МІЖНАРОДНИЙ НАУКОВО-ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ АКАДЕМІКА ЮРІЯ БУГАЯ

ПОЛТАВСЬКИЙ ІНСТИТУТ БІЗНЕСУ

# АКТУАЛЬНІ ПРОБЛЕМИ РОЗВИТКУ СУЧАСНОЇ НАУКИ

*присвяченої пам'яті засновника і фундатора Міжнародного науково-технічного університету – академіка, доктора технічних наук, професора Юрія Миколайовича Бугая*

## МАТЕРІАЛИ
**XVI Всеукраїнської науково-практичної конференції**

**3 червня 2021 року**

Полтава

**УДК 001**
**А 43**

*Рекомендовано до друку вченою радою*
*Полтавського інституту бізнесу ЗВО «МНТУ»*
*(протокол № 5 від 27.05.2021)*



**А 43** **Актуальні проблеми розвитку сучасної науки**: матеріали XVI Всеукр. наук-практ. конф., (м. Полтава, 3 червня 2021 р.). – Полтава: Сімон, 2021. – 151 с.

*Матеріали збірника присвячені соціально-економічним, суспільним, правовим проблемам та пов'язаними з ними проблемами генофонду й здоров'я нації. Тези розміщені відповідно до секцій, за якими була організована робота конференції.*

*Матеріали можуть бути використані у науково-дослідній та практичній діяльності студентами, аспірантами, науковцями та викладачами вищих навчальних закладів з обов'язковим посиланням на автора наукової праці.*

**УДК 001**

**Відповідальність за зміст та достовірність опублікованих матеріалів несуть автори публікацій.**

залучення хмарних технологій загалом. Окрім цього, споріднена діяльність додає можливість здобувачам освіти бути скерованими у сфері всіх інноваційних розробок, досить швидко їх опановувати, і використовувати власні концепції не марнуючи на це досить помітних затрат.

**Список використаних джерел:**


1. Биков В. Ю. Хмарні технології, ІКТ-аутсорсинг і нові функції ІКТ підрозділів освітніх і наукових установ. Інформаційні технології в освіті. №10. 2011. С. 8–23.
2. Глуховець Ю.В., Дашко Ю.С. Хмарні технології – важлива альтернатива в сучасній перспективі. *Сучасні світові тенденції розвитку інформаційних технологій, економіки і права*: матеріали науково-практичної конференції, м. Чернігів, 18 квітня 2019 р. ЧІІБІП МНТУ імені академіка Юрія Бугая. Чернігів, 2019. С. 175 – 177.
3. Про затвердження Положення про дистанційну освіту. URL: http://zakon5.rada.gov.ua/laws/show/z0703-13 (дата звернення 25.05.21)
4. Рашевська Н. В. Хмарні технології дистанційного навчання у процесі навчання вищої математики. UR: http://ite.kspu.edu/webfm_send/458 (дата звернення 26.05.21)
5. Microsoft Live@edu. URL: https://service.iv-edu.ru/live-edu (дата звернення 26.05.21)


## ОЦІНКА КРИТИЧНОСТІ ВРАЗЛИВОСТЕЙ ВЕБ-КОМПОНЕНТ ІНФОРМАЦІЙНОЇ СИСТЕМИ


***Поночовний Юрій Леонідович***

кандидат технічних наук, старший науковий співробітник, доцент кафедри інформаційних систем та технологій Полтавського державного аграрного університету

***Шрамко Антон Юрійович***

здобувач вищої освіти спеціальності «Інформаційні системи та технології» Полтавського державного аграрного університету


За останній час істотно зросла залежність суспільства від інформаційних систем. Управління торгівлею, банківські операції, медицина, військові і державні системи залежать від комп'ютерних систем, які не можуть функціонувати без підключення до глобальної мережі. Як результат – суттєвий ризик для критично важливих об'єктів від експлуатації вразливостей як програмного, так і апаратного забезпечення шляхом реалізації різних класів атак [1].

Через це сьогодні різні організації та інститути проводять масштабні дослідження проблем безпеки, викликаних слабкими місцями та вразливостями апаратно-програмного забезпечення. Незважаючи на існуючі загрози, суспільство не готове відмовитися від використання мережі Інтернет і комп'ютерних мереж в цілому, так як

вони надають величезні можливості у фінансовій, політичній і військовій сферах [2]. Та навіть постійне вдосконалення технологій безпеки не може дати гарантій абсолютної захищеності інформаційних систем.

