	0,2
32	0,8	0,4	0,25	0,08	2,48	1,64	0,8	0,5
33	0,9	0,7	0,25	0,06	2,76	1,92	0,6	0,3
34	0,6	0,8	0,25	0,04	3,08	1,78	0,5	0,2
35	0,4	0,6	0,25	0,07	2,62	156	0,8	0,4

$P_{\text{I}}(A)$ – ймовірність виникнення проблеми з технікою;
$P_{\text{II}}(A)$ – ймовірність перехоплення інформації або НСД через допоміжне обладнання;
$P_{\text{III}}(A)$ – ймовірність лихого задуму;
$P_{IV}(A)$ – ймовірність виникнення реальної техногенної або стихійної загрози ззовні;
$\rho_I\ (A)$ – ймовірність виникнення проблеми із технікою;

$\rho_{II}\ (A)$ – ймовірність перехоплення інформації або НСД через допоміжне обладнання;
$\rho_{III}\ (A)$ – ймовірність лихого задуму;
$\rho_{IV}\ (A)$ – ймовірність виникнення реальної техногенної або стихійної загрози ззовні.

2. ТЕСТОВІ ЗАВДАННЯ

1. Поняття інформаційної безпеки це –
А) захищеність інформаційного середовища суспільства, що забезпечує його формування і розвиток в інтересах громадян, організацій, держави;
Б) стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання, і розвиток в інтересах громадян, організацій, держави;
В) захищеність інформаційного середовища, що забезпечує його формування, використання, і розвиток в інтересах громадян, організацій, держави;
Г) формування, розвиток, захищеність інформаційного суспільства в інтересах організацій і держави;
Д) це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання, і розвиток в інтересах держави.

2. Якими чинниками визначається державна політика в сфері інформатизації та інформаційної безпеки особистості, суспільства, держави?
А) пріоритетністю національних інтересів і має на меті унеможливлення реалізації загроз для інформації;
Б) має на меті унеможливлення реалізації загроз для інформації;
В) пріоритетністю національних інтересів в сфері інформатизації;
Г) пріоритетністю національних інтересів в сфері інформаційної безпеки;
Д) пріоритетністю державних інтересів і має на меті унеможливлення реалізації загроз для інформації;

3. Основою правового регулювання захисту та обмеження доступу до інформації є:
А) норми ч. 2 ст. 32 Конституції України, норми ч. 1 ст. 34 Конституції України;
Б) норми ч. 1 ст. 32 Конституції України, норми ч. 1 ст. 34 Конституції України;
В) норми ч. 1 ст. 31 Конституції України, норми ч. 2 ст. 32 Конституції України;
Г) норми ч. 1 ст. 31 Конституції України, норми ч. 2 ст. 34 Конституції України;
Д) норми ч. 1 ст. 32 Конституції України, норми ч. 2 ст. 34 Конституції України;

4. Об'єктами інформаційної безпеки можуть бути:
А) інформаційні системи різного масштабу і різного призначення;
Б) психіка людини, інформаційні системи різного масштабу і різного призначення;
В) свідомість, інформаційні системи різного масштабу і різного призначення;
Г) свідомість, психіка людини, інформаційні системи різного масштабу і різного призначення;
Д) підсвідомість, інформаційні системи різного масштабу і різного призначення;

5. До суб'єктів інформаційної безпеки відносяться:

А) держава, яка здійснює свої функції через відповідні органи; громадяни, суспільні та організації і об'єднання, що володіють повноваженнями по забезпеченню інформаційної безпеки у відповідності до законодавства;
Б) громадяни, суспільні та організації і об'єднання, що володіють повноваженнями по забезпеченню інформаційної безпеки у відповідності до законодавства;
В) держава, громадяни, суспільні та організації і об'єднання, що володіють повноваженнями по забезпеченню інформаційної безпеки у відповідності до законодавства;
Г) держава, яка володіє повноваженнями по забезпеченню інформаційної безпеки у відповідності до законодавства;
Д) громадяни, суспільні та організації і об'єднання, які здійснюють свої функції по забезпеченню інформаційної безпеки у відповідності до законодавства;

6. Під інформаційним середовищем розуміють:
А) сферу діяльності суб'єктів, пов'язану із створенням, перетворенням і споживанням інформації;
Б) сферу діяльності суб'єктів, пов'язану із створенням і споживанням інформації;
В) сферу діяльності суб'єктів, пов'язану із створенням, перетворенням інформації;
Г) сферу діяльності об'єктів, пов'язану із створенням, і споживанням інформації;
Д) сферу діяльності суб'єктів, пов'язану із модифікацією інформації;

7. Інформаційне середовище умовно поділяється на три основні складові:
А) створення вихідної та похідної інформації; формування інформаційних ресурсів, підготовки інформаційних продуктів, споживання інформації;
Б) розповсюдження вихідної та похідної інформації; формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг; споживання інформації;
В) створення і розповсюдження вихідної та похідної інформації; формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг; споживання інформації;
Г) створення вихідної та похідної інформації; підготовки інформаційних продуктів, надання інформаційних послуг; споживання інформації;
Д) розповсюдження вихідної та похідної інформації; надання інформаційних послуг; споживання інформації;

8. Як класифікуються загрози для інформаційної безпеки відповідно до критичних сфер міжнародного співробітництва ?
А) технологічні; комунікаційні; психологічні;
Б) інформаційно-технологічні; інформаційно-комунікаційні; інформаційно-психологічні;
В) антропогенні; психологічні; техногенні;
Г) інформаційно-антропогенні; інформаційно-техногенні; інформаційно-психіатричні;
Д) інформаційно-технологічні; інформаційно-комунікаційні; обумовлені стихійними
Е) джерелами;

9. Що розуміють під національним інформаційним простором ?
А) усю сукупність інформаційних потоків національного походження, що доступні на території держави;
Б) усю сукупність інформаційних потоків іноземного походження, що доступні на території держави;
В) усю сукупність інформаційних потоків як національного походження, так і іноземних, що доступні на території держави;
Г) усю сукупність інформаційних ресурсів як національного походження, так і іноземних, що доступні на території держави;

