УДК 004.415.056.5(075) DOI https://doi.org/10.35546/kntu2078-4481.2024.2.33

Н. О. ФЕСЬОХА
доктор філософії,
старший викладач кафедри комп'ютерних інформаційних технологій
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут
ORCID: 0000-0002-9797-5589

СТАН ТА ТЕНДЕНЦІЇ РОЗВИТКУ КІБЕРБЕЗПЕКИ В ЕПОХУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ – АНАЛІЗ СУЧАСНИХ ЗАГРОЗ ТА ЗАХОДІВ ЗАХИСТУ

В статті наголошено, що кібератаки стають все більш поширеними і небезпечними в сучасному світі інформаційних технологій. Вони можуть призвести до серйозних наслідків для організацій та приватних осіб, включаючи крадіжку особистих даних, фінансові втрати, порушення конфіденційності, переривання бізнес-процесів і навіть загрозу національній безпеці. Щоб захиститися від кібератак, необхідно використовувати сучасні методи захисту та профілактичні заходи. Це включає в себе регулярне оновлення програмного забезпечення і антивірусних програм, навчання співробітників організацій безпеки інформації, використання багатофакторної аутентифікації і шифрування даних. Безпека інформації є ключовим питанням в сучасному світі, і важливо вживати всіх необхідних заходів для захисту себе і своєї організації від кіберзагроз.

Математичне забезпечення таких систем включає моделі процесів атаки на механізми захисту та блокування або усунення кіберзагроз. Описано модель для множин процесу захисту інформації з повним перекриттям загроз. Зроблено узагальнення про те, що система захисту інформації і кібербезпеки – це складний комплекс програмних, криптографічних, організаційних та інших засобів, методів і заходів призначених для захисту інформації та кібербезпеки.

Кібербезпека на державному рівні має спиратися на реалізацію функцій органів державної влади, які забезпечують національну кібербезпеку, впровадження стратегії, національної політики та сучасного ефективного інструментарію кіберзахисту. Зроблено висновок, що серед першочергових завдань, які стоять перед державними інститутами України в рамках забезпечення інформаційного та цифрового суверенітетів, є: здійснення автоматичного моніторингу свого інформаційного простору; впровадження законодавства про відповідальність за контент; впровадження законодавства, яке регулює фільтрацію інтернет-контенту; недопущення використання новітніх інформаційних технологій для поширення соціально шкідливих ідей і закликів.

Ключові слова: *безпека, державна безпека, шифрування, інформаційна безпека, інформаційний захист, цифрова трансформація.*

N. O. FESOKHA
PhD, Senior Lecturer at the Department of Computer Information Technologies
Kruty Heroes Military Institute of Telecommunications
and Information Technology
ORCID: 0000-0002-9797-5589

THE STATE AND TRENDS OF CYBERSECURITY DEVELOPMENT IN THE ERA OF DIGITAL TRANSFORMATION – ANALYSIS OF CURRENT THREATS AND PROTECTION MEASURES

The article emphasizes that cyberattacks are becoming increasingly widespread and dangerous in today's world of information technology. They can lead to serious consequences for organizations and individuals, including personal data theft, financial losses, confidentiality breaches, disruption of business processes, and even threats to national security. To protect against cyberattacks, it is necessary to use modern security methods and preventive measures. This includes regularly updating software and antivirus programs, training organizational staff in information security, using multi-factor authentication, and data encryption. Information security is a key issue in the modern world, and it is important to take all necessary measures to protect oneself and one's organization from cyber threats.

Mathematical support for such systems includes models of attack processes on defense mechanisms and blocking or eliminating cyber threats. A model for sets of information protection processes with complete threat coverage is described. It is generalized that the information security and cybersecurity system is a complex combination of software, cryptographic, organizational, and other means, methods, and measures designed to protect information and cybersecurity.

Cybersecurity at the state level should rely on the implementation of functions of state authorities responsible for national cybersecurity, the implementation of strategies, national policies, and modern effective cyber defense tools. It is concluded that among the priority tasks facing Ukrainian state institutions in ensuring information and digital sovereignty are: automatic monitoring of their information space; implementation of legislation on liability for content; implementation of legislation regulating internet content filtering; prevention of the use of advanced information technologies for the dissemination of socially harmful ideas and calls.