Вразливості виявляють не тільки в усіх відомих операційних системах і додатках, а і в апаратних компонентах інформаційних систем. Так як нові вразливості знаходять безперервно, єдиним шляхом зменшення ймовірності їх експлуатації зловмисниками є виконання безперервного моніторингу захищеності, що полягає в постійному відстеженні появи вразливостей, оперативному встановленні патчів та оновлень і використанні інструментів протидії атакам, що базуються на експлуатації цих вразливостей [3].

В даний час існує цілий ряд інформаційних ресурсів Інтернет, які надають інформацію про вразливості на сторінках своїх сайтів. Наприклад, база даних CVE [4] є єдиним і первинним постачальником ідентифікаторів вразливостей; база даних вразливостей NVD дозволяє точно ідентифікувати уразливий програмний продукт і його версію, отримати інформацію про спосіб атак, при яких дана уразливість проявляє себе, різновид загрози та іншу корисну інформацію. Ідентифікатори CVE використовуються для однозначного позначення однієї і тієї ж уразливості іншими відомими базами даних (Secunia, Security Focus і ін.), базами експлойтів (Exploit Database і ін.) і бюлетенями безпеки (Microsoft Security Bulletin , US-CERT [5] Security Bulletin та ін.).

Для опису методів забезпечення кібербезпеки розроблено спеціальну онтологію CYBEX, у якій показана модель опису узагальненої області операцій кібербезпеки. Онтологія складається з набору типів, властивостей і відносин (рис.1). Суцільними лініями позначені відносини між типами інформації, а стрілки показують вхідні інформаційні сигнали від функціональних об'єктів до баз знань / даних. Зображені справа функціональні об'єкти є типовими, і такі об'єкти, як CIRT, можуть виконувати одну або кілька функцій.

У даній онтології використана модель, що визначає домени операцій кібербезпеки, які далі застосовуються для ідентифікації необхідних об'єктів, що підтримують операції в кожному домені. Операції кібербезпеки складаються з трьох доменів: обробки інцидентів, управління ресурсами ІС та накопичення знань.

Система оцінки загальновідомих вразливостей (CVSS) забезпечує відкриту структуру подання інформації о характеристиках і впливі вразливостей ІС. Система CVSS складається з трьох груп: базової, часової і групи зовнішніх факторів. За кожною з них формується бальна оцінка, що знаходиться в межах від 0 до 10, а також вектор - стислий

текстовий опис значень, використаних для отримання оцінки. Базова група відображає внутрішні якості, притаманні тій чи іншій уразливості.