Д) усю сукупність інформаційних знань як національного походження, так і іноземних, що доступні на території держави;

10. Державна таємниця (секретна інформація) це:

А) вид таємної інформації, що охоплює відповідні відомості у сфері державної безпеки, розголошення яких може завдати шкоди безпеці України та які визначені в порядку, встановленому законом, державною таємницею і підлягають охороні державою;

Б) вид таємної інформації, що охоплює відповідні відомості у сфері державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визначені в порядку, встановленому державною таємницею і підлягають охороні державою;

В) вид таємної інформації, що охоплює відповідні відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, розголошення яких може завдати шкоди національній безпеці України та які визначені в порядку, встановленому законом і підлягають охороні державою;

Г) вид таємної інформації, що охоплює відповідні відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визначені в порядку, встановленому цим законом, державною таємницею і підлягають охороні державою;

Д) вид таємної інформації, що охоплює відповідні відомості у сфері оборони, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди інформаційній безпеці України та які підлягають охороні державою;

11. У чому полягає доступ до державної таємниці ?

А) надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею;

Б) надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень;

В) надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень;

Г) надання дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності;

Д) надання повноважною посадовою особою дозволу громадянину на ознайомлення з секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з секретною інформацією та провадження діяльності, пов'язаної з державною таємницею;

12. У чому полягає допуск до державної таємниці ?

А) оформлення права громадянина на володіння секретної інформації;

Б) оформлення права громадянина на доступ до конфіденційної інформації;

В) оформлення права громадянина на доступ до секретної інформації;

Г) оформлення права громадянина на доступ до секретної інформації;

Д) оформлення права громадянина на доступ до секретної інформації;

13. У якому документі викладена інформація, що може бути віднесена до державної таємниці відповідно до норм ст. 8 Закону України «Про державну таємницю»?

А) Законі України «Про інформацію»;
Б) Доктрині інформаційної безпеки України;
В) Концепції інформаційної безпеки;
Г) Зводі відомостей, що становлять державну таємниці;
Д) рішенням Ради національної безпеки і оборони України від 21.03.2008 р. «Про невідкладні заходи щодо забезпечення інформаційної безпеки України»;

14. Звід відомостей, що становлять державну таємницю це:

А) наказ, у якому зведено переліки відомостей, що згідно з рішенням державних експертів із питань таємниць становлять державну таємницю у визначених Законом сферах;
Б) акт, у якому зведено переліки відомостей, що становлять державну таємницю у визначених Законом сферах;
В) документ, у якому зведено відомості, що згідно з рішенням державних експертів із питань таємниць становлять державну таємницю у визначених Законом сферах;
Г) акт, у якому зведено перелік даних, що державну таємницю у визначених Законом сферах;
Д) документ, у якому перелічені відомості, що згідно з рішенням державних експертів із питань таємниць становлять державну таємницю у визначених Законом сферах;

15. Технічний захист інформації (ТЗІ) це:

А) діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу до інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації;
Б) діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави;
В) діяльність, спрямована на забезпечення інженерно-технічними заходами цілісності та унеможливлення блокування інформації, яка становить державну та іншу передбачену законом таємницю, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави;
Г) діяльність, спрямована на забезпечення порядку доступу, цілісності та доступності інформації, яка становить державну та конфіденційну інформації, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави;
Д) діяльність, спрямована на забезпечення організаційне забезпечення порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом конфіденційну інформацію, а також цілісності та доступності відкритої інформації, важливої для особи;

16. Основними напрямами державної політики у сфері ТЗІ є:

А) нормативно-правове забезпечення, інженерно-технічне забезпечення, науково-технічна та виробнича діяльність;
Б) документальне забезпечення, організаційне забезпечення, науково-технічна та виробнича діяльність;
В) нормативно-правове забезпечення, організаційне забезпечення, технічна та виробнича діяльність;
Г) нормативно-правове забезпечення, організаційне забезпечення, науково-технічна та виробнича діяльність;

Д) нормативно-правове забезпечення, інженерно-технічне забезпечення, науково та виробнича діяльність;

17. Конфіденційність це:
А) властивість інформації бути захищеною від несанкціонованого спотворення;
Б) властивість інформації бути захищеною від несанкціонованого блокування;
В) властивість інформації бути захищеною від несанкціонованого спотворення;
Г) властивість інформації бути захищеною від несанкціонованого руйнування;
Д) властивість інформації бути захищеною від несанкціонованого ознайомлення;

18. Цілісність це:
А) властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;
Б) властивість інформації бути захищеною від несанкціонованого ознайомлення;
В) властивість інформації бути захищеною від несанкціонованого модифікування;
Г) властивість інформації бути захищеною від несанкціонованого руйнування або знищення;
Д) властивість інформації бути захищеною від несанкціонованого блокування;

19. Доступність це:
А) властивість інформації бути захищеною від несанкціонованого ознайомлення;
Б) властивість інформації бути захищеною від несанкціонованого руйнування;
В) властивість інформації бути захищеною від несанкціонованого блокування;
Г) властивість інформації бути захищеною від несанкціонованого знищення;
Д) властивість інформації бути захищеною від несанкціонованого спотворення;

20. Криптографічний захист інформації це:
А) вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних з метою приховування змісту інформації;
Б) вид захисту, що реалізується за допомогою перетворень інформації з використанням ключових даних з метою приховування (або відновлення) змісту інформації, підтвердження її справжності;
В) вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її конфіденційності;
Г) вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження авторства;
Д) вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

21. Які існують загрози безпеці інформації при забезпеченні конфіденційності ?
А) крадіжка (копіювання) інформації; втрата (витік) інформації та засобів обробки;
Б) крадіжка (копіювання) інформації та засобів обробки; втрата (витік) інформації та засобів обробки;
В) крадіжка (копіювання) інформації та засобів обробки; втрата (витік) інформації;
Г) крадіжка засобів обробки інформації; втрата (витік) інформації та засобів обробки;
Д) копіювання інформації та засобів обробки; втрата засобів обробки;