Key words: *security, national security, encryption, information security, information protection, digital transformation.*

Постановка проблеми

На сьогоднішній день IT-ринок наповнений значною кількістю технологій, кожна з яких спрямована на покращення будь-якого аспекту роботи з інформаційними ресурсами, будь то зберігання, обробка або передача даних. Володіючи рядом серйозних переваг, дані тенденції представляють собою ще більший обсяг загроз і уразливостей. Вихід кожної наступної вдосконаленої версії продукту тягне за собою певні уразливості, які могли вже надаватися з первісною версією, а часто з'являються ще й додаткові уразливості. Це лише сприяє все більшому проникненню в корпоративні мережі, крадіжці інформації та інших негативних моментів. Існуюча значна кількість інформаційних джерел, легко доступних допоміжних програмних засобів сприяє збільшенню інтересу до чужої інформації, серверів, станцій, комп'ютерів. До основних загроз безпеки інформації та нормального функціонування ІС відносяться: витік конфіденційної інформації; компрометація інформації; несанкціоноване використання інформаційних ресурсів; помилкове використання інформаційних ресурсів; несанкціонований обмін інформацією між абонентами; відмова від інформації; порушення інформаційного обслуговування; незаконне використання привілеїв.

Швидкий розвиток інформаційних загроз в сучасному світі спонукав проведення різних систематичних досліджень, спрямованих на вивчення найбільш ефективних методів боротьби і запобігання загроз, трансляцію накопиченого досвіду в питаннях управління інформаційною безпекою.

Аналіз останніх досліджень і публікацій

Важливості питань інформаційної безпеки нашої країни і формуванню механізму кібербезпеки приділяли увагу праці таких науковців, як Капітон А. [3], Капля О. М. [4], Мальцева І. Р. [6], Ткач Ю. [7]. Проте ці дослідження здебільшого зосереджені на сфері правового регулювання та формування системи інформаційної безпеки України.

Формулювання мети дослідження

Мета дослідження полягає в аналізі стану та головних тенденцій розвитку кібербезпеки в епоху цифрової трансформації.

Викладення основного матеріалу дослідження

Перелік інформаційних загроз в наш час дуже широкий і їх список щодня розширюється. Сьогодні ці загрози можна поділити на дві основні групи: внутрішні і зовнішні.

Зовнішні загрози виходять з «зовнішнього світу» (зазвичай з мережі Інтернет), тоді як внутрішні загрози виходять з самої організації. Сьогодні також виділяють ще й деяку «проміжну» групу загроз, які пов'язані з роботою провайдерів послуг. Цими послугами користуються організації, і вони доповнюють її інформаційні ресурси.

Внутрішні загрози. Згідно даних Глобального дослідження тенденцій інформаційної безпеки помітна тенденція зростання внутрішніх загроз від колишніх співробітників компаній. При цьому, серед усіх джерел загроз найбільший приріст (58%), в порівнянні з попереднім роком, був відзначений у інцидентів, що пов'язані з колишніми постачальниками послуг і сервісів. Незважаючи на це необхідно відзначити, що помітна тенденція спаду кількості інцидентів інформаційної безпеки (ІБ) щодо діючих співробітників. Такий немаловажний факт, як витік інформації або її поширення з вини чинного співробітника досі актуальний і передбачається, залишиться таким, поки існує конкуренція і суперництво.

Причиною стрімкого зростання рівня внутрішніх загроз є швидке зростання кількості мобільних пристроїв і популярності хмарних обчислень, що істотно розширює горизонт атак. З появою принципово нових пристроїв і інфраструктур перед зловмисниками відкриваються нові можливості атак, що використовують непередбачені слабкі місця і погано захищені ресурси. Так само, повсюдний доступ з мобільних пристроїв до службової інформації компанії або до інформації, яка може зацікавити конкуруючу сторону, збільшує ризик її розкрадання [2].

Таким чином, компанії збільшуючи зростання безконтрольного застосування мобільних пристроїв для скорочення часу виконання завдань і функцій, збільшують імовірнісний відсоток навмисного розкрадання конфіденційних даних або атаки на внутрішні інформаційні ресурси.

