УДК 621.396 **Стефурак О.Р., Тихонов Ю.О., Лаптєв О.А., Зозуля С.А.**
DOI: 10.31673/2409-7292.2020.021926

УДОСКОНАЛЕННЯ СТОХАСТИЧНОЇ МОДЕЛІ З МЕТОЮ ВИЗНАЧЕННЯ ЗАГРОЗ ПОШКОДЖЕННЯ АБО НЕСАНКЦІОНОВАНОГО ВИТОКУ ІНФОРМАЦІЇ

Ключову роль при побудові систем безпеки інформаційних ресурсів, як складових національних інформаційних ресурсів держави, відіграє теорія та практика, в якій науково-методологічна база є основою для прийняття обґрунтованих та ефективних управлінських рішень суб'єктами забезпечення інформаційної безпеки держави на усіх рівнях. У статті на основі аналітичного аналізу загроз пошкодження або несанкціонованого витоку інформації на об'єктах інформаційної діяльності визначаються критичні складові безпеки інформаційного простору. На основі отриманих аналітичних даних удосконалено стохастичну модель загроз пошкодження або несанкціонованого витоку інформації на об'єктах інформаційної діяльності. За результатами запропонованої моделі проведено моделювання, з метою підтвердження аналітичних даних та визначених пріоритетів забезпечення інформаційної безпеки. Визначаються найбільш критичні напрямки та загрози інформаційної безпеки. Отримані результати дозволяють планувати систему інформаційної безпеки з урахуванням найбільш ймовірних загроз. Планувати та впроваджувати першочергові заходи інформаційної безпеки. Зосереджувати кошти для захисту більш імовірних напрямків загроз.

Ключові слова: інформаційна безпека, критичні загрози, модель, виток інформації.

Вступ

У сучасних умовах, як показала практика, важлива роль у забезпеченні національної безпеки України та особливо її економічної складової належить процесам забезпечення інформаційної безпеки держави. Ключову роль при побудові систем безпеки інформаційних ресурсів як складових національних інформаційних ресурсів держави, відіграє теорія та практика, в якій науково-методологічна база є основою для прийняття обґрунтованих та ефективних управлінських рішень суб'єктами забезпечення інформаційної безпеки держави на усіх рівнях. Революційні зміни останнього десятиліття, що відбулися в безпеці держави, зумовили об'єднання інформаційних та комп'ютерних мереж в єдиний інформаційний та кібернетичний простір, що спонукало до створення автоматизованих систем, які істотно розширили спектр електронних послуг державних і комерційних банків світу та України. Як наслідок, суттєво трансформувалися і загрози такому національному інформаційному ресурсу держави. Прояви ознак гібридності внаслідок одночасного впливу загроз інформаційній безпеці, кібернетичній безпеці та безпеці інформації призвели до виникнення явища синергізму, негативні прояви якого потребують кардинального перегляду концепцій побудови діючих систем безпеки. Потребують кардинального перегляду діючі методологічні засади побудови системи безпеки інформаційних ресурсів як України зокрема, так і світу в цілому. Перспективним підходом до безпеки інформаційних ресурсів є одночасне та раціональне поєднання організаційних і технічних зусиль, спрямованих на забезпечення інформаційної та кібербезпеки. При цьому комплексування сил і засобів безпеки у кожному окремому випадку не можна вважати ефективним та таким, що гарантує досягнення очікуваного безпекового синергетичного ефекту.

З метою визначення імовірних загроз системи захисту інформації потрібно визначати максимальні ризики. Тому методологічні підходи які забезпечують виявлення критичних загроз є дуже актуальними.

Короткий аналіз літературних даних

Більшість відомих підходів до моделювання, відрізняються тим, які параметри при моделюванні ними використовують в якості вхідної інформації та які характеристики модельованої системи розраховуються та надходять на вихід моделі (будують моделі з використанням Теорії ймовірностей, випадкових процесів, мереж Петрі, Теорії автоматів, Теорії графів, нечітких множини, Теорії катастроф, ентропійного підходу та ін.).