22. Які існують загрози безпеці інформації при забезпеченні доступності ?
А) блокування інформації; спотворення інформації;

Б) знищення інформації та засобів її обробки; втрата інформації;
В) блокування інформації; копіювання інформації;
Г) спотворення інформації; знищення засобів її обробки;
Д) блокування інформації; знищенні інформації та засобів її обробки;

23. Які існують загрози безпеці інформації при забезпеченні цілісності ?
А) модифікація (спотворення) інформації; заперечення автентичності інформації; нав'язування дестабілізуючої інформації;
Б) модифікація (спотворення) інформації; заперечення автентичності інформації; нав'язування фальшивої інформації;
В) заперечення автентичності інформації; нав'язування фальшивої інформації; знищення засобів обробки інформації;
Г) модифікація (спотворення) інформації; заперечення автентичності інформації; знищення інформації;
Д) модифікація (спотворення) інформації; блокування інформації; нав'язування фальшивої інформації;

24. Які принципи покладені в основу забезпечення інформаційної безпеки держави ?
А) дотримання балансу інтересів особистості, суспільства і держави; взаємна відповідальність суб'єктів забезпечення інформаційної безпеки; інтеграція систем національної і міжнародної безпеки;
Б) законність, дотримання балансу інтересів особистості, суспільства і держави; взаємна відповідальність суб'єктів забезпечення інформаційної безпеки; інтеграція систем національної і регіональної безпеки;
В) законність, дотримання балансу інтересів особистості, суспільства і держави; взаємна відповідальність суб'єктів забезпечення інформаційної безпеки; інтеграція національної і міжнародної системи телекомунікацій;
Г) законність, дотримання балансу інтересів особистості, суспільства і держави; взаємна відповідальність суб'єктів забезпечення інформаційної безпеки; інтеграція систем національної і міжнародної безпеки;
Д) правомірність, дотримання балансу інтересів особистості, суспільства і держави; взаємна відповідальність суб'єктів забезпечення інформаційної безпеки; інтеграція систем національної і міжнародної безпеки;

25. На які групи діляться джерела загроз безпеці інформації ?
А) обумовлені діями суб'єкта (антропогенні джерела загроз); обумовленні технічними засобами (техногенні джерела загроз); обумовлені стихійними джерелами;
Б) обумовлені діями суб'єкта (антропогенні джерела загроз); обумовленні організаційними заходами; обумовлені стихійними джерелами;
В) обумовлені бездіяльністю суб'єкта (антропогенні джерела загроз); обумовленні технічними засобами (техногенні джерела загроз);
Г) обумовлені діями суб'єкта (антропогенні джерела загроз); обумовленні технічними засобами (техногенні джерела загроз); обумовлені глобальним інформаційним моніторингом;
Д) обумовлені інтеграцією систем національної і міжнародної безпеки; обумовленні технічними засобами; обумовлені стихійними джерелами;

26. Хто є антропогенними джерелами загроз ?
А) суб'єкти, дії яких можуть бути кваліфіковані як навмисні злочини; суб'єкти, які мають санкціонований доступ до роботи зі штатними засобами об'єкта, що підлягає захисту;
Б) суб'єкти, дії яких можуть бути кваліфіковані як навмисні або випадкові злочини; суб'єкти, які можуть отримати несанкціонований доступ до роботи зі штатними засобами

об’єкта, що підлягає захисту; суб’єкти, дії яких можуть призвести до порушення безпеки інформації (зовнішні та внутрішні);

В) суб’єкти, дії яких можуть бути кваліфіковані як навмисні або випадкові злочини; суб’єкти, які мають доступ (санкціонований або несанкціонований) до роботи зі штатними засобами об’єкта, що підлягає захисту; суб’єкти, дії яких можуть призвести до порушення безпеки інформації (зовнішні та внутрішні);

Г) суб’єкти, дії яких можуть бути кваліфіковані як випадкові злочини; суб’єкти, які мають санкціонований доступ до роботи зі штатними засобами об’єкта, що підлягає захисту; суб’єкти, дії яких можуть призвести до порушення безпеки інформації (зовнішні);

Д) суб’єкти, дії яких можуть бути кваліфіковані як навмисні або випадкові злочини; суб’єкти, які мають необмежений доступ до роботи зі штатними засобами об’єкта, що підлягає захисту; суб’єкти, дії яких можуть призвести до порушення безпеки інформації (внутрішні);

27. Глобальні фактори загроз інформаційній безпеці це:

А) недружня політика іноземних держав у галузі глобального інформаційного моніторингу; діяльність іноземних розвідувальних та спеціальних служб; злочинні дії міжнародних груп, формувань та окремих осіб;

Б) недружня політика іноземних держав у галузі глобального інформаційного моніторингу; діяльність іноземних розвідувальних та спеціальних служб; комп’ютерна злочинність;

В) недружня політика іноземних держав у галузі глобального інформаційного моніторингу; інформаційні війни; злочинні дії міжнародних груп, формувань та окремих осіб;

Г) недружня політика іноземних держав; діяльність іноземних розвідувальних та спеціальних служб; злочинні дії міжнародних груп, формувань та окремих осіб;

Д) недружня політика сусідніх держав у галузі глобального інформаційного моніторингу; діяльність іноземних розвідувальних та спеціальних служб; адекватна інформованість щодо об’єктів безпеки;

28. У чому полягає засекречування матеріальних носіїв інформації ?