Зовнішні загрози. На практиці зустрічаються різні типи шкідливого програмного забезпечення, використовуваного зловмисниками для отримання доступу до корпоративних мереж. Аналіз наукової літератури показав, що найчастіше зустрічається таке шкідливе програмне забезпечення (ПЗ): рекламне, шпигунське, програми небажаного перенаправлення, експлойти, що використовують iFrame, і програми фішингу [1].

Список ПЗ можна розглядати як програмні коди, що використовуються для отримання початкового доступу. Це найбільш економічні способи, що дозволяють з легкістю скомпрометувати великі обсяги користувачів. Існує багато різних типів кібератак, кожен з яких має свої унікальні характеристики та цілі. Деякі з найбільш поширених типів кібератак включають:

1. Віруси – це програми, які можуть заражати комп'ютери та інші пристрої, поширюватися через мережі та завдавати різних видів шкоди, таких як знищення даних, блокування роботи системи та навіть крадіжка конфіденційної інформації. На сьогоднішній день відомо більше 45000 вірусів, і їх число продовжує збільшуватися. Джерелами вірусної загрози є електронна пошта, переважна більшість вірусів проникає за допомогою послань через e-mail.

2. Черв'яки – це програми, які здатні поширюватися самостійно через мережі і заражати безліч комп'ютерів. Вони можуть завдати серйозної шкоди, блокуючи роботу системи та видаляючи файли [5].

3. Троянські коні – це програми, які можуть маскуватися під звичайні файли та заражати комп'ютери, надаючи зловмисникам віддалений доступ до пристрою та конфіденційної інформації.

4. Фішинг – це атака, яка призначена для отримання конфіденційної інформації, такої як паролі та номери кредитних карток, шляхом обману користувачів та надання їм неправдивої інформації.

5. DDoS-атаки – це атаки, які спрямовані на блокування роботи системи шляхом перевантаження її трафіком, що унеможливлює доступ до ресурсу. Прикладом може бути атака на сайт компанії Twitter в 2016 році, коли ботнет Mirai перевантажив сайт і його сервіси [8].

6. Атаки на інфраструктуру – це атаки, спрямовані на руйнування фізичної інфраструктури, такої як електронні системи управління транспортом або електроживлення.

Крім того, існують і інші типи кібератак, такі як атаки на мобільні пристрої, атаки на хмарні сховища даних і багато інших. Важливо розуміти, що кожен тип кібератаки має свої унікальні методи та інструменти, і необхідно вжити відповідних заходів захисту, щоб запобігти їх проведенню та захистити свою систему та конфіденційну інформацію [9].

Експлойти JavaScript та шахрайство у Facebook (соціальна інженерія) виявилися найбільш використовуваними методами атаки. Не можна виключати і того факту, що до більшого ризику схильні компанії, що займаються фінансовою діяльністю, що оперують конфіденційними даними або ж надають різні інформаційно-комунікаційні послуги широкому колу користувачів мережі Інтернет. Зловмисники крадуть цінні дані або утримують під контролем цифрові активи користувачів заради викупу. Виходячи з усього, при відстеженні шкідливого ПЗ з Інтернету, недостатньо просто зосереджуватися на найбільш поширених типах загроз, необхідно розглядати повний спектр атак при організації захисту інформаційних ресурсів і проведення оцінки ефективності її роботи по закінченню заданого періоду часу роботи [3].

Метою визначення загроз безпеці інформації є встановлення того, чи існує можливість порушення конфіденційності, цілісності або доступності інформації, що міститься в інформаційній системі, і чи призведе це порушення хоча б однієї із зазначених властивостей безпеки інформації до настання неприйнятних негативних наслідків для володаря інформації або оператора, а в разі обробки персональних даних і для суб'єктів персональних даних.

Визначення загроз безпеці інформації повинно носити систематичний характер і здійснюватися як на етапі створення інформаційної системи та формування вимог щодо її захисту, так і в ході експлуатації інформаційної системи. Систематичний підхід до визначення загроз безпеці інформації необхідний для того, щоб визначити потреби в конкретних вимогах до захисту інформації та створити адекватну ефективну систему захисту інформації в інформаційній системі. Заходи захисту інформації, що вживаються власником інформації і оператором, повинні забезпечувати ефективне і своєчасне виявлення і блокування (нейтралізацію) загроз безпеки інформації, в результаті реалізації яких можливе настання неприйнятних негативних наслідків (збитку).