При цьому аналітичні моделі, що розглядаються з позиції теоретичної математики не тотожні реальній дійсності, зважаючи на обмежену точність результатів. [1,3].

У [4] розглядається модель інформаційної безпеки на основі Марковських випадкових процесів. Отримані чисельні значення, однак вони розглядають питання загрози уразливості. Питання загроз уразливості не торкається питання взаємозалежності основних параметрів моделі, що можливо призводить до ускладнення моделювання процесу.

У [5,6] звертається увага на нестійкість і отже, великі варіації отриманих рішень при поганій обумовленості систем лінійних алгебраїчних рівнянь і неточно заданих значень ефектів і результатів спостережень. Це пов’язане з питанням не врахування взаємозалежності основних параметрів

Разом з тим у всіх зазначених джерелах математичне моделювання розглядається як математична модель конкретних параметрів (деякі параметри мають імовірнісний характер). Питання взаємозв'язку вхідних параметрів при моделюванні процесів та глибину їх взаємозв'язку в моделі не розглядають. Ці чинники взаємозв'язку і взаємовпливу можуть істотно спотворити результати моделювання і поставити під сумнів адекватність моделі.

Виходячи з цього оцінка можливості пошкодження або несанкціонованого витоку інформації, взаємний вплив однієї критичної характеристики параметра на інший, залежність цих параметрів від числа проведених практичних заходів є дуже важливою на сучасному етапі.

Постановка проблеми

В процесі захисту інформації виникає задача визначення основного переліку критичних загроз, параметрів і властивостей, за якими створюються системи захисту інформації. Виявлення мінімальної кількості критичних загроз залежить від кількості взаємопов'язаних параметрів. При виключенні на першому етапі взаємопов'язаних параметрів які менш за все впливають на загрозу пошкодження або несанкціонованого витоку інформації значно скорочується час локалізації загрози та економить кошти. Тому питання розробки методу оцінки загроз пошкодження або несанкціонованого витоку інформації на основі Стохастичної моделі є дуже актуальним.

Мета

Удосконалити стохастичну модель з метою визначення загроз пошкодження або несанкціонованого витоку інформації на основі статистичного аналізу загроз зарубіжних аналітиків.

Виклад основного матеріалу.

Гарантією безпечної роботи з інформаційної системи є виконання необхідних заходів, які зводять до мінімуму всі існуючі ризики з урахуванням їх ступеня впливу на безпеку. Ці вимоги визначаються необхідністю врахування всіх ризиків і інтересів, що виникають в процесі впровадження нових інформаційних технологій. Метою дослідження є побудова моделей створення та оцінки ефективності систем, що забезпечують безпеку при роботі з інформаційно-вимірювальними системами на основі системного підходу до врахування впливу ризиків. Для визначення необхідного комплексу заходів, що забезпечують безпеку, побудована модель створення системи безпеки. Компанії, що мають стратегії кібербезпеки, повинні гарантувати, що кожна з підкатегорій кібербезпеки (розглянуто нижче) буде врахована, не зважаючи на будь-яку, потенційно залишить організації вразливими.

Критична інфраструктура. Громади повсякденно покладаються на критичну інфраструктуру. До таких систем належать лікарні, комунальні компанії, такі як електричні, газові чи водопровідні, та автоматизовані системи, що застосовуються у всіх містах, наприклад, світлофори та залізничні переїзди. Ці критичні інфраструктурні системи пов'язані з Інтернетом, і все, що має підключення до Інтернету, загрожує кібератакою. Організації, що керують критичною інфраструктурою, повинні забезпечувати найвищий рівень планування кібербезпеки і постійно переоцінювати їх планування, плани на випадок надзвичайних ситуацій та аналіз / запобігання ризикам - це тривалий процес.