А) введення порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;

Б) введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу таємності матеріальним носіям цієї інформації;

В) введення у встановленому законодавством порядку обмежень на поширення секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;

Г) введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;

Д) введення у встановленому законодавством порядку обмежень на доступ до конкретної таємної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;

29. Категорія режиму секретності це:

А) категорія, яка характеризує важливість відомостей, що становлять державну таємницю і зосереджені в органах державної влади, на підприємствах, в установах і організаціях;

Б) категорія, яка характеризує важливість та обсяги відомостей, що становлять державну таємницю і зосереджені в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях;

В) категорія, яка характеризує обсяги відомостей, що становлять державну таємницю і зосереджені в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях;
Г) категорія, яка характеризує доцільність відомостей, що становлять державну таємницю і зосереджені в органах державної влади, на підприємствах;
Д) категорія, яка характеризує важливість та обсяги відомостей, що становлять державну таємницю і зосереджені в органах місцевого самоврядування, на підприємствах, в установах і організаціях;

30. Охорона державної таємниці це:
А) комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв;
Б) комплекс організаційно-правових, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв;
В) комплекс організаційно-правових, інженерно-технічних, криптографічних заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв;
Г) комплекс інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв;
Д) комплекс організаційно-правових, інженерно-технічних, оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв;

31. Відповідно до яких сфер державної діяльності у ЗВДТ систематизовані відомості, що становлять державну таємницю ?
А) сфера оборони; сфера економіки, науки і техніки; сфера міжнародних відносин; сфера державної безпеки і охорони правопорядку;
Б) сфера оборони; сфера економіки, науки і техніки; сфера регіональних відносин; сфера державної безпеки і охорони правопорядку;
В) сфера оборони; сфера економіки, науки і техніки; сфера зовнішніх відносин; сфера державної безпеки і охорони правопорядку;
Г) сфера оборони; сфера зовнішніх відносин; сфера безпеки інформації, сфера охорони правопорядку;
Д) сфера оборони; сфера економіки; сфера зовнішніх відносин; сфера національної безпеки і охорони правопорядку;

32. Основними завданнями органів, щодо яких здійснюється ТЗІ, є:
А) забезпечення ТЗІ згідно з вимогами правових актів з питань технічного захисту інформації; видання в межах своїх повноважень правових актів; здійснення контролю за станом технічного захисту інформації;
Б) забезпечення ТЗІ згідно з вимогами нормативно-правових актів з питань технічного захисту інформації; надання пропозицій до нормативно-правових актів із зазначених питань в межах своїх повноважень; здійснення нагляду за станом технічного захисту інформації;
В) забезпечення ТЗІ згідно з вимогами нормативно-правових актів з питань технічного захисту інформації; видання в межах своїх повноважень нормативно-правових актів із зазначених питань; здійснення управління станом технічного захисту інформації;

Г) забезпечення ТЗІ згідно з вимогами нормативно-правових актів з питань технічного захисту інформації; видання в межах своїх повноважень нормативно-правових актів із зазначених питань; здійснення контролю за станом технічного захисту інформації;
Д) забезпечення ТЗІ згідно з вимогами внутрішніх документів з питань технічного захисту інформації; видання в межах своїх повноважень нормативно-правових актів із зазначених питань; реалізація технічного захисту інформації;

32. Які можуть бути уразливості безпеці інформації ?
А) технічними, суб'єктивними, випадковими;
Б) об'єктивними, суб'єктивними, випадковими;
В) об'єктивними, економічними, випадковими;
Г) суб'єктивними, випадковими, організаційними;
Д) об'єктивними, суб'єктивними, стихійними;

33. Від чого залежать об'єктивні уразливості безпеці інформації ?
А) від особливостей побудови обладнання, що застосовується на об'єкті захисту;
Б) від технічних характеристик обладнання, що застосовується на об'єкті захисту;
В) від особливостей побудови та електричних характеристик обладнання, що застосовується на об'єкті захисту;
Г) від особливостей побудови та технічних характеристик обладнання, що застосовується на об'єкті захисту;
Д) від особливостей побудови та магнітних характеристик обладнання, що застосовується на об'єкті захисту;

34. Від чого залежать суб'єктивні уразливості безпеці інформації ?
А) від дій співробітників і, в основному, вилучаються організаційними методами;
Б) від дій співробітників і, в основному, вилучаються організаційними та програмно-апаратними методами;
В) від дій співробітників і, в основному, вилучаються програмно-апаратними методами;
Г) від особливостей побудови обладнання, що застосовується на об'єкті захисту;
Д) від особливостей середовища, яке оточує об'єкт захисту, та непередбачених обставин;

35. Від чого залежать випадкові уразливості безпеці інформації ?
А) від дій співробітників і, в основному, вилучаються організаційними та програмно-апаратними методами;
Б) від особливостей середовища, яке оточує об'єкт захисту, та непередбачених обставин;
В) від особливостей середовища, яке оточує об'єкт захисту, та стихійних обставин;
Г) від особливостей середовища, яке оточує об'єкт захисту, та непередбачених обставин;
Д) від особливостей побудови та технічних характеристик обладнання, що застосовується на об'єкті захисту;

36. На які групи прийнято ділити технічні канали витоку інформації ?
А) радіоканали, акустичні канали, електричні канали, оптичні канали, матеріально-речові канали;
Б) радіоканали, мовні канали, електричні канали, оптичні канали, матеріально-речові канали;
В) радіоканали, акустичні канали, магнітні канали, оптичні канали, матеріально-речові канали;
Г) радіоканали, акустичні канали, електричні канали, кабельні канали, матеріально-речові канали;
Д) радіоканали, акустичні канали, електричні канали, оптичні канали, електромагнітні канали;

37. За якими ознаками можлива класифікація каналів передачі інформації ?

А) по виду сигналів, за способом виконання (дротяні, кабельні, радіо тощо), за принципом дії (електромагнітні, акустичні);

Б) по способу передавання, за способом виконання (кабельні, радіо тощо), за принципом дії (електромагнітні, оптичні, акустичні);

В) по виду сигналів і способу передавання, за способом виконання (дротяні, кабельні, радіо тощо), за принципом дії (електромагнітні, оптичні, акустичні);

Г) по виду сигналів і способу приймання, за способом виконання (дротяні, кабельні, радіо тощо), за принципом дії (електромагнітні, оптичні, акустичні);

Д) по виду сигналів і способу передавання, за способом виконання (дротяні, кабельні, радіо тощо), за технічними характеристиками;

38. За якими ознаками можлива класифікація радіоканалів витоку інформації ?

