Використані літературні джерела

1. Економіка знань та її перспективи для України : наук. доп. / В. М. Геєць, В. П. Александрова, Ю. М. Бажал, М. С. Данько, В. В. Дем'яненко ; Ін-т екон. прогнозування НАН України. – Київ, 2005. – 168 с.
2. *Геєць В.* Характер перехідних процесів до економіки знань / В. Геєць // Економіка України. – 2004. – № 5. – С. 4–14.
3. *Вознюк А. В.* Педагогическая парадоксология: аксиоматический, теоретический, прикладной аспекты : монография / А. В. Вознюк. – Житомир : Рута, 2016. – 622 с.
4. *Плигин А. А.* Познавательные стратегии школьников : монография / А. А. Плигин. – М. : Профит Стайл, 2007. – 528 с.
5. *Пономарев Я. А.* Психология творчества / Я. А. Пономарев. – М. : Наука, 1976. – 298 с.
6. *Музика О. Л.* Ціннісна регуляція і ціннісна підтримка розвитку творчих здібностей (теоретична модель і принципи побудови методики) / О. Л. Музика // Здібності, творчість, обдарованість: теорія, методика, результати досліджень / за ред. В. О. Моляко, О. Л. Музики. – Житомир : Рута, 2006. – 320 с.

Bibliography

1. Ekonomika znan ta yii perspektyvy dlia Ukrainy : nauk. dop. / V. M. Heiets, V. P. Aleksandrova, Yu. M. Bazhal, M. S. Danko, V. V. Dem'yanenko ; In-t ekon. prohnozuvannia NAN Ukrainy. – Kyiv, 2005. – 168 s.
2. *Heiets V.* Kharakter perekhidnykh protsesiv do ekonomiky znan / V. Heiets // Ekonomika Ukrainy. – 2004. – № 5. – S. 4–14.
3. *Vozniuk A. V.* Pedahohycheskaia paradoksolohyia: aksyomatycheskyi, teoretycheskyi, prykladnoi aspekty : monohrafyia / A. V. Vozniuk. – Zhytomyr : Ruta, 2016. – 622 s.
4. *Plyhyn A. A.* Poznavatelnye stratehyy shkolnykov : monohrafyia / A. A. Plyhyn. – M. : Profyt Stail, 2007. – 528 s.
5. *Ponomarev Ya. A.* Psykholohyia tvorchestva / Ya. A. Ponomarev. – M. : Nauka, 1976. – 298 s.
6. *Muzyka O. L.* Tsinnisna rehuliatsiia i tsinnisna pidtrymka rozvytku tvorchykh zdibnostei (teoretychna model i pryntsypy pobudovy metodyky) / O. L. Muzyka // Zdibnosti, tvorchist, obdarovanist: teoriia, metodyka, rezultaty doslidzhen / za red. V. O. Moliako, O. L. Muzyky. – Zhytomyr : Ruta, 2006. – 320 s.

Толюпа Сергій,
Толюпа Євген,
Агапова Єлізавета,
м. Київ

УДК 37.013.8:303.725.36

ВПЛИВ КІБЕРНЕТИЧНИХ АТАК НА ІНФОРМАЦІЙНУ СИСТЕМУ

Сьогодні система виявлення кібервторження та кібератак є програмні або апаратно-програмові рішення, що автоматизують процес контролю, що здійснюється в інформаційній системі або мережі, а також самостійно аналізує ці дії у пошуках ознак проблем кібербезпеки. Отже існує підхід до побудови систем виявлення кібератак на інформаційні системи є недоліки та слабкі місця, що дозволяють поганим звичкам діяти успішно та долати системи захисту інформації. Перехід від пошуку сигнатур кібератак до виявлення передбачень виникнення загроз інформаційній безпеці повинна допомогати, щоб на корню змінити цю ситуацію, скоротивши дистанцію відставання у розвитку системи захисту від системи подолання.

Ключові слова: *кібербезпека, кіберзагроза, кібератака, інформаційні технології, засоби захисту.*

Сегодня системы обнаружения кибервторжений и кибератак обычно представляют собой программные или аппаратно-программные решения, которые автоматизируют процесс контроля происходящих

в информационной системе или сети, а также самостоятельно анализируют эти события в поисках признаков проблем кибербезопасности. Однако существующий подход к построению систем обнаружения кибератак на информационные системы полны недостатков и уязвимостей, позволяющих, к сожалению, вредным воздействиям успешно преодолевать системы защиты информации. Переход от поиска сигнатур кибератак к выявлению предпосылок возникновения угроз информационной безопасности должна способствовать тому, чтобы в корне изменить данную ситуацию, сократив дистанцию отставание в развитии систем защиты от систем их преодоления.