Проаналізуємо особливості математичного аналізу кіберзагроз. Нехай на інформаційну систему (ІС) в довільний момент часу t_i впливає і загроза. В результаті такого впливу ІС переходить із стану S_0 в стан S_i.

Нехай в момент часу $t<t_0$ ІС перебувала в стаціонарному стані попередньому впливу і загрози. Такий стан характеризує передісторію процесу-минулий стан ІС до моменту часу t_0. У момент часу t_0 на ІС впливає і загроза, в результаті якої ІС за час $t_1 = t_0 + \tau$ переходить із стану S_0 – о в стан $S_{1\text{-}e}$. Якщо такий процес відповідає випадковому процесу, то можна передбачити такий перехід, враховуючи тільки даний стан ІС-S_0 і, забувши про її передісторії. Сам стан S_0 залежить від минулого, але як тільки він буде досягнутим, про минулий стан можна забути.

Отже, випадковий процес стосовно ІС називається Марковським, якщо для будь-якого моменту часу t_0 імовірнісні характеристики ІС в майбутньому залежать тільки від її стану в даний момент t_0 і не залежать від того, коли і як ІС прийшла в цей стан.

Постановка задачі. Нехай на ІС за кінцевий час τ впливає n найпростіших потоків загроз з інтенсивностями λ_i, i = 1, n. Нехай μ_i – інтенсивність парирування наслідків і загрози. Відповідно, R – ймовірність виявлення, а R_i – ймовірність не виявлення і загрози. Тоді, μ_i*R – інтенсивність парирування, а μ_i*R_i – інтенсивність не парирування наслідків впливу на ІС потоку загроз.

Припущення: потік виявлення і не виявлення загрози найпростіший; можливості по виявленню наслідків впливу на ІС і загрози необмежені, тобто $\mu_i \geq \lambda_i$; так як розглядаються найпростіші потоки, то поява одночасно двох і більше загроз є неможливою подією.

Для визначення ймовірності позитивного результату при впливі на ІС потоку N загроз представимо ІС у вигляді графа (рис. 1). Відповідно до рис. 1 можна скласти матрицю інтенсивностей переходу виду.

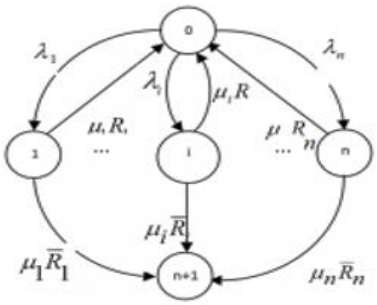

Рис. 1. Граф стану ІС

$$\|\lambda_{ik}\| = \begin{vmatrix} -\lambda_0 & \dots & \lambda_i & \dots & \lambda_n & 0 \\ \mu_i \cdot R_i & \dots & -\mu_i & \dots & 0 & \mu_i R_i \\ \mu_n \cdot R_n & \dots & 0 & \dots & -\mu_n & \mu_n \cdot \bar{R}_n \\ 0 & \dots & 0 & \dots & 0 & \dots 0 \end{vmatrix}, \quad (1)$$

де $\lambda = \lambda + \lambda + \dots + \lambda_n$; $j = k = 1,2,\dots,n+2$.

Відповідно до рис. 1 ІС в момент часу τ може перебувати в одному з наступних станів:

стан «0» – потік загроз за час τ не проявився;

стан «1»,..., i,..., n – одна із загроз проявилася;

стан «n-1» – неблагополучний поглинаючий стан, при якому загроза реалізувалася.

Матриця володіє наступними властивостями: діагональні члени матриці рівні сумі інших елементів даного рядка, взятих із зворотним знаком; сума всіх елементів кожного рядка дорівнює нулю; число нульових рядків в матриці інтенсивностей переходів відповідає кількості поглинаючих станів; інтенсивність переходу дорівнює нулю при відсутності стрілки.