А) за технічними характеристиками, по діапазону приймання, по середовищу розповсюдження;

Б) за природою утворення, по діапазону випромінювання, по середовищу виникнення;

В) за природою передавання, по діапазону випромінювання, по середовищу розповсюдження;

Г) за природою утворення, по діапазону випромінювання, по середовищу утворення;

Д) за природою утворення, по діапазону випромінювання, по середовищу розповсюдження;

39. Які розрізняють методи дублювання інформації у відповідності з процедурою дублювання ?

А) повного копіювання; дзеркального копіювання; часткового копіювання; комбінованого копіювання;

Б) технічного копіювання; дзеркального копіювання; часткового копіювання; комбінованого копіювання;

В) повного копіювання; розподіленого копіювання; часткового копіювання; комбінованого копіювання;

Г) повного копіювання; дзеркального копіювання; комбінованого копіювання;

Д) повного копіювання; дзеркального копіювання; часткового копіювання; контрольного копіювання;

40. Які існують шляхи отримання захищених від несанкціонованого доступу комп'ютерних систем ?

А) створення спеціалізованих комп'ютерних систем, оснащення універсальних систем додатковими засобами захисту, використання додаткових програмних засобів;

Б) створення спеціалізованих комп'ютерних систем, оснащення універсальних систем додатковими засобами захисту, використання додаткових апаратно-програмних засобів;

В) створення ізольованих комп'ютерних систем, оснащення універсальних систем додатковими засобами захисту, використання додаткових програмних або апаратно-програмних засобів;

Г) створення спеціалізованих комп'ютерних систем, розроблення криптографічних систем захисту, використання додаткових програмних або апаратно-програмних засобів;

Д) створення спеціалізованих комп'ютерних систем, оснащення універсальних систем додатковими засобами захисту, використання додаткових програмних або апаратно-програмних засобів;

41. Які рівні захисту можна виділити для окремого об'єкта комп'ютерної системи?

А) охорона території об'єкта, охорона по периметру будівлі, охорона приміщення, захист апаратних засобів, захист програмних засобів, захист інформації;

Б) охорона по периметру території об’єкта, охорона по периметру будівлі, охорона приміщення, захист апаратних засобів, захист програмних засобів, блокування інформації;
В) охорона по периметру території об’єкта, охорона будівлі, охорона приміщення, захист апаратних засобів, захист програмних засобів, захист інформації;
Г) охорона по периметру території об’єкта; охорона по периметру будівлі; охорона приміщення; захист апаратних засобів; криптографічний захист програмних засобів; захист інформації;
Д) охорона по периметру території об’єкта, охорона по периметру будівлі, охорона приміщення, захист апаратних засобів, захист програмних засобів, захист інформації;

42. За якими ознаками можуть бути кваліфіковані комп’ютерні віруси ?
А) по середовищу розповсюдження; за способу зараження; за ступенем небезпеки деструктивних впливів; за алгоритмом функціонування;
Б) по середовищу знаходження; за способу зараження; за ступенем небезпеки деструктивних впливів; за алгоритмом функціонування;
В) по середовищу знаходження; засобами зараження; за ступенем небезпеки деструктивних впливів; за алгоритмом функціонування;
Г) по середовищу знаходження; за способу зараження; за ступенем небезпеки сторонніх впливів; за алгоритмом функціонування;
Д) по середовищу розповсюдження; за способу зараження; за ступенем небезпеки деструктивних впливів; за способом функціонування;

43. По середовищу знаходження комп’ютерні віруси поділяються на:
А) локальні, файлові, завантажувальні, комбіновані;
Б) мережеві, системні, завантажувальні, комбіновані;
В) мережеві, файлові, завантажувальні, комбіновані;
Г) мережеві, файлові, алгоритмічні, комбіновані;
Д) мережеві, файлові, завантажувальні, характерологічні;

44. На які класи у відповідності з особливостями алгоритму функціонування діляться комп’ютерні віруси ?
А) віруси, які не змінюють середовище знаходження (файли і сектори) при розповсюдженні; віруси, які змінюють середовище знаходження при розповсюдженні;
Б) віруси, які змінюють середовище знаходження (сектори) при розповсюдженні; віруси, які змінюють середовище знаходження при розповсюдженні;
В) віруси, які змінюють середовище знаходження (файли) при розповсюдженні; віруси, які не змінюють середовище знаходження при розповсюдженні;
Г) віруси, які не змінюють середовище розповсюдження (файли і сектори); віруси, які не змінюють середовище знаходження при розповсюдженні;
Д) віруси, які не змінюють середовище знаходження (файли і сектори) при розповсюдженні; віруси, які змінюються при розповсюдженні;

45. З якою метою проводиться категорювання об’єктів ?
А) визначення ефективності захисту об’єкта;
Б) визначення нижчого грифа таємності циркулюючої на об’єкті інформації з метою вживання обґрунтованих заходів з технічного захисту;
В) дослідження внутрішньої структури, зовнішніх зв’язків, умов функціонування і зовнішнього середовища інформаційної системи щодо виявлених об’єктів, що підлягають захисту;
Г) визначення вищого грифа таємності циркулюючої на об’єкті інформації з метою вживання обґрунтованих заходів з технічного захисту;
Д) проведення організаційно-технічних і режимних заходів і методів захисту інформації;

46. Що не вказується в рішенні державного експерта з питань таємниць ?
А) інформація, що представляє державну таємницю;
Б) для якого відомства дана інформація вважається державною таємницею;
В) термін дії рішення про віднесення інформації до державної таємниці;
Г) ступінь таємності зазначеної інформації;
Д) підстави віднесення інформації до державної таємниці і, у випадку її розголошення, обґрунтування збитку життєво важливим інтересам держави;

47. Що в цілому розуміється під об'єктом захисту інформації ?
А) інформаційна система;
Б) модель порушника;
В) відносини в сфері захисту інформації;
Г) автоматизована система;
Д) апаратно-програмні засоби;

48. Хто формує та публікує звід відомостей, що становлять державну таємницю ?
А) Служба безпеки України;
Б) Міністерство внутрішніх справ України;
В) Генеральна прокуратура України;
Г) експерти з питань таємниць;
Д) Міністерство оборони;

