зору працівників, рекламі [2].

Список використаних джерел

1. Карпухіна О.В. Основи Інтернет-технологій : навч. посіб. / О.В. Карпухіна – Х. : Компанія СМІТ, 2010. – 394 с.

2. Дурняк Б.В Пректування реклами в мережі Internet на основі семантичного аналізу / Б.В Дурняк, О.Ю. Коростіль Львів: УАД, 2014. – 35 с.

Нестеренко Олександр Васильович
кандидат технічних наук, доцент,
дійсний член Міжнародної академії інформатики,
професор ВНЗ «Національна академія управління»,
Заслужений працівник сфери послуг України
м. Київ, Україна

СТІЙКІСТЬ, ЖИВУЧІСТЬ ТА КІБЕРБЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ В СФЕРІ АДМІНІСТРАТИВНОГО УПРАВЛІННЯ

Сучасний розвиток інформаційно-комунікаційних технологій створив умови для впровадження в органах адміністративного управління автоматизованих систем підтримки прийняття рішень, які, з урахуванням парадигми відкритості діяльності, забезпечують оприлюднення власних інформаційних ресурсів в Інтернеті. Разом із тим на сьогодні вже є очевидною глобальна небезпека, на яку наражаються веб-ресурси сфери адміністративного управління у зв’язку із екстенсивним зростанням інцидентів кібербезпеки, що призводить до спотворення ресурсів, перешкоджання діяльності органів управління та погіршення їх іміджу, особливо у надзвичайних ситуаціях та в критичних сферах, і, як наслідок, до відповідного зниження рівня безпеки органів управління та держави в цілому [1, 2].

Водночас в публічному дискурсі останніх років підіймаються питання про нові шляхи попередження природних та техногенних катастроф, забезпечення процесів життєдіяльності в кризових умовах, пов’язані зі зростанням рівня глобальних загроз у різних сферах як для держави, так і для громадян. Особливого значення це набуває в умовах цифрової трансформації державного управління, курс на яку проголошено керівництвом країни. Внаслідок цього виникло поняття стійкости інфраструктур, екосистем й інших сфер [3]. На порядок денний вийшли завдання розбудови стійкости держави і суспільства до інформаційних атак, стійкости комп’ютерних систем до хакерських атак, стійкости до терористичних загроз як складової національної стійкости. Питаннями стійкости опікуються й міжнародні організації, зокрема ООН, НАТО, ОЄСР.

Поняття стійкости, що використовується в різних сферах, є складним, багатогранним й має різні відтінки. Певною мірою така ситуація є відображенням неоднозначності й багато в чому новизни процесів, що відбуваються, а також відсутності чіткої стратегії дій в різних ситуаціях. Крім того, поняття стійкости та інші пов'язані з ним поняття, зокрема в сфері інформаційних систем та їх кібербезпеки, ще не знайшли належного термінологічного врегулювання.

Приміром, поняття стійкості для технічних систем є не новим і використовується вже тривалий час. Наприклад, для систем автоматичного регулювання – це їх здатність не допускати відхилення регульованої величини від заданого значення при будь-якому реальному збуренні у системі.

У загальному системному плані стійкість (*robustness*) – це якість, що дозволяє системі витримувати зміни параметрів зовнішнього та/або внутрішнього середовища, відмінні від розрахункових. Система може бути названою стійкою, якщо вона в змозі впоратися з варіаціями (іноді непередбачуваними) в операційному середовищі з мінімальними збитком, зміною або втратою функціональності.

У суспільній сфері поширюється поняття стійкості, яке пов'язують зі словом *resilience*. Але насправді воно означає пружність – міру швидкості повернення до початкового стану після виведення з нього (порушення). Вочевидь, при розгляді стійкості необхідно виділяти й опір (*resistance*) як показник здатності протистояти змінам.

Отже стійкість системи залежить від гомеостатичних реакцій її складових, а здатність системи повертатися до деякого певного стану пов'язана з поняттям стійкої рівноваги.

Повертаючись до інформаційних систем необхідно згадати й про їх функціональну стійкість, яка, в першу чергу, обумовлена здатністю системи надавати регламентовані послуги на протязі визначеного часу [4]. При цьому функціональна стійкість інформаційної системи поєднує властивости надійности (безвідмовности), відмовостійкости й живучости.

У свою чергу живучість (survivability), згідно зі стандартним визначенням стосовно автоматизованої системи (АС) – це здатність АС виконувати установлений обсяг функцій в умовах впливу зовнішнього середовища та відмов компонентів системи в заданих межах [5].

Вищенаведені поняття той чи іншою мірою стосуються підтримки кібербезпеки інформаційних систем, і лише їх фрагментарний перелік свідчить про неоднозначність трактувань і умов використання. Тому в науково-прикладному плані постає проблема розроблення відповідного веб-глосарію термінології національної стійкости, особливо в сфері кібербезпеки, та формалізованої моделі стійкости веб-ресурсів сфери адміністративного управління, до якої входять як до спільного інформаційного простору не

лише органи управління, а й установи, підприємства та організацій, що використовують ці веб-ресурси.

Іншою проблемою є врахування результатів цього моделювання при формуванні та розвитку захищеного середовища функціонування інформаційного простору сфери адміністративного управління, особливо в частині виявлення вразливостей веб-ресурсів та їх захисту не лише з точки зору цілісності та доступності інформації, а й для запобігання можливості зараження через них комп'ютерів зовнішніх користувачів і, таким чином, попередження вірусних епідемій [6].

Список використаних джерел

1. Горбулін В.П. Системно-концептуальні засади стратегії національної безпеки України / В.П. Горбулін, А.Б. Качинський. – К.: ДП «НВЦ «Євро-атлантикінформ», 2007. – 592 с.

2. Нестеренко О.В. Безпека інформаційного простору державної влади. Технологічні основи / О.В. Нестеренко. – К.: Наук. думка, 2009. – 352 с.

3. Резнікова О.О. Концептуальні підходи до вибору моделі забезпечення національної стійкості / Ольга Резнікова // Стратегічні пріоритети. – 2019. – № 1 (49). *– С. 18-27.*

4. Саланда І.П. Система показників та критеріїв формалізації процесів забезпечення локальної функціональної стійкості розгалужених інформаційних мереж / І.П. Саланда, О.В. Барабаш, А.П. Мусієнко // Наукове періодичне видання «Системи управління, навігації та зв'язку». – Полтава: ПНТУ, 2017. – Вип. 1 (41). – С. 122-126.

5. Додонов А.Г. Компьютерные информационные системы и хранилища данных. Толковый словарь / А.Г.Додонов, С.Р. Коженевский, Д.В. Ланде, В.Г. Путятин. – Киев: Феникс, ИПРИ НАН Украины, 2013. – 554 с.

6. Нестеренко О.В. Методологія використання результатів прогностичного моделювання зараження комп'ютерними вірусами веб-ресурсів органу державного управління на основі епідеміологічного підходу / О.В. Нестеренко // Національна безпека у фокусі викликів глобалізаційних процесів в економіці, матеріали IV-ої міжнародної наукової Інтернет-конференції (Київ – Nowy Sącz, 27-28 червня 2019 року), ВНЗ «Національна академія управління». – Київ: НАУ. – 2019. – С. 55-57.