Мережі. Захист даних та інформації в мережі в межах організації може контролюватися з різним рівнем доступу для входу користувача. Такий крок обмежує доступ для осіб у межах організації та для зловмисних користувачів поза організацією, які, можливо, отримали

доступ. Існують спеціалізовані інструменти, які керують трафіком в мережі; ці інструменти також підкреслять потенційні ризики. Проблема цих інструментів полягає в тому, що вони постійно генерують дані. Завдяки тисячам створених журналів у процесі можуть бути пропущені справжні сповіщення. Завдяки постійному просуванню штучного інтелекту (AI) та машинного навчання програмне забезпечення безпеки може виявити та оповістити про неминучі ризики.

Хмарна безпека. Більше організацій зберігає та обмінюється даними у хмарі, (GSuite для електронної пошти, DropBox та One Drive для зберігання, Office365 для підвищення продуктивності, і т.п.). Це створює подальші проблеми щодо кібербезпеки, а також для нових нормативно-правових актів, таких як GDPR. Погано налаштовані хмарні рішення можуть призвести до кібератак, і це створює істотний ризик. Кібербезпека вже не перебуває під контролем вашої організації. Підприємства покладаються на інших, щоб реалізувати стратегії кібербезпеки. Організації повинні ретельно розглянути окремі хмарні рішення, перш ніж підключатись, провести ретельну перевірку, щоб гарантувати, що ці постачальники також сприйматимуть кібербезпеку серйозно.

Програми. Найбільш вразливою областю для кібербезпеки є веб-програми. З розробниками по всьому світу, що створюють веб-додатки, кожна команда розробників має різні набори навичок та стандарти кодування. Часто розробники не створювали системи з безпечними методами кодування, залишаючи ці системи вразливими та схильними до атак.

Веб-додатки повинні бути протестовані на слабкість безпеки, виконавши тестування Penetration (PEN). Програмне забезпечення, наприклад OWASP або Fortify, визначатиме проблеми у веб-додатках, які можуть вирішувати розробники. Тестування PEN - це не разова процедура; процес повинен повторюватися через певні проміжки часу, коли стають відомі нові методи злому, щоб програмне забезпечення завжди було захищеним.

Інтернет речей (IoT). Може бути пов'язаним з будь-якою системою, до якої можна отримати доступ через Інтернет, наприклад автоматизованим освітленням та опаленням вдома, фітнес-додатками, що відстежують ваші щоденні дії, або датчиком швидкості в автомобільному транспортному засобі для страхової компанії. Системи IoT встановлені, а оновлення програмного забезпечення або безпеки ігноруються. Така поведінка може загрожувати конфіденційності користувачів IoT систем, а також інших, оскільки часто IoT системи є частиною ботнету.

Удосконалення стохастичної моделі загроз пошкодження або несанкціонованого витоку інформації на об'єктах інформаційної діяльності

З метою визначення імовірних загроз системи захисту інформації потрібно визначати максимальні ризики. Тому удосконалимо модель визначення ризиків втрачання або пошкодження інформації

Процес втрачання або пошкодження інформації має випадковий характер тому може бути описаний Стохастичною моделлю. [6,7].

Стохастична модель – це модель де враховуються випадкові фактори. Випадковий процес $X(t)$ це функція, яка в будь-який момент часу t приймає значення, що є випадковою величиною [8]. Оскільки процес виникнення загроз інформації залишається постійним то будемо розглядати Р – схему, в яких t – дискретна величина. Характеристики випадкового процесу це функції аргументу t, а саме:

Математичне очікування $m_x(t)$ – це середня функція, навколо якої відбувається відхилення $X(t)$, тобто функція $m_x(t)$ вже є невипадковою. Значення функції $m_x(t)$ є мат. очікуванням кожного перерізу випадкового процесу $X(t): m_x(t) = M\left[X(t)\right]$, в нашому випадку для дискретного випадкового процесу $M[X] = \sum_i x_i P_i$.