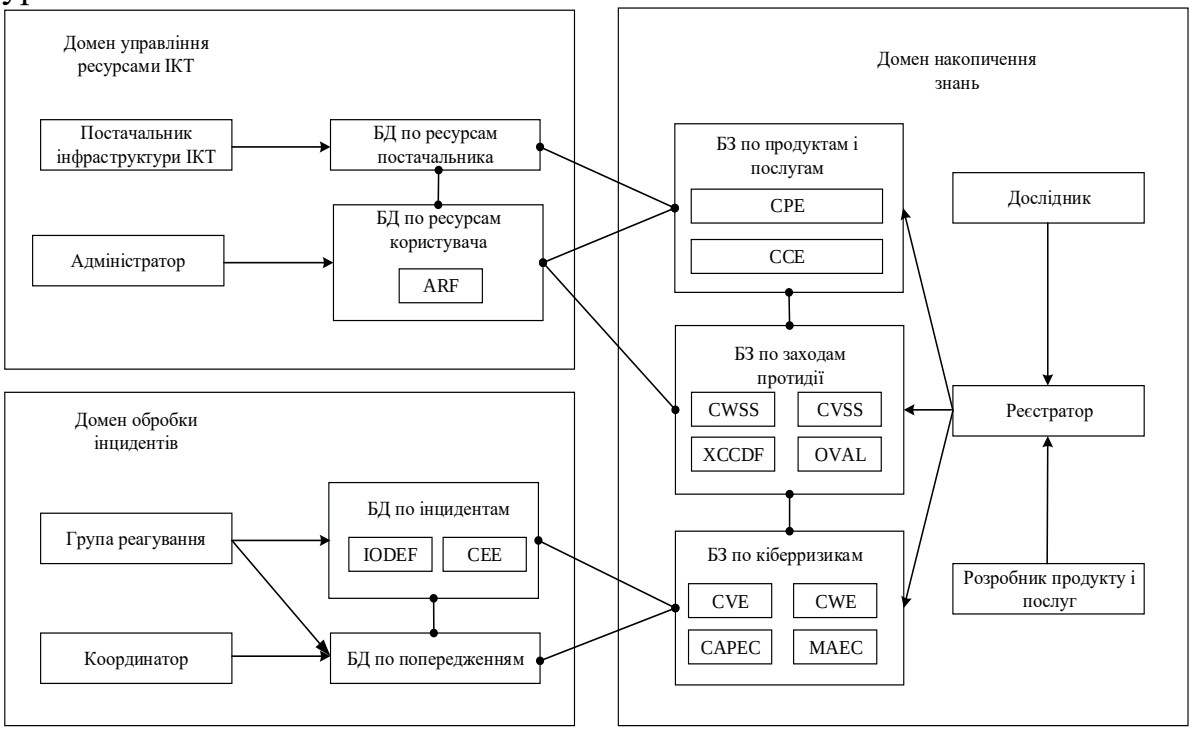


Рис. 1. Модель онтології CYBEX

Часова група відображає характеристики уразливості, які змінюються в часі. У групі зовнішніх факторів представлені характеристики уразливості, властиві тільки зовнішньому середовищу користувача. Система CVSS дозволяє адміністраторам засобів інформаційних систем, постачальникам бюлетенів з описом вразливостей, розробникам засобів безпеки, розробникам додатків і дослідникам скористатися прийняттям спільної мови оцінки вразливостей.

Кожна вразливість в базі NVD [6] має як мінімум чотири атрибути:

- унікальний ідентифікатор (наприклад, CVE-2021-0001);
- коротка загальна інформація про уразливість, в яких продуктах вона виявлена (Summary);
- дата публікації (Published);
- рівень серйозності (CVSS Severity).

Є також інші атрибути, доступні при деталізації конкретної вразливості на окремій веб-сторінці. Серед додаткових атрибутів можна виділити «Vulnerability Type», який використовує класифікатор зі словника CWE (Common Weakness Enumeration), а також базову метрику (CVSS Base Score) - параметр, який розраховується за спеціальною формулою виходячи з експертних оцінок окремих метрик

AccessComplexity, Authentication, AccessVector, ConfImpact, IntegImpact, AvailImpact.

Таким чином, існує можливість дослідити критичність компонент інформаційної системи за показником CVSS Severity.

**Список використаних джерел:**

1. Присяжний Д.П. Удосконалення захисту веб-ресурсів від атак на основі комбінованого евристично-статистичного підходую. Реєстрація, зберігання і обробка даних. 2016. Т. 18. № 1. С. 63–69.

2. Федорченко А.В., Чечулин А.А., Котенко И.В. Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализазащищенности компьютерных сетей. Информационно-управляющие системы. 2014. № 5. С. 72–79.

3. Поночовний Ю. Л., Рогочий С. Ю., Шарай О. І., Кнуренко В.О., Воронянський В. С. Дослідження баз вразливостей для параметризації марковських моделей оцінювання доступності веб-ресурсів. Системи та технології. 2019. № 1. С. 68–80.

4. Common Vulnerabilities and Exposures. The MITRE Corporation. URL: http://cve.mitre.org (дата звернення 26.05.21)

5. CERT Vulnerability Notes Database. Carnegie Mellon University Software Engineering Institute. URL: https://www.kb.cert.org/vuls (дата звернення 26.05.21)

6. NVD – Search and Statistics. NIST Computer Security Division,Information Technology Laboratory. URL: https://nvd.nist.gov/vuln/search (дата звернення 26.05.21)

## АЛГОРИТМ ОЦІНКИ РИЗИКІВ ФІЗИЧНОГО ЗАХИСТУ ТА КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ

***Поночовний Юрій Леонідович***

кандидат технічних наук, старший науковий співробітник, доцент кафедри інформаційних систем та технологій Полтавського державного аграрного університету

***Гаркавенко Євгеній Сергійович***

здобувач вищої освіти спеціальності «Інформаційні системи та технології»

Тенденції розвитку сучасного суспільства напряму пов'язані з переходом від ручної до автоматизованої обробки даних і засобами автоматизації завдяки впровадженню сучасних інформаційних технологій. Сучасні інформаційні системи (ІС) послідовно реалізують принципи єдності інформаційних процесів, інформації та бізнес-процесів шляхом застосування технічних та програмних засобів [1]. На сьогодні важливу роль в будь-якому бізнесі відіграє інформаційне забезпечення, яке дозволяє збирати і опрацьовувати інформацію, необхідну для прийняття обґрунтованих управлінських рішень [2].