Для визначення ймовірностей переходу ІС в кожен можливий стан скористаємося системою диференціальних рівнянь, відповідно до яких можна написати:

$$\frac{dP_0(\tau)}{d\tau} = -P_0(\tau)\sum_{i=1}^{n}\lambda_i + \sum_{i=1}^{n}\mu_i R_i P_i(\tau); \quad (2)$$

$$\frac{dP_i(\tau)}{d\tau} = \lambda_i P_0(\tau) - \mu_i P_i(\tau); \quad (3)$$

$$\frac{dP_{n+1}(\tau)}{d\tau} = \sum_{i=1}^{n}\mu_i \bar{R}_i P_i(\tau). \quad (4)$$

Застосовуючи до системи диференціальних рівнянь пряме перетворення Лапласа з урахуванням вихідних даних $P_0(0) = 1$, $P_i(0) = P_{n+1}(0) = 0$ і з урахуванням того, що $\int_0^\infty P_i(\tau)e^{-St}d\tau = -P_i(0) + SP_j(S)$, отримаємо наступні вирази для визначення ймовірностей відповідно до графу станів:

$$-P_0(0) + SP_0(S) = -\lambda_0 P_0(S) + \sum_{i=1}^{n}\mu_i R_i P_i(S); \quad (5)$$

$$-P_i(0) + SP_i(S) = \lambda_i P_0(S) - \mu_i P_i(S); \quad (6)$$

$$-P_{n+1}(0) + SP_{n+1}(S) = \sum_{i=1}^{n}\mu_i \bar{R}_i(S). \quad (7)$$

Де $P_i(S) = \int_0^\infty P_i(\tau)e^{-St}d\tau$ – шукане зображення.

При початкових умовах система рівнянь набуде вигляду:

$$(S + \lambda_0)P_0(S) = \sum_{i=1}^{n}\mu_i R_i(S) = 1; \quad (8)$$

$$-\lambda_i P_0(S) + (S + \mu_i)P_i(S) = 0; \quad (9)$$

$$-\sum_{i=1}^{n}\mu_i R_i P_i(S) + SP_{n+1}(S) = 0. \quad (10)$$

За правилом Крамера шукані зображення визначаються відношенням:

$$P_j(S) = \frac{\Delta_j(S)}{\Delta(S)}, j = 1, n. \quad (11)$$

Де $\Delta(S) = S[(S + \lambda_0)\prod_{i=1}^{n}(S + \mu_i) - \sum_{i=1}^{n}\lambda_i\mu_i R_i \prod_{i=1}^{n}(S + \mu_i)]$ – головний визначник системи;

$\Delta_j(S)$ – приватний визначник системи, знаходиться з головного визначника шляхом заміни j-го стовпця коефіцієнтами, що стоять в правих частинах рівнянь.

Окремі визначники, отримані за допомогою введення визначників по індукції, будуть рівні:

$$\Delta_0(S) = S\prod_{i=1}^{n}(S+\mu_i) \tag{13}$$

$$\Delta_i(S) = S\lambda_0\prod_{i=1}^{n}(S+\mu_i) \tag{14}$$

$$\Delta_{n+1}(S) = \sum_{i=1}^{n}\lambda_i\mu_i R_i\prod_{i=1}^{n}(S+\mu_i). \tag{15}$$

З урахуванням зазначеного і за умови, що $\rho_i(S) = \frac{\Delta_i(S)}{S}$, $\rho(S) = \frac{\Delta(S)}{S}$ система рівнянь набуде вигляду:

$$P_0(S) = \frac{q_0(S)}{\rho(S)} = \frac{\Delta_0(S)S}{S\Delta(S)} = \frac{\Delta_0(S)}{\Delta(S)} \tag{16}$$

$$P_i(S) = \frac{q_i(S)}{\rho(S)} = \frac{\Delta_i(S)S}{S\Delta(S)} = \frac{\Delta_i(S)}{\Delta(S)} \tag{17}$$

$$P_{n+1}(S) = \frac{q_{n+1}(S)}{\rho(S)} = \frac{\Delta_{n+1}(S)S}{S\Delta(S)} = \frac{\Delta_{n+1}(S)}{\Delta(S)} \tag{18}$$

