оскільки кожна нова версія містить виправлення та захист від сучасних комп'ютерних вірусів і троянських програм. Для безпечної роботи системи необхідно періодично змінювати паролі адміністраторів. Вживати заходи протидії впровадженню SQL ін'єкцій. Використовувати антивірусні програми тощо. Безпека системи полягає в постійному адмініструванні веб-сервера та бази даних, захисту від перенавантажень, а також вирішення технічних та організаційних питань.

Список використаної літератури:

1. Логінова Н.І. Забезпечення інформаційної безпеки в системі управління навчанням MOODLE / Н. І. Логінова // Правові та інституційні механізми забезпечення розвитку України в умовах європейської інтеграції: матер. міжнар. наук.-практ. конф. (18 травня 2018 р.): у 2 т. – Т. 1. – Одеса: Видавничий дім «Гельветика», 2018. – С. 598–600.
2. Логінова Н.І. Напрями захисту інформації в системі управління навчанням MOODLE / Н. І. Логінова // // Правове життя сучасної України: матер. міжнар. наук.-практ. конф. (17 вересня 2018 р.). – Одеса: Видавничий дім «Гельветика», 2018. – С. 188–191.
3. Tawfiq S. Barhoom, Rola J. Azaiza. Enhance MOODLE Security Against XSS Vulnerabilities // International Journal of Computing and Digital Systems. – № 5. – 2016.

Ключові слова: система управління навчанням Moodle, інформаційна безпека, вразливість інформації.

Ключевые слова: система управления обучением Moodle, информационная безопасность, уязвимость информации.

Key words: learning management systems Moodle, information security, information vulnerability

ТРОФИМЕНКО ОЛЕНА ГРИГОРІВНА

Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат технічних наук, доцент

МОНІТОРИНГ СТАНУ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Під час становлення інформаційного суспільства інформаційно-комунікаційні технології (ІКТ) – інтернет, новітні технології, цифрові послуги і пристрої – стають невід'ємною частиною нашого сьогодення. Разом з усіма перевагами від впровадження ІКТ вкрай небезпечно не враховувати можливі кіберзагрози світовому співтовариству як зворотній бік цього процесу. Останнім часом дедалі частіше суспільство стикається з різноманітними видами кібератак: збої при наданні електронних послуг, блокування роботи державних органів, фішингові атаки електронною поштою, кіберзлочини, порушення цілісності та

конфіденційності даних, інформаційно-психологічний тиск на населення, кібертероризм, кібершпигунство, інформаційна експансія у національний інформаційний простір країни, блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення й об'єктів підвищеної небезпеки. Позаяк кіберзагрози не можливо обмежити якоюсь однією сферою, це вимагає від усіх зацікавлених сторін всебічної обізнаності з факторами ризику, умінь та навиків для їх вирішення та відповідних заходів для запобігання кібератак ще до їх початку.

Саме держава має взяти на себе відповідальність за забезпечення доступу до стабільного безпечного цифрового простору, яким можуть скористатися її громадяни. Для цього країна повинна орієнтуватися у складній, наскрізній сфері кібербезпеки, застосовувати адекватні інструменти і ресурси про перехоплення інформації про можливі загрози, спрямовані на країну, і забезпечувати вирішення комплексу стратегічних, правових, політичних, технічних та організаційних питань. Доцільно агрегувати та розповсюджувати дані про відповідні інциденти для більш ефективного реагування, надавати доступ до своєчасних і надійних звітів про кіберзагрози, брати участь у багатогалузевому міжнародному співробітництві

Через значне зростання інформаційної складової агресії Російської Федерації проти України проблема кіберзагроз є надзвичайно актуальною і вимагає ефективних заходів з покращенння стану кібербезпеки держави [1]. Упродовж останніх років через кібератаки країні були завдані значні матеріальні та репутаційні збитки. Наша держава дорогою ціною зрозуміла неприпустимість зневажання питаннями власної кібербезпеки, оскільки, крім значних матеріальних збитків через втрату або спотворення стратегічно важливої інформації, це може спровокувати техногенні катастрофи, збитки цивільної, фінансової і військової інфраструктури аж до втрати суверенітету держави [2]. Саме тому гарантування кібербезпеки є надзвичайно актуальним для України, а заходи з протидії викликам і загрозам у цій галузі мають носити комплексний характер, позаяк кібербезпека повинна бути невід'ємною частиною технічного прогресу.

Усвідомлюючи важливість боротьби з кіберзлочинністю, більшість країн світу скоригували політику своїх урядів, розробили відповідні законодавчі акти і прийняли національні стратегії кібербезпеки [3].

Різноманітні індикатори реалізованих заходів у сфері захисту комп'ютерних і телекомунікаційних мереж від кібератак та створення умов для безпечного функціонування кіберпростору оцінюються у щорічних міжнародних рейтингах, найбільш авторитетними з яких є «Глобальний індекс кібербезпеки» (Global Cybersecurity Index, GCI) і «Національний індекс кібербезпеки» (National Cyber Security Index, NCSI). Дані цих рейтингів варто використовувати для моніторингу та порівняння стану кібербезпеки різних країн світу, а також задля вдосконалення механізмів міжнародної боротьби з кіберзлочинністю.

Дослідження **GCI** проводиться Міжнародним союзом електрозв'язку (ITU) і враховує п'ять комплексних показників [4]:

— *правові заходи*, оцінка яких ґрунтується на основі кількості наявних правових інституцій у сфері кібербезпеки держави, відповідної законодавчої бази, державних механізмів реагування шляхом розслідування кіберзлочинів та запровадження санкцій за невиконання або порушення закону. Основною метою цього чинника є створення достатнього законодавства на регіональному і міжнародному рівнях та спрощення міжнародної боротьби з кіберзлочинністю;

— *технічні заходи* оцінюються на