Ключевые слова: *кибербезопасность, киберугроза, кибератака, информационные технологии, средства защиты.*

Today, cybercrime detection and cyberattack systems are typically software or hardware-software solutions that automate the control of what's happening in the information system or network and also independently analyze these events in search of signs of cyber security issues. However, the existing approach to building cyberattack detection systems on information systems is full of weaknesses and vulnerabilities that, unfortunately, allow harmful influences to successfully overcome information security systems. The transition from searching for cyberattack signatures to identifying the preconditions for information security threats should help to radically change this situation by reducing the gap in the development of security systems from overcoming systems.

Key words: *cybersecurity, cyber threats, cyberattack, information technologies, means of protection.*

Однією з ключових проблем, що в умовах глобалізації інформаційного обміну та широкого впровадження інформаційних технологій в усіх сферах життєдіяльності суспільства постали перед державами світу, є проблема захисту інформації, яка обробляється в інформаційно-телекомунікаційних системах, від викликів і загроз у кібернетичному просторі. Можливості кібернетичного простору, лавиноподібний процес розвитку та впровадження новітніх інформаційних і телекомунікаційних технологій забезпечують безпрецедентні умови для накопичення та використання інформації, а також створюють фундаментальну залежність від їх нормального функціонування всіх сфер життєдіяльності суспільства та держави: економіки, політики, сфери національної та міжнародної безпеки тощо. Така залежність стає вразливим місцем у функціонуванні систем та об'єктів критичних національних інфраструктур і дає можливість негативно налаштованим елементам та угрупованням скористатися нею для реалізації протиправних дій у кібернетичному просторі шляхом порушення цілісності, доступності, конфіденційності інформації та нанесення шкоди інформаційним ресурсам і телекомунікаційним системам. При цьому особливу занепокоєність викликає можливість застосування інформаційних технологій у кібернетичному просторі в інтересах здійснення військово-політичного та силового протиборства, тероризму та проведення хакерських кібератак [1].

Сьогодні для захисту інформації потрібна не просто розробка приватних механізмів захисту, а реалізація системного підходу, що містить комплекс взаємопов'язаних заходів. Головною метою будь-якої системи забезпечення інформаційної безпеки є створення умов функціонування підприємства, запобігання кіберзагроз його безпеки, захист законних інтересів підприємства від протиправних посягань, недопущення розкрадання фінансових засобів, розголошення, втрати, витоку, спотворення і знищення службової інформації, забезпечення в рамках діяльності установи [2].

Системи виявлення мережевих вторгнень та виявлення ознак кібератак на інформаційні системи вже давно застосовуються як один з необхідних рубежів оборони інформаційних систем. Розробниками систем захисту інформації та консультантами в цій галузі активно застосовуються такі поняття, як: захист по периметру; стаціонарний і динамічний захист; стали з'являтися власні терміни, наприклад, проактивні засоби захисту.

Сьогодні системи виявлення вторгнень і кібератак є програмні або апаратно-програмні рішення, які автоматизують процес контролю подій, що відбуваються в інформаційній системі або мережі, а також самостійно аналізують ці події в пошуках ознак проблем кібербезпеки. Оскільки кількість різних типів і способів організації несанкціонованих проникнень в чужі мережі за останні роки значно збільшилася, системи виявлення кібератак (СВКа) стали необхідним компонентом інфраструктури безпеки більшості організацій [3].

Сучасні системи виявлення вторгнень і кібератак ще далекі від ергономічних та ефективних рішень, з точки зору безпеки. Підвищення ефективності необхідно ввести не тільки в області виявлення зловмисних дій на інфраструктуру захищених об'єктів інформатизації, але і з точки зору повсякденної експлуатації цих засобів, а також економії обчислювальних та інформаційних ресурсів власника цієї системи захисту.