Інформаційна система сучасного підприємства забезпечує виконання інформаційних процесів для задоволення потреби в інформації різних рівнів прийняття рішень для управління бізнесом [2]. ІС складається з компонентів обробки і зберігання інформації та внутрішніх і зовнішніх каналів її передачі, причому як компоненти обробки, так і канали можуть бути представлені як у локальному, так і у віддаленому (хмарному) виконанні. Сучасні ІС послідовно реалізують принципи єдності інформаційних процесів, інформації та бізнес процесів шляхом застосування технічних та програмних засобів [3].

Архітектура сучасної ІС агропромислового комплексу побудована з використанням технології «клієнт-сервер» [4]. Це спосіб взаємодії апаратних та програмних компонентів, при якому вони утворюють єдину систему. Є певний клієнтський процес, що вимагає певних ресурсів, а також серверний процес, який ці ресурси надає. На рисунку 1 показана архітектура цього типу.

Програмний продукт автоматизованої інформаційної системи управління аграрним виробництвом складається з серверної і клієнтської частини. На серверну частину покладаються функції управління базою даних (БД): постачальників-замовників, замовлень-заявок, товарів, договорів, накладних, а також підтримки цілісності даних, обробка запитів, управління транзакціями, правами доступу до різних даних [4,5]. Реалізація сервера БД часто здійснюється на базі сучасних хмарних технологій. На ринку сьогодні існує багато платформ для організації хмарних обчислень. Існують як пропрієтарні (комерційні), так і відкриті (вільні). На основі відкритих платформ, таких як OpenStack [6], CloudFoundry [7] багато компаній створюють свої інфраструктури та пропонують засоби для їх управління, зокрема, надають комплекси для перетворення наявних ресурсів в хмари [5].

Моделі оцінки ризиків містять вказівки для оцінки відомих факторів ризику в умовах ймовірних загроз з урахуванням джерел поставки, наявних вразливостей і наслідків для продукції, репутації та прибутку підприємства. Наслідки при оцінці ранжуються в залежності від конкретного компонента і конфігурації, а також від важливості додатків.

Модель оцінки ризиків враховує також фактори надмірності, закладеної в архітектуру ІС, старіння компонентів, оновлення ПЗ, тощо. Кожен з факторів ризику отримує кількісну оцінку, після чого з їх сукупності складається інтегрована оцінка, яка може перебувати на одному з рівнів, що показують характер важливості компонента, який визначається другою моделлю.

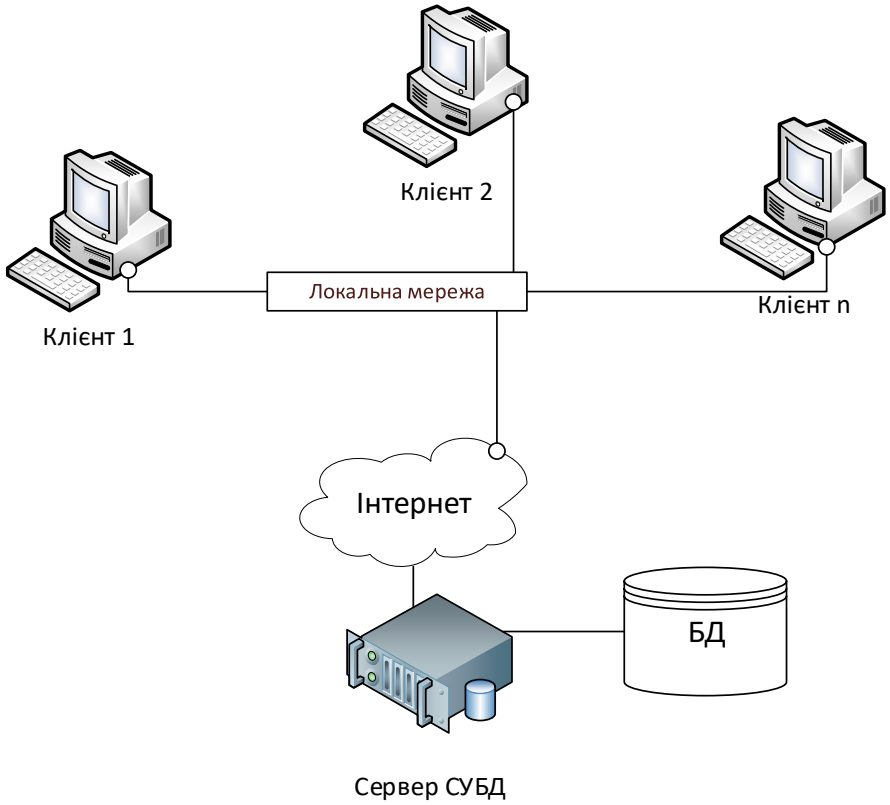


Рис. 1. Загальна схема ІС з архітектурою «клієнт-сервер»

Питання кібербезпеки стосуються сьогодні всіх, починаючи від фахівців з інформаційних технологій і закінчуючи службою контролю якості. Разом з тим велике число учасників кіберпростору стимулює його динамічність - поряд з ускладненням захисних засобів ускладнюються і засоби атаки. Традиційні статичні оцінки з появою нових технологій і методів швидко застарівають. На відміну від страхової галузі, яка при оцінці потенційної шкоди широко використовує історичні дані, в кіберпросторі історичні дані абсолютно неактуальні. Все це заважає систематизації існуючих ризиків, оцінці ймовірності їх виникнення та визначення масштабів наслідків.