Дисперсія $D_x(t)$. $D_x(t) = M\left[(m_x(t) - X(t))^2\right] = M\left[X^2(t)\right] - x\left[m_x{}^2(t)\right]$ Тобто дисперсія випадкового процесу також невипадкова величина, дисперсія випадкового процесу $X(t)$ в момент часу t [7,9].

Середньоквадратичне відхилення СКО. $\sigma_x(t) = \sigma_x\left[X(t)\right] = \sqrt{D\left[X(t)\right]}$.

Мета даного моделювання – знаходження характеристики вразливості в стаціонарному стані (стаціонарної ймовірності). Якщо за основу брати рівняння Котельникова, то для стаціонарної моделі необхідно взяти до уваги, що похідна постійній є нульова. Тоді рівняння Котельникова для графа приймають вигляд зручний для рішення. Для моделювання скористаємося пакетом прикладних програм Матлаб.

Побудуємо граф перехідних станів для вирішення задачі визначення ймовірності зняття інформації різними методами та принципами в певний випадковий момент часу (рис. 1). Імовірнісні параметри конкретного варіанту пошкодження або несанкціонованого отримання інформації будемо використовувати з бази загроз (данні Інтернет) накопиченої за останні 5 років.

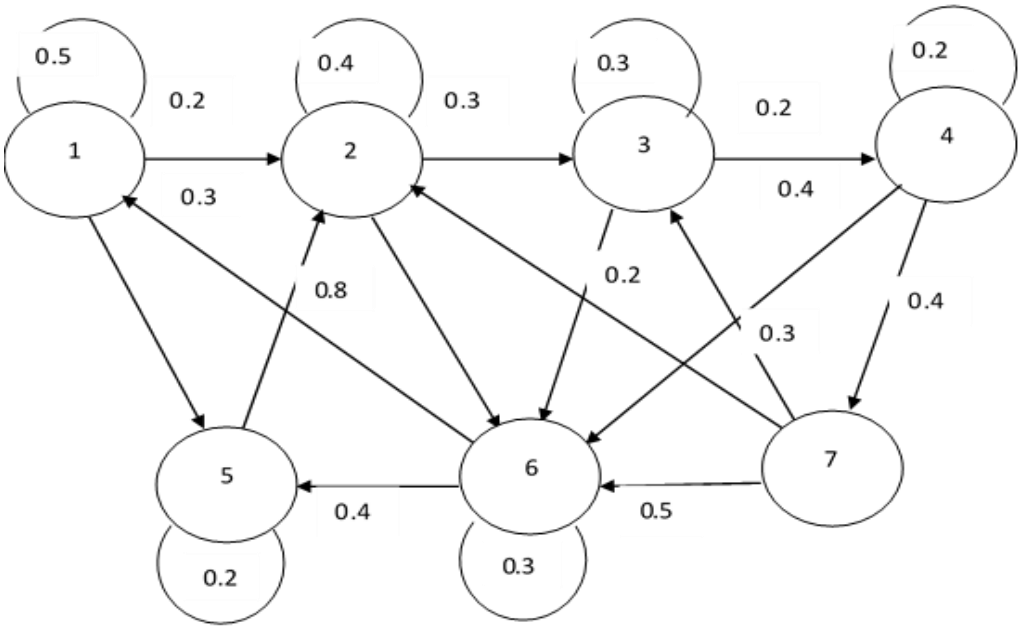

Рис. 1.Граф дискретної ергодичної мережі загрози інформації

Матриця перехідних станів для графу (див. рис. 1) буде матиме вигляд, приведений у табл. 1.

Таблиця 1.

Матриця перехідних станів

	1	2	3	4	5	6	7
1	0.5	0.2	0	0	0.3	0	0
2	0	0.4	0.3	0	0	0.3	0
3	0	0	0.3	0.2	0.3	0.2	0
4	0	0	0	0.2	0	0.4	0.4
5	0	0.8	0	0	0.2	0	0
6	0.3	0	0	0	0.4	0.3	0
7	0	0.2	0.3	0	0	0.5	0

Дані середньостатистичної достовірності для кожної вершини взяті на основі узагальнення досвіду робіт по попередження загроз на протязі останніх 5 років, данні отриманні за рахунок аналізу відкритих даних іноземних компаній.