Якщо говорити безпосередньо про модулі обробки даних, то кожна сигнатура кібератаки в системі обробки інформації про кібератаку, є базовим елементом для розпізнавання більш загальних дій – розпізнавання фази кібератаки (етапи її реалізації). Поняття сигнатури узагальнюється до деякого вирішального правила, а кожна кібератака, навпаки, розбивається на набір етапів її проведення. Чим простіше кібератака, тим простіше її виявити та більше з'являється можливостей щодо її аналізу [4].

Сценарій кібератаки є графом переходів, в аналогічний графу кінцевого детермінованого автомата. Фази кібератак можна описати, наприклад, наступним чином: випробування портів; ідентифікація програмних і апаратних засобів; збір банерів; застосування експлойтів; дезорганізація функціоналу мережі з допомогою атак на відмову в обслуговуванні; управління через бекдори; пошук встановлених троянів; пошук проксі-серверів; видалення слідів присутності тощо (за необхідності з різним ступенем деталізації).

Переваги такого підходу очевидні – у випадку роздільної обробки різних етапів кібератаки з'являється можливість розпізнавати кіберзагрозу ще у процесі її підготовки та формування, а не на стадії реалізації, як це відбувається в існуючих системах. При цьому, елементною базою для розпізнавання може бути як сигнатурний пошук, так і виявлення аномалій, використання експертних методів та систем, довірчих стосунків та інших інформаційних, відомих та реалізованих, мережевих та локальних примітивів оцінювання того, що відбувається в інформаційному середовищі потоку подій. Узагальнюючий підхід до аналізу дозволяє визначати відповідно й розподілені (у всіх сенсах) кіберзагрози, як у логічному, так і фізичному просторі. Загальна схема обробки вступників подій також дозволяє здійснювати пошук розподілених кібератак шляхом подальшої агрегації даних з різних джерел та конструювання мета-даних про відомі інциденти [5−6].

Системи виявлення кібератак, як і більшість сучасних програмних продуктів/продукції, повинні задовольняти певним вимогам. Це – сучасні технології розробки, орієнтування на особливості сучасних інформаційних мереж, сумісність з іншими програмами. Щоб зрозуміти, як правильно використовувати СВКа, потрібно чітко представляти, як вони працюють та їх вразливі місця.

Якщо не враховувати різні несуттєві інновації в області виявлення кібератак, то можна сміливо стверджувати, що існують дві основні технології побудови СВКа. Суть їх полягає в тому, що СВКа володіють певним набором знань про методи вторгнень.

Більш широко кіберзагрози інформаційним ресурсам можна розглядати як потенційно можливі випадки природного, технічного або антропогенного характеру, що можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію, яка зберігається в ній. Виникнення кіберзагрози, тобто, віднаходження джерела актуалізації певних подій у загрози, характеризується таким елементом, як уразливість. Інтегруючи різні підходи, а також пропозиції щодо розв'язання цього питання, вважаємо, що можна виділити такі види кіберзагроз інформаційній безпеці: розкриття інформаційних ресурсів; порушення їх цілісності; збій в роботі самого обладнання.

Сьогодні за стрімким розвитком мережевих технологій і глобальної інформатизації суспільства на перший план висуваються проблеми забезпечення високо рівня захищеності інформаційних систем. Зі збільшенням числа комп'ютерних інцидентів, пов'язаних з безпекою, почали стрімко розроблятися системи виявлення атак (СВКа). СВКа є одним з важливих рішень для захисту систем і мереж зв'язку [7].

Традиційно СВКа класифікуються відповідно до двох характеристик: *перший* – методу виявлення, *другий* – рівень системи на якому здійснюється захист. Не дивлячись на те, що ці

дві класифікаційні ознаки є важливими при виборі систем виявлення кібератак, все ж існують й інші характеристики, що відіграють не менш важливу роль у проектуванні СВКа. Найбезпечніше рішення не може бути досягнуто при розгляді одного чи двох аспектів таксономії. Всі розробники систем виявлення атак та організації, що використовують СВКа повинні розуміти і вивчати їх класифікацію, щоб вибрати кращі рішення для систем захисту інформації. При дослідженні різних аспектів таксономії та застосуванні різних варіантів ми зможемо досягти більш високого рівня безпеки інформаційних систем. Структурна схема кібербезпеки інформаційної системи представлена на рисунку 1.