Для оцінювання ризиків фізичного захисту та кібербезпеки інформаційної системи використано послідовний алгоритм, який включає виконання наступних етапів:

1. Використовуючи особливості архітектури ІС виділити фактори, які необхідно обов'язково врахувати при побудові моделі оцінки ризиків;
2. Визначити кількість станів моделі;
3. Визначити переходи між станами;
4. Побудувати орієнтований граф;
5. Виконати розмітку графа;

6. Побудувати систему диференціальних рівнянь Колмогорова-Чепмена;

7. Виконати рішення СДУ;

8. Визначити функції ймовірності ризиків для заданих рівнів деградації системи.

Подальше визначення рівня ризиків потребує конкретизації втрат, які зазнає ІС, перебуваючи в станах деградації. Загальна формула для визначення ризикових втрат наступна:

$$C = \sum_{j=0}^{3} P_{\text{sec}}^{(j)} \cdot C_j ,$$

де $C_j$ – втрати від перебування системи на j-му рівні деградації.

За допомогою марковської моделі оцінювання ймовірності ризику [8] для ІС з трьохзоновою архітектурою захисту отримано значення ймовірності трьох рівнів деградації:

- $Psec^{(0)}$ = 0,012855592;
- $Psec^{(I)}$ = 2,27152E-05;
- $Psec^{(II)}$ = 1,0878E-08.

**Список використаних джерел:**


1. Сазонець О. М. Інформаційні системи і технології в управлінні зовнішньоекономічною діяльністю: навч. посіб. К. : «Центр учбової літератури», 2014. 256 с.
2. Інформаційне забезпечення менеджменту URL: https://library.if.ua/book/23/1721.html (доступно 01.05.2021)
3. Сфери застосування інформаційних систем та їх використання в зовнішньоекономічній діяльності. URL: https://eki.wunu.edu.ua/2016/04/сфери-застосування-інформаційних-си/ (доступно 01.05.2021)
4. Поняття моделі даних, бази даних (БД), система управління базами даних (СУБД). URL: https://vseosvita.ua/library/prezentacia-ponatta-modeli-danih-bazi-danih-bd-sistema-upravlinna-bazami-danih-subd-9-klas-68079.html (доступно 01.05.2021)
5. Адміністрування даних та адміністрування БД. URL: http://sun.vtei.com.ua/mod/resource/view.php?id=54482 (доступно 01.05.2021)
6. OpenStack: Open Source Cloud Computing Infrastructure. URL: https://www.openstack.org/ (accessed 01.05.2021)
7. Cloud Foundry – Open Source Cloud Native Application. URL: https://www.cloudfoundry.org/ (accessed 01.05.2021)
8. Аль-Хафаджі А. В., Поночовний Ю. Л, Харченко В. С., Узун Д. Д. Дослідження марковської моделі готовності системи фізичного захисту з деградацією внаслідок атак і апаратних відмов. Радіоелектронні і комп'ютерні системи. 2020. № 1. С. 37–43.

*Наукове видання*

**МАТЕРІАЛИ**
**XVI Всеукраїнської науково-практичної конференції**

# АКТУАЛЬНІ ПРОБЛЕМИ РОЗВИТКУ СУЧАСНОЇ НАУКИ

*присвяченої пам'яті засновника і фундатора Міжнародного науково-технічного університету – академіка, доктора технічних наук, професора Юрія Миколайовича Бугая*

**3 червня 2021 року**

Здано до друку 02.06.2021 р.
Формат 60x84/16. Папір офсетний.
Гарнітура Times New Roman. Друк офсетний.
Ум.-друк. арк. 10,8
Наклад 100 прим. Зам. № 6312-93

Віддруковано у друкарні ТОВ «СІМОН»
м. Полтава, вул. Пушкіна, 42
050-590-12-52
simon@simon.com.ua
www.simon.com.ua
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовників
і розповсюджувачів видавничої продукції
Серія ПЛ № 17 від 23.03.2004 р.