49. До якого виду інформації відносяться «зведення, що знаходяться у володінні, чи використанні розпорядженні окремих фізичних або юридичних осіб і розповсюджувані за їхнім бажанням у відповідності передбаченими ними умовами» ?
А) конфіденційна інформація;
Б) комерційна таємниця;
В) державна таємниця;
Г) відкрита інформація;
Д) з обмеженим доступом;

50. До якої властивості інформації відноситься визначення «властивість інформації бути захищеної від несанкціонованого блокування» ?
А) конфіденційність;
Б) доступність;
В) комунікабельність;
Г) режимна адекватність;
Д) цілісність;

51. Яка інформація підлягає захисту від загроз порушення конфіденційності, цілісності і доступності ?
А) відкрита інформація;
Б) інформація з обмеженим доступом;
В) комерційна таємниця;
Г) секретна інформація і конфіденційна інформація;
Д) відкрита інформація й інформація з обмеженим доступом;

52. Як називаються об'єкти (приміщення), у яких циркулює інформація, що підлягає захисту ?
А) режимні об'єкти;
Б) виділені об'єкти;
В) захищені об'єкти;

Г) атестовані об’єкти;
Д) спеціальні об’єкти;

53. До якої категорії відносяться об’єкти, на яких циркулює інформація, що містить зведення, що складають державну таємницю, для якої встановлений гриф таємності «особливої важливості» ?
А) четвертої категорії;
Б) другої категорії;
В) особливої категорії;
Г) першої категорії;
Д) третьої категорії;

54. Як називаються події, що потенційно можуть порушити одне з властивостей інформації, з погляду її захисту ?
А) форс-мажор;
Б) правопорушення;
В) події;
Г) атака;
Д) загрози;

55. Якому терміну відповідає визначення «територія, на якій виключається несанкціоноване перебування сторонніх осіб і виключена можливість застосування технічних засобів розвідки» ?
А) захищена зона;
Б) тимчасово контрольована зона;
В) контрольована зона;
Г) режимна зона;
Д) виділена зона;

56. З якого часу інформація вважається державною таємницею ?
А) з часу винесення рішення державним експертом;
Б) з часу включення інформації в Розгорнутий перелік відомостей що становлять державну таємницю;
В) з часу підписання наказу СБ України;
Г) з часу включення інформації в Звід відомостей, що становлять державну таємницю;
Д) з часу підписання наказу МВС України;

57. Перерахувати основні види інформаційної діяльності:
А) отримання, використання, розповсюдження, зберігання інформації;
Б) визначення, використання, розповсюдження, зберігання інформації;
В) отримання, модифікація, розповсюдження, зберігання інформації;
Г) визначення, використання, обмеження, зберігання інформації;
Д) отримання, розповсюдження, перероблення, зберігання інформації;

58. Право власності на інформацію – це:
А) врегульовані законом суспільні відносини щодо володіння, користування і розпорядження інформації;
Б) майнові права щодо володіння, користування і розпорядження інформації;
В) перетворення інформації своїми силами і за свій рахунок;
Г) отримання інформації про діяльність органів місцевого і регіонального самоврядування та місцевої адміністрації;
Д) інформаційні відносини щодо володіння, користування і розпорядження інформацією;

59. Коли інформація вважається захищеною ?

А) інформація вважається захищеною, якщо при її переміщенні дотримується режимна адекватність комунікабельних носіїв інформації;
Б) інформація вважається захищеною, якщо при її переміщенні дотримується секретна адекватність комунікабельних носіїв інформації;
В) при наданні їй грифу таємності;
Г) при захисті її програмними та технічними засобами;
Д) інформація вважається захищеною, якщо при її переміщенні дотримується нормативно-правова адекватність носіїв інформації;

60. «Гриф секретності» це:

А) реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації;
Б) реквізит носія секретної інформації, що засвідчує секретність інформації;
В) реквізит носія таємної інформації, що засвідчує секретність інформації;
Г) реквізит носія таємної інформації, що засвідчує санкціонованість доступу до інформації;
Д) ступінь секретності даної інформації;

61. Як розшифровується абревіатура ОІД ?

А) об’єкт дослідження документів;
Б) відділ дослідження документів;
В) об’єкт інформаційної діяльності;
Г) організаційно-інформаційний доступ;
Д) відділ інноваційної діяльності;

62. Як розшифровується абревіатура КВІ ?

А) канали витоку інформації;
Б) канали визначення інформації;
В) комітет по впровадженню інвестицій;
Г) комітет вітчизняної інформатизації;
Д) каскад витоку інформації;

63. До якої групи джерел загроз інформації відносяться суб’єкти, котрі можуть бути кваліфіковані як навмисні чи випадкові злочини ?

А) антропогенні джерела загроз;
Б) електромагнітні джерела загроз;
В) стихійні джерела загроз;
Г) техногенні джерела загроз;
Д) свідомі джерела загроз;

64. Як розшифровується абревіатура НСД ?

А) незрозумілий стан даних;
Б) несанкціонований доступ;
В) несвоєчасний сеанс доступу;
Г) налагоджена система доступу;
Д) недоступність системи даних;

65. До якої групи джерел загроз інформації відносяться обставини, що складають нездоланну силу, тобто такі обставини, що носять об'єктивний і абсолютний характер, що поширюється на всіх ?