Остаточно робоча формула буде мати такий вигляд:

$$P_0(S) = \frac{\prod_{i=1}^{n}(S+\mu_i)}{[(S+\lambda_0)\prod_{i=1}^{n}(S+\mu_i)-\sum_{i=1}^{n}\lambda_i\mu_i R_i\prod_{i=1}^{n}(S+\mu_i)]} \tag{19}$$

$$P_i(S) = \frac{\lambda_0\prod_{i=1}^{n}(S+\mu_i)}{[(S+\lambda_0)\prod_{i=1}^{n}(S+\mu_i)-\sum_{i=1}^{n}\lambda_i\mu_i R_i\prod_{i=1}^{n}(S+\mu_i)]} \tag{20}$$

$$P_{n+1}(S) = \frac{\sum_{i=1}^{n}\lambda_i\mu_i R_i\prod_{i=1}^{n}(S+\mu_i)}{[(S+\lambda_0)\prod_{i=1}^{n}(S+\mu_i)-\sum_{i=1}^{n}\lambda_i\mu_i R_i\prod_{i=1}^{n}(S+\mu_i)]}. \tag{21}$$

Тоді випливає, що ймовірність благополучного результату від впливу на ІС n незалежних потоків внутрішніх загроз визначається наступним виразом: $P_{БІ}(\tau) = \sum_{i=1}^{n} P_{,}(\tau)$, а ймовірність протилежної події, тобто неблагополучного результату, буде дорівнює $P_{БІ}(\tau) = 1 - \sum_{i=1}^{n} P_{,}(\tau) = P_{n+1}(\tau)$.

Окремий випадок: інтенсивність парирування і-го потоку загрози μ_i дорівнює інтенсивності впливу і-го потоку загрози λ_i. Нехай $\mu_i = \lambda_i$, тобто інтенсивність парирування наслідків і-го потоку загроз дорівнює інтенсивності і-го потоку загроз. Тоді зображення ймовірностей можна представити наступним чином:

$$P_0(S) = \frac{\prod_{i=1}^{n}(S+\mu_i)}{[(S+\lambda_0)\prod_{i=1}^{n}(S+\mu_i)-\sum_{i=1}^{n}\lambda_i^2\mu_i R_i\prod_{i=1}^{n}(S+\mu_i)]} \tag{22}$$

$$P_i(S) = \frac{\lambda_0\prod_{i=1}^{n}(S+\mu_i)}{[(S+\lambda_0)\prod_{i=1}^{n}(S+\mu_i)-\sum_{i=1}^{n}\lambda_i^2\mu_i R_i\prod_{i=1}^{n}(S+\mu_i)]} \tag{23}$$

$$P_{n+1}(S) = \frac{1}{S}\sum_{i=1}^{n}\lambda_i\bar{R}_i P_i(S) \tag{24}$$

Функції $q_i(S)$ і c_i (S) можуть бути представлені у вигляді поліномів з коефіцієнтами b_i і c_i, а саме:

$$q_0(S) = S^n + b_{n-1}S^{n-1}+,\dots,b_1S + b_0 \tag{25}$$

$$q_i(S) = S^{n-1} + b_{n-2}S^{n-2}+,\dots,b_1S + b_0 \tag{26}$$

$$\rho(S) = S^{n+1} + c_nS^n+,\dots,c_1S + c_0 \tag{27}$$

З виразу випливає, що зображення ймовірностей P_j (S) є правильними раціональними дробами, у яких ступеня поліномів чисельників чисельно менше поліномів знаменників.

Тоді застосовуючи табличне перетворення Лапласа, отримаємо наступний вираз для характеристичних оригіналів шуканих ймовірностей:

$$G^{-1}\left(P_j(S)\right) = \begin{cases} \sum_{k=1}^{\omega}\frac{1}{\rho'_j(S_k)}e^{S_k\tau}, \text{если } P_j(S) = \frac{a}{\rho_i(S)}; \\ \sum_{k=1}^{\omega}\frac{q_j(S_k)}{\rho'_j(S_k)}e^{S_k\tau}, \text{если } P_j(S) = \frac{q_i(S)}{\rho_i(S)}; \\ a\left[\frac{1}{\rho(0)} + \sum_{k=1}^{\omega}\frac{1}{S_k\rho'_j(S_k)}e^{S_k\tau},\right], \text{если } P_j(S) = \frac{a}{S\rho_i(S)}. \end{cases} \tag{28}$$

Де ω – кількість коренів і-го характеристичного рівняння.