Системи виявлення аномального поведінки засновані на тому, що СВКа відомі деякі ознаки, що характеризують правильну чи допустиму поведінку об'єкта спостереження. Датчики пристроїв кібервторгнень ідентифікують незвичайну поведінку, аномалії у функціонуванні окремого об'єкта – труднощі їх застосування на практиці пов'язані з нестабільністю самих об'єктів, що захищаються та взаємодіючих з ними із зовнішніх об'єктів.

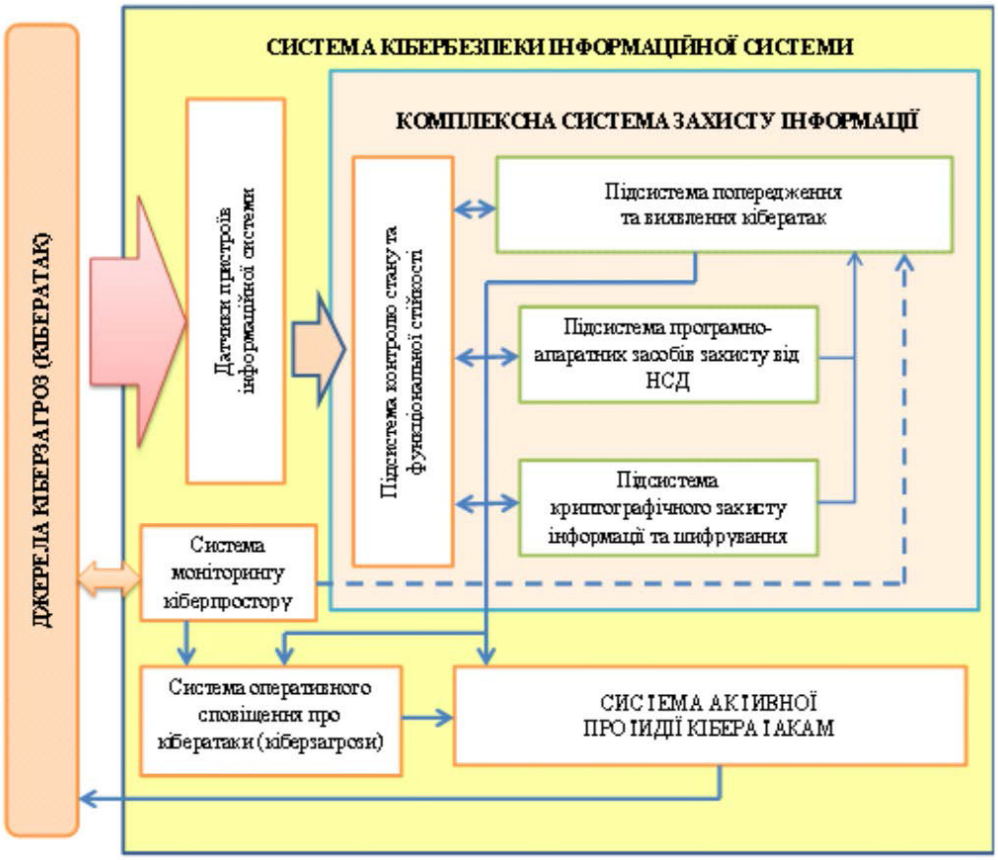

Рис. 1. Системи кібербезпеки інформаційної системи

Як об'єкт спостереження, мережа може виступати в цілому, як: окремий комп'ютер, мережева служба, користувач тощо. Датчики спрацьовують за умови, що вторгнення порушують нормальне функціонування інформаційної системи.

Сучасний підхід до побудови систем виявлення кібератак на інформаційні системи сповнений недоліків та вразливостей, що дозволяють шкідливим впливам успішно долати системи захисту інформації. Перехід від пошуку сигнатур кібератак до виявлення передумов виникнення загроз інформаційної безпеки має сприяти тому, щоб докорінно змінити таку ситуацію, скоротивши дистанцію відставання в розвитку систем захисту від систем їх подолання. Крім того, такий перехід має сприяти підвищенню ефективності управління інформаційною безпекою і, нарешті, більш конкретних прикладів застосування нормативних і керівних документів, що вже стали стандартами.