А) навмисні джерела загроз;
Б) стихійні джерела загроз;
В) ненавмисні джерела загроз;
Г) техногенні джерела загроз;
Д) антропогенні джерела загроз;

66. Який з перерахованих каналів не відноситься до технічних каналів витоку інформації ?
А) канал побічних електромагнітних випромінювань і наведень;
Б) хімічний канал;
В) акустичний канал;
Г) телевізійний канал;
Д) радіотехнічний канал;

67. Яким шляхом передбачається захистити інформацію основними технічними мірами ?
А) виявлення загроз інформації з використанням спеціальних засобів ТЗІ;
Б) блокування виявлених загроз з використанням спеціальних засобів ТЗІ;
В) ранжування загроз інформації з використанням спеціальних засобів ТЗІ;
Г) виявлення загроз інформації без використання спеціальних засобів ТЗІ;
Д) руйнування виявлених загроз з використанням спеціальних засобів ТЗІ;

68. У результаті якої з причин відбуваються найбільші загрози втрати інформації ?
А) помилка оператора;
Б) пожежі;
В) стихійні лиха;
Г) помилки апаратури, програми;
Д) збій електроживлення;

69. Як доцільно оформляти політику інформаційної безпеки ?
А) окремими документами;
Б) кількома документів;
В) єдиним документом;
Г) двома документами;
Д) документом з грифом секретності;

70. Якому терміну відповідає визначення «описує мету, задачі, загальні вимоги, правила, обмеження, рекомендації в сфері інформаційної безпеки» ?
А) окрема модель загроз;
Б) окрема модель техногенних і стихійних джерел загроз;
В) контрольована зона;
Г) політика інформаційний безпеки;
Д) окрема модель порушника;

71. Якому терміну відповідає визначення «опис загроз і схематичне представлення шляхів їхнього здійснення для об’єкта захисту» ?
А) ситуаційний план об’єкта;
Б) окрема модель техногенних і стихійних джерел загроз;
В) окрема модель загроз;
Г) контрольована зона;
Д) окрема модель порушника;

72. **Укажіть повний перелік носіїв інформації:**
А) паперові, магнітні, оптичні носії;
Б) електричний струм, акустичне поле;
В) фізичні поля, середовища, людина;
Г) паперові, магнітні, електричний струм, акустичне поле;
Д) оптичні носії, електричний струм, акустичне поле;

73. Яка задача є зайвої при визначенні об'єктів, які підлягають захисту?
А) дослідження внутрішньої структури, зовнішніх зв'язків, умов функціонування і зовнішнього середовища інформаційної системи щодо виявлених об'єктів, що підлягають захисту;
Б) визначення носіїв інформації та об'єктів, що підлягають захисту;
В) визначення інформації, що підлягає захисту;
Г) оцінка інформації, що підлягає захисту;
Д) усі задачі необхідні;

74. Що не вказується в рішенні державного експерта з питань таємниць?
А) інформація, що представляє державну таємницю;
Б) для якого відомства дана інформація вважається державною таємницею;
В) термін дії рішення про віднесення інформації до державної таємниці;
Г) ступінь таємності зазначеної інформації;
Д) підстави віднесення інформації до державної таємниці і, у випадку її розголошення, обґрунтування збитку життєво важливим інтересам держави;

75. При дослідженні інформаційної системи вирішуються наступні задачі:
А) визначається місцезнаходження організації та контрольована територія;
Б) визначається перелік виділених приміщень, автоматизованих систем та об'єктів;
В) проводиться категоріювання об'єктів, на яких циркулює ІОД;
Г) складається план контрольованої зони, що до якої здійснюється ТЗІ;
Д) усі вищезазначені відповіді вірні;

76. Які задачі не входять до переліку задач при дослідженні інформаційної системи?
А) визначається місцезнаходження організації та контрольована територія;
Б) визначається перелік виділених приміщень, автоматизованих систем та об'єктів;
В) проводиться категоріювання об'єктів, на яких циркулює ІОД;
Г) складається план контрольованої зони, що до якої здійснюється ТЗІ;
Д) немає правильної відповіді;

77. Дати визначення терміну «допуск до державної таємниці»:
А) допуск до державної таємниці – оформлення права громадянина на доступ до секретної інформації;
Б) допуск до державної таємниці – дозвіл громадянину на доступ до секретної інформації;
В) допуск до державної таємниці – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності;
Г) надання дозволу громадянину на ознайомлення з конкретною секретною інформацією;
Д) усі відповіді вірні;

78. Як називаються об'єкти (приміщення), у яких циркулює інформація, що підлягає захисту?
А) режимні об'єкти;
Б) виділені об'єкти;

В) захищені об’єкти;
Г) атестовані об’єкти;
Д) всі перераховані об’єкти;

79. Що не є основою побудови системи захисту інформації ?
А) організаційно-технічні і режимні міри і методи захисту інформації;
Б) законодавча, нормативно-правова, наукова і методична база забезпечення захисту інформації;
В) програмно-технічні способи і засоби, використовувані для захисту інформації;
Г) структура і задачі органів (підрозділів), що забезпечують безпеку інформаційних технологій;
Д) усі зазначені відповіді правильні;

80. Якому терміну відповідає визначення «територія, на якій виключається несанкціоноване перебування сторонніх осіб і виключена можливість застосування технічних засобів розвідки»?
А) захищена зона;
Б) тимчасово контрольована зона;
В) контрольована зона;
Г) режимна зона;
Д) немає правильної відповіді;

81. З якого моменту інформація вважається державною таємницею?
А) з часу винесення рішення державним експертом;
Б) з часу її включення в Розгорнутий перелік відомостей, що становлять державну таємницю;
В) з часу підписання наказу СБ України;
Г) з часу її включення в Звід відомостей що становлять державну таємницю;
Д) з часу підписання наказу МВС України;

82. Який елемент не включається у план контрольованої зони?
А) ситуаційний план розташування організації на місцевості;
Б) проходження кордону контрольованої зони;
В) віддалення виділених приміщень і об’єктів, на яких циркулює ІОД;
Г) складається план контрольованої зони, що до якої здійснюється ТЗІ;
Д) усі вищезазначені елементи включаються до плану;

83. Перерахувати необхідні умови для забезпечення безпеки інформації при здійсненні інформаційних відносин?
А) оформлений належний допуск, обґрунтована службова необхідність цих відносин, забезпечений достатній рівень захисту від НСД;
Б) забезпечений достатній рівень захисту від НСД;
В) відсутність засобів перехоплення інформації;
Г) наявність режимної комунікації;
Д) немає правильної відповіді;

84. Який захід не відноситься до основних технічних заходів?
А) перетворення (шифрування, скремблірування) сигналів у каналах зв’язку;
Б) блокування ТКВІ з використанням активних засобів;
В) блокування ТКВІ з використанням активно-пасивних засобів;
Г) блокування ТКВІ з використанням пасивних засобів;
Д) встановлення портативних електронних пристроїв перехоплення інформації (заставних пристроїв);