Тоді з урахуванням нормованої умови $\sum_{i=1}^{n} P_i = 1$, де p_i – ймовірність знаходження ІС в і-му стані, можна записати, що кінцева ймовірність:

$$P_{БІ}(\tau) = \sum_{i=1}^{n} P_j(\tau), \quad (29)$$

характеризує благополучний і неблагополучний результат.

$$Q_{БІ}(\tau) = 1 - \sum_{i=1}^{n} P_i(\tau) = P_{n+1}(\tau). \quad (30)$$

Таким чином, одним з основних методів захисту від кібератак є використання комплексних систем безпеки, які включають в себе антивірусне ПЗ, міжмережеві екрани, системи виявлення вторгнень і багато інших технологій.

В цілому, ефективний захист від кібератак вимагає комплексного підходу, який включає в себе використання різних технологій, навчання користувачів і підтримку спеціальних служб. Тільки так можна досягти високого рівня безпеки і захистити інформацію від кіберзагроз.

Деякі приклади сучасних методів захисту від кібератак включають:

багатофакторна автентифікація – це метод, який вимагає від користувача кількох форм автентифікації, таких як пароль та код, що надісланий на мобільний телефон або електронну пошту. Це ускладнює для зловмисників доступ до системи;

криптографія – шифрування даних може допомогти захистити конфіденційність інформації. Криптографічні алгоритми використовуються для захисту даних у дорозі та в сховищі;

файрволи – це програмні або апаратні пристрої, які моніторять і фільтрують вхідний і вихідний трафік в комп'ютерній мережі. Файрволи можуть бути налаштовані для блокування доступу до певних сайтів або додатків;

оновлення безпеки: оновлення програмного забезпечення, такі як патчі безпеки, можуть закривати вразливості, які можуть бути використані зловмисниками. Оновлення слід встановлювати якомога швидше після їх випуску;

моніторинг безпеки – це процес безперервного моніторингу мережі та систем на наявність можливих загроз. Можна використовувати спеціалізовані програми і пристрої, щоб відстежувати активність в мережі і виявляти підозрілу діяльність.

Висновки

Проаналізовано стан та перелічено головні тенденції розвитку кібербезпеки в епоху цифрової трансформації. Констатовано, що серед першочергових завдань, які стоять перед державними інститутами України в рамках забезпечення інформаційного та цифрового суверенітетів, є: здійснення автоматичного моніторингу свого інформаційного простору; впровадження законодавства про відповідальність за контент; впровадження законодавства, яке регулює фільтрацію інтернет-контенту; недопущення використання новітніх інформаційних технологій для поширення соціально шкідливих ідей і закликів (расизму, шовінізму, радикального націоналізму); правовий захист національної культури і мови від впливу домінуючих в інформаційному плані країн; знаходження соціально прийнятного балансу між свободою слова і поширенням інформації та невід'ємним правом держави забезпечувати незалежну політику; захист від культурної експансії зарубіжних інтернет-ресурсів; перехід державних установ на використання програмного та технічного забезпечення власної розробки і виробництва.

Список використаної літератури

1. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»: Указ Президента України від 19 березня 2022 року № 152/2022 URL: https://zakon.rada.gov.ua/go/152/2022. Дата звернення: 26.03.2024.

2. Дрозд І., Маковець О. Кібербезпека як фактор фінансової безпеки підприємства. *Економіка. Фінанси. Право*. 2020. № 5/3, С. 31–35.

3. Капітон А. Перспективи розвитку кіберпростору та його соціально-психологічні наслідки. *Системи управління, навігації та зв'язку. Збірник наукових праць*. Полтава: ПНТУ, 2021. Т. 3 (65). С. 89–91. doi: https: //doi. org/ 10.26906/SUNZ.2021.3.089.

4. Капля О. М. Правове регулювання інформаційної безпеки громадянина під час дії воєнного стану. *Експерт: парадигми юридичних наук і державного управління.* 2023. № 6 (24). С. 16–20. doi: https://doi.org/ 10.32689/2617-9660-2022-6(24)-16-20.