Використані літературні джерела

1. *Бурячок В. Л.* Інформаційний та кіберпростори. Проблеми безпеки, методи та засоби боротьби : навч. посіб. / В. Л. Бурячок, С. В. Толюпа, В. В. Семко. – Київ : Наш формат, 2016. – 176 с.
2. *Бурячок В. Л.* Інформаційна та кібербезпека: соціотехнічний аспект : навч. посіб. / В. Л. Бурячок, С. В. Толюпа, В. Б. Толубко, В. О. Хорошко. – Київ : Наш формат, 2015. – 288 с.
3. *Debar H.* Towards a Taxonomy of Intrusion Detection Systems / H. Debar, M. Dacier, A. Wespi // Computer Networks. – 1999. – Vol. 31. – P. 805–822.
4. *Debar H.* A Revised Taxonomy for Intrusion-Detection Systems / H. Debar, M. Dacier, A. Wespi. – 2000. – Vol. 55. – P. 361−378.
5. *Kabiri P.* Research on Intrusion Detection and Response: A Survey / P. Kabiri, A. Ghorbani // International Journal of Network Security. – 2005. – Vol. 1. – No. 2. – P. 84−102.
6. *Amer S. H.* Intrusion Detection Systems, (IDS) Taxonomy – A Short Review / S. H. Amer, J. A. Hamilton // DOD Software Tech News. – 2010. – Vol. 13. – No. 2. – P. 23–30.
7. *Бабенко І. К.* Разработка комплексной системы обнаружения атак / І. К. Бабенко, О. Б. Макаревич, О. Ю. Пескова // Информационная безопасность : материалы V междунар. науч.-практ. конф. – 2003. – №4 (33). – С. 235–239.

Bibliography

1. *Buriachok V. L.* Informatsiinyi ta kiberprostory. Problemy bezpeky, metody ta zasoby borotby : navch. posib. / V. L. Buriachok, S. V. Toliupa, V. V. Semko. – Kyiv : Nash format, 2016. – 176 s.
2. *Buriachok V. L.* Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt : navch. posib. / V. L. Buriachok, S. V. Toliupa, V. B. Tolubko, V. O. Khoroshko. – Kyiv : Nash format, 2015. – 288 s.
3. *Debar H.* Towards a Taxonomy of Intrusion Detection Systems / H. Debar, M. Dacier, A. Wespi // Computer Networks. – 1999. – Vol. 31. – P. 805–822.
4. *Debar H.* A Revised Taxonomy for Intrusion-Detection Systems / H. Debar, M. Dacier, A. Wespi. – 2000. – Vol. 55. – P. 361−378.
5. *Kabiri P.* Research on Intrusion Detection and Response: A Survey / P. Kabiri, A. Ghorbani // International Journal of Network Security. – 2005. – Vol. 1. – No. 2. – P. 84−102.
6. *Amer S. H.* Intrusion Detection Systems, (IDS) Taxonomy – A Short Review / S. H. Amer, J. A. Hamilton // DOD Software Tech News. – 2010. – Vol. 13. – No. 2. – P. 23–30.
7. *Babenko I. K.* Razrabotka kompleksnoi systemy obnaruzhenyia atak / I. K. Babenko, O. B. Makarevych, O. Yu. Peskova // Ynformatsyonnaia bezopasnost : materyaly V mezhdunar. nauch.-prakt. konf. – 2003. – №4 (33). – S. 235–239.

Оксана Дубініна,
м. Київ

УДК 378.091:004.9

РОЗВИТОК ІНФОРМАЦІЙНОЇ КОМПЕТЕНТНОСТІ МАЙБУТНІХ ПРОЕКТ-МЕНЕДЖЕРІВ У ПРОЦЕСІ ВИВЧЕННЯ ДИСЦИПЛІНИ «УПРАВЛІННЯ ІТ-ПРОЕКТАМИ»

У статті обґрунтовано застосування інформаційних технологій у підготовці майбутніх фахівців нового профілю – проект-менеджер, розкрито особливості застосування інформаційних технологій в управлінні проектами, розглянуто матеріали і методи реалізації проекту. Окреслено зміст підготовки проект-менеджерів у Навчально-науковому інституті менеджменту та психології ДВНЗ «Університет менеджменту освіти».

Ключові слова: *проект-менеджер, вищий навчальний заклад, інформаційні технології, управління проектами.*

В статье обоснованно применения информационных технологий в подготовке будущих специалистов нового профиля – проект- менеджер, раскрыты особенности применения информационных технологий в управлении проектами, рассмотрены материалы и методы реализации проекта. Определены