На графі станів та переходів позначено:

вершина 1 – ймовірність визначення загроз пошкодження або несанкціонованого витоку інформації через Інтернет;

вершина 2 – ймовірність визначення загроз пошкодження або несанкціонованого витоку інформації через мережі об'єкта;

вершина 3 – ймовірність визначення загроз пошкодження або несанкціонованого витоку інформації з використанням хмарної технології;

вершина 4 – ймовірність визначення загроз пошкодження або несанкціонованого витоку інформації програмними втручаннями;

вершина 5 – ймовірність визначення загроз пошкодження або несанкціонованого витоку інформації через персонал

вершина 6 – ймовірність визначення загроз пошкодження або несанкціонованого витоку інформації у інфраструктури об'єкта ;

вершина 7 –. ймовірність визначення загроз пошкодження або несанкціонованого витоку інформації через веб додатки.

$\pi^{(i)} = (1,0,0,0,0,0,0)$ – вектор ймовірностей станів (показує ймовірність того що пошкодження або несанкціонованого отримання інформації буде проведено з використанням методу i-ого стану). $\pi^{(i)}$ це перетин процесу пошкодження або несанкціонованого отримання інформації.

Для знаходження ймовірностей можливих варіантів пошкодження або несанкціонованого отримання інформації, необхідно вирішити систему рівнянь:

$$\begin{cases} \pi_1 = P_{11} \cdot \pi_1 + P_{21} \cdot \pi_2 + ... + P_{n1} \cdot \pi_n \\ \pi_2 = P_{12} \cdot \pi_1 + P_{22} \cdot \pi_2 + ... + P_{1n} \cdot \pi_n \\ ..... \\ \pi_n = P_{1n} \cdot \pi_1 + P_{2n} \cdot \pi_2 + ... + P_{nn} \cdot \pi_n \end{cases}. \quad (1)$$

Запишемо вираз (1) в матричному вигляді:

$$(P^T - E) \cdot \pi = 0, \quad (2)$$

де Е – одинична матриця.

Додаємо до рівнянь (2) умови нормування:

$$\pi_1 + \pi_2 + ... + \pi_n = 1, \quad (3)$$

для вирішення матричних рівнянь (1) і (2) і графічного представлення результатів будемо використовувати пакет програм Матлаб. При цьому обчислення будемо вважати закінченими коли середньоквадратичне відхилення буде менше або дорівнює заданому ε, тобто $(\|\pi^{(n-1)} - \pi^n\|) \le \varepsilon$. Задаємо значення середньоквадратичного відхилення 0,0049 та проведемо моделювання.

Вектор стану для графа (див. рис. 1) та заданого середньоквадратичного відхилення матиме вигляд:

$$\pi = \left| 0.1190 \quad 0.3040 \quad 0.1361 \quad 0.0340 \quad 0.1949 \quad 0.1984 \quad 0.0136 \right|. \qquad (4)$$

Графік середньоквадратичних відхилень від заданого значення представлено на рис. 2.

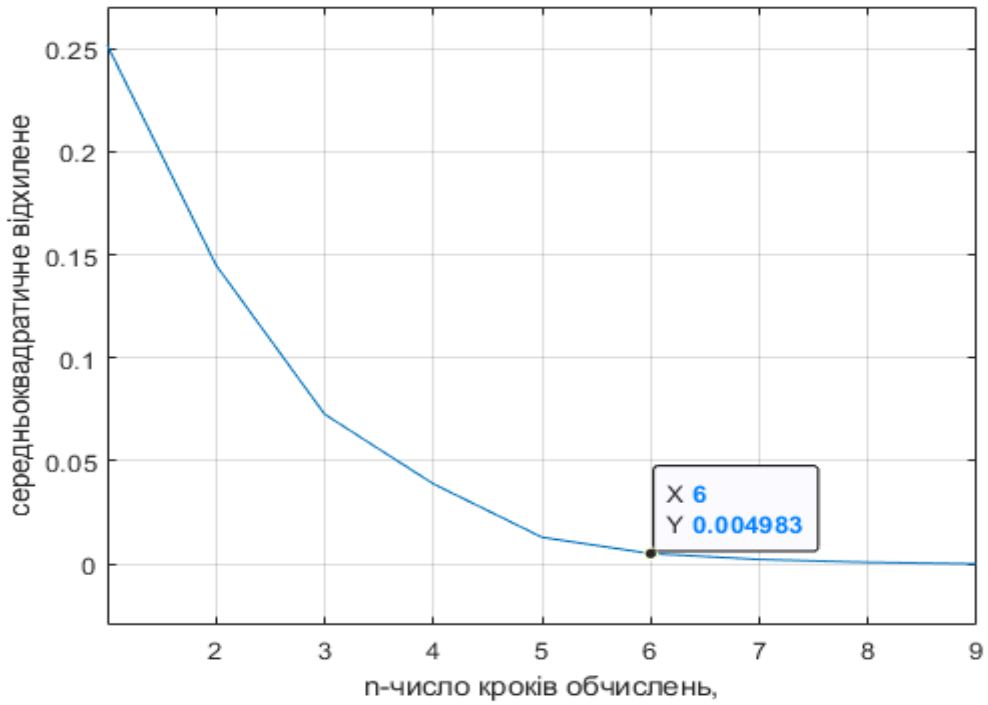

Рис. 2. Графік середньоквадратичних відхилень від заданого значення

З отриманих в результаті моделювання результатів, вектор ймовірностей для кожної із загроз пошкодження або несанкціонованого витоку інформації наведено в матриці (табл. 1), причому результати моделювання не залежать від початкового положення вектору стану. Тобто можливо зробити висновок, що на сучасному етапі пошкодження або несанкціонованого витоку інформації може бути проведений з найбільшою ймовірністю через загрози мережі об'єктів, на другому місці йде загроза пошкодження або несанкціонованого витоку інформації через персонал, далі через загрози інфраструктури. Останні загрози пошкодження або несанкціонованого витоку інформації:

загроза пошкодження або несанкціонованого витоку інформації з використанням хмарної технології

загроза пошкодження або несанкціонованого витоку інформації програмними втручаннями;

загроза пошкодження або несанкціонованого витоку інформації програмними втручаннями;

загроза пошкодження або несанкціонованого витоку інформації через веб-додатки.

Мають саму низьку ймовірність та враховуються у останню чергу.

Але з метою забезпечення інформаційної безпеки потрібно ще враховувати та провести наступні засоби:

Стандартизовані моделі процесів для системного підходу, які закріплені в повному процесі розробки. Це починається на етапі аналізу вимог і продовжується від розробки та розробки до тестування та інтеграції компонентів та мережі.

Швидкі оновлення програмного забезпечення для усунення вразливості програмного забезпечення ECU.

Надійні протоколи, які є сучасними та відповідають довгостроковим вимогам безпеки. Що стосується безпеки, це часто поєднується з криптографічними ключами. Тому необхідно підтримувати ключове управління протягом життєвого циклу транспортного засобу.

Внутрішні мережі та системна архітектура, які забезпечують гнучкість та масштабованість, розроблені з урахуванням аспектів безпеки.

На основі закордонного досвіду додатково показали, які інженерно-технічні заходи необхідні для створення захищених інформаційних систем.

Висновки

У результаті аналітичного аналізу загроз пошкодження або несанкціонованого витоку інформації на об’єктах інформаційної діяльності визначили критичні складові безпеки інформаційного простору. Провели додаткові аналітичні порівняння існуючих загроз на основі даних закордонних аналітиків. Отримали незначні відхилення, тобто підтвердили чітко визначенні нами критичні складові загроз пошкодження або несанкціонованого витоку інформації.

На основі отриманих аналітичних даних удосконалено стохастичну модель загроз пошкодження або несанкціонованого витоку інформації на об’єктах інформаційної діяльності.

З метою визначення пріоритетів провели моделювання. На основі результатів моделювання за допомогою удосконаленої стохастичної моделі, отримали наступні результати:

1. результати моделювання не залежать від початкового положення вектору стану
2. на сучасному етапі пошкодження або несанкціонованого витоку інформації може бути проведений з найбільшою ймовірністю через загрози мережи об’єктів інформаційної діяльності, на другому місці йде загроза пошкодження або несанкціонованого витоку інформації через персонал, далі через загрози інфраструктури об’єкта.

Отримані результати дозволяють планувати систему інформаційної безпеки з врахування найбільш імовірних загроз. Планувати та впроваджувати першочергові заходи інформаційної безпеки. Зосереджувати кошти для захисту більш ймовірних напрямків загроз.

Перелік посилань

1. Лаптєв О.А. Модель інформаційної безпеки на основі марковських випадкових процесів. Науково-практичний журнал «Зв'язок». К.: ДУТ,2018. №6(136), С.45 – 49.
2. Laptiev.O., Shuklin G., Stefurak O., Svynchuk O., Urdenko O., Hohoniants S. Metod of the increasing the detection system and recognition of digital radiosignals. East European Scientific Journal, Poland, , № 2 (54), 2020 part 5, P.4– 17.
3. Щеглов К. А., Щеглов А. Ю. Эксплуатационные характеристики риска нарушений безопасности информационной системы. Научно-технический вестник информационных технологий, механики и оптики. 2014. №1(89). С. 129–139.
4. Богданович В.Ю., Алексєєв М.М. Методологічний підхід до обґрунтування режимів функціонування системи забезпечення кібернетичної безпеки України. Сучасний захист інформації. 2013. № 4. С. 68 – 77.
5. Браіловський М.М., Лазарєв Г.П., Хорошко В.О. Захист інформації у банківській діяльності. К: ТОВ “Поліграф Консалтинг”, 2004. 216 с.
6. Вентцель Е.С., Овчаров Л.А. Теория вероятностей и ее инженерные приложения. М.: Наука, 1988. 480 с.
7. Лаптєв О.А. Уразливість інформаційної системи як основний елемент моделювання схем інформаційної безпеки. Тези доповідей: XIII Міжнародна науково-технічна конференція «Проблеми інформатизації», м. Київ, ДУТ, 11 – 12 квітня 2019 р. С. 5.
8. Грищук Р.В. Бурячок В.Л., Мамарєв В.М. Науково-технічне обґрун-тування вибору підходу до формування множини інформативних параметрів для систем захисту інформації. Специальные телекоммуникационные системы и защита информации. 2014. № 2 (26). С. 82 – 86.

9. Державний стандарт України ДСТУ 3396.0-96 "Захист інформації. Технічний захист інформації. Основні положення".

10. Лаптєв О.А., Степаненко В.І., Тихонов Ю.О. Формальні математичні моделі для забезпечення безпеки інформації. Сучасний захист інформації: науково-технічний журнал. К.: ДУТ, 2019. № 1. С. 59 – 64.

11. Державний стандарт України ДСТУ 3396.1-96 "Захист інформації. Технічний захист інформації. Порядок проведення робіт".

12. Доктрина інформаційної безпеки України [Електронний ресурс]. – Режим доступу: URL: https://www.president.gov.ua/documents/472017–21374.

13. Забара С. Характеристики моделювання систем у середовищі MATLAB. К.: Вид. Университет "Украина", 2011. 137 с.

14. Закон України “Про Державну службу спеціального зв’язку та захисту інформації України”.

.

Надійшла: 15.03.2020 Рецензент: д.т.н., професор Кожухівський А.Д.