85. Який захід, з використанням активних засобів, не відноситься до заходів щодо блокування ТКВІ?
А) просторове зашумлення;
Б) немає правильної відповіді;
В) лінійне зашумлення;
Г) контроль і обмеження доступу на об'єкти ТЗПІ;
Д) знищення заставних пристроїв;

86. Який з каналів не відноситься до каналів, що виникаючим між джерелом і одержувачем інформації?
А) людина – технічний засіб;
Б) технічний засіб – людина;
В) технічний засіб – технічний засіб;
Г) людина – людина;
Д) усі відповіді неправильні;

87. Які із зазначених технічних каналів витоку інформації, у залежності від використовуваних фізичних полів (трактів), є зайвими?
А) оптичні;
Б) віброакустичні;
В) провідні;
Г) усі відповіді правильні;
Д) електромагнітні;

88. Яка з загроз інформації є зайвої ?
А) загроза порушення цілісності;
Б) загроза порушення комунікативності;
В) загроза порушення доступності;
Г) загроза порушення конфіденційності;
Д) усі загрози;

89. Яким способом передбачається захистити інформацію первинними технічними засобами ?
А) виявлення загроз інформації без використання спеціальних засобів ТЗІ;
Б) виявлення загроз інформації з використанням спеціальних засобів ТЗІ;
В) блокування виявлених загроз без використання спеціальних засобів ТЗІ;
Г) блокування виявлених загроз з використанням спеціальних засобів ТЗІ;
Д) немає правильної відповіді;

90. Який захід не відноситься до заходів щодо виявлення закладних пристроїв з використанням пасивних засобів?
А) встановлення у виділених приміщеннях засобів і систем виявлення лазерного опромінення (підсвічування) віконного скла;
Б) спеціальна перевірка виділених приміщень з використанням нелінійних локаторів;
В) встановлення у виділених приміщеннях стаціонарних виявлювачів диктофонів;
Г) організація радіоконтролю (постійно на час проведення конфіденційних заходів) і побічних електромагнітних випромінювань ТЗПІ;
Д) пошук заставних пристроїв з використанням індикаторів поля, інтерсепторів, частотомірів, скануючих приймачів і програмно-апаратних комплексів контролю;

91. Що розуміється під загрозою в сфері захисту інформації ?
А) дія чи бездіяльність у результаті якого може відбутися витік інформації;
Б) залякування співробітників які зберігають інформацію;

В) усі відповіді невірні;
Г) існування небезпеки життя і здоров'ю членів родини які володіють інформацією;
Д) подія, що потенційно може порушити одне з властивостей інформації, що захищаються;

92. Якому терміну відповідає визначення «це комплекс адміністративних і обмежувальних заходів, спрямованих на оперативне рішення задач захисту шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) забезпечення інформаційної діяльності і засобів (систем) забезпечення ТЗІ»?
А) організаційні заходи захисту інформації;
Б) організаційно-технічні заходи захисту інформації;
В) технічні заходи захисту інформації;
Г) комплексна система захисту інформації;
Д) немає правильної відповіді;

93. У результаті якої дії відбувається несанкціонований доступ до інформації?
А) підключення до апаратури і ліній зв'язку;
Б) маскування під зареєстрованих (законних) користувачів;
В) подолання мір захисту для одержання (використання) інформації або нав'язування помилкової;
Г) застосування заставних пристроїв і вбудованих програм і впровадження комп'ютерних вірусів;
Д) усі відповіді правильні;

94. Який захід не відноситься до пасивного засобу по блокуванню ТКВІ?
А) контроль і обмеження доступу у виділені приміщення;
Б) розв'язання інформаційних сигналів;
В) контроль і обмеження доступу на об'єкти ТЗПІ;
Г) просторове зашумлення;
Д) локалізація випромінювань;

95. Що не є підставою для перегляду політики безпеки?
А) інформація, зібрана в процесі аналізу ризиків і аудита;
Б) інформація, зібрана в процесі аналізу;
В) зміна вартості устаткування захисту інформації;
Г) дані, зібрані в процесі впровадження правил і процедур, створених на базі цих правил;
Д) усі відповіді вірні;

96. Як доцільно оформляти політику інформаційної безпеки?
А) єдиним документом, а не у виді декількох документів;
Б) не єдиним документом;
В) у виді декількох документів;
Г) єдиним документом;
Д) немає правильної відповіді;

97. Якому терміну відповідає визначення «описує мету, задачі, загальні вимоги, правила, обмеження, рекомендації в сфері інформаційної безпеки»?
А) окрема модель загроз;
Б) окрема модель техногенних і стихійних джерел загроз;
В) контрольована зона;
Г) політика інформаційний безпеки;
Д) окрема модель порушника;

98. Якому терміну відповідає визначення «опис загроз і схематичне представлення шляхів їхнього здійснення для об’єкта захисту»?

А) ситуаційний план об'єкта;
Б) окрема модель техногенних і стихійних джерел загроз;
В) окрема модель загроз;
Г) контрольована зона;
Д) окрема модель порушника;

99. Які об’єкти підлягають інвентаризації при опису компонентів АС (автоматизованої системи) ?

А) обладнання ЕОМ і їх складові частини;
Б) програмне забезпечення;
В) данні тимчасового та постійного зберігання;
Г) персонал АС(автоматизованої системи);
Д) усі вищеназвані об’єкти;

100. Які об’єкти не являються об’єктами інвентаризації при опису компонентів АС (автоматизованої системи) ?

А) обладнання ЕОМ і їх складові частини;
Б) програмне забезпечення;
В) данні тимчасового та постійного зберігання;
Г) персонал АС(автоматизованої системи);
Д) засоби і системи кондиціювання.

Розробник(и):
старший викладач кафедри організації та технічного
забезпечення аварійно-рятувальних робіт
факультету цивільного захисту, к.ю.н., доцент Лариса БОРИСОВА