5. Легомінова С., Гайдур Г. Аналіз сучасних загроз інформаційній безпеці організацій та формування інформаційної платформи протидії їм. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2023. № 2(22), С. 54–67. https://doi.org/10.28925/2663-4023.2023.22.5467.

6. Мальцева І. Р. Аналіз деяких кіберзагроз в умовах війни. *Кібербезпека: освіта, наука, техніка.* 2022. № 4 (16). С. 37–43. doi: 10.28925 / 2663–4023.2022.16.3744.

7. Ткач Ю. Концептуальна модель безпеки кіберпростору. *Технічні науки та технології.* 2021. № 4 (22). С. 96–108. https: // doi. org / 10.25140 / 2411–5363–2020–4 (22) – 96–108.

8. Khlaponin Y., Kozubtsova, L., Kozubtsov, I., Shtonda, R. Функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2022. № 3(15), С. 124–134. https://doi.org/10.28925/2663-4023.2022.15.1241341.

9. Onyshchenko S., Hlushko A. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. *Науковий журнал «Економіка і регіон»*, 2022. № 1(84), С. 13–20. https://doi.org/https://doi.org/10.26906/EiR.2022.1(84).2540.

References

1. Pro rishennja Rady nacionaljnoji bezpeky i oborony Ukrajiny vid 18 bereznja 2022 roku «Shhodo realizaciji jedynoji informacijnoji polityky v umovakh vojennogho stanu»: Ukaz Prezydenta Ukrajiny vid 19 bereznja 2022 roku # 152/2022. URL: https://zakon.rada.gov.ua/go/152/2022. Data zvernennja: 26.03.2024.

2. Drozd, I., Makovecj, O. (2020). Kiberbezpeka jak faktor finansovoji bezpeky pidpryjemstva. *Ekonomika. Finansy. Pravo*. 5/3, 31–35.

3. Kapiton, A. (2021). Perspektyvy rozvytku kiberprostoru ta jogho socialjno-psykhologhichni naslidky. Systemy upravlinnja, navighaciji ta zv'jazku. *Zbirnyk naukovykh pracj.* Poltava: PNTU, T. 3 (65). 89–91. doi: https://doi.org/10.26906/SUNZ.2021.3.089.

4. Kaplja, O. M. (2023). Pravove reghuljuvannja informacijnoji bezpeky ghromadjanyna pid chas diji vojennogho stanu. *Ekspert: paradyghmy jurydychnykh nauk i derzhavnogho upravlinnja*. 6 (24). 16–20. doi: https://doi.org/10.32689/2617-9660-2022-6(24)-16-20.

5. Leghominova. S., Ghajdur, Gh. (2023). Analiz suchasnykh zaghroz informacijnij bezpeci orghanizacij ta formuvannja informacijnoji platformy protydiji jim. *Elektronne fakhove naukove vydannja «Kiberbezpeka: osvita, nauka, tekhnika»,* 2(22), 54–67. https://doi.org/10.28925/2663-4023.2023.22.5467.

6. Maljceva, I. R. (2022). Analiz dejakykh kiberzaghroz v umovakh vijny. Kiberbezpeka: osvita, nauka, tekhnika. (16). 37–43. doi: 10.28925/2663-4023.2022.16.3744.

7. Tkach, Ju. (2021). Konceptualjna modelj bezpeky kiberprostoru. Tekhnichni nauky ta tekhnologhiji. 4 (22). 96–108. https://doi.org/10.25140/2411-5363-2020-4 (22)-96-108.

8. Khlaponin, Y., Kozubtsova, L., Kozubtsov, I., Shtonda, R. (2022). Funkciji systemy zakhystu informaciji i kiberbezpeky krytychnoji informacijnoji infrastruktury. *Elektronne fakhove naukove vydannja «Kiberbezpeka: osvita, nauka, tekhnika»,* 3(15), 124-134. https://doi.org/10.28925/2663-4023.2022.15.1241341.

9. Onyshchenko, S., Hlushko, A. (2022). Analitychnyj vymir kiberbezpeky Ukrajiny v umovakh zrostannja vyklykiv ta zaghroz. *Naukovyj zhurnal «Ekonomika i reghion»,* 1(84), 13–20. https://doi.org/https://doi.org/10.26906/EiR.2022.1 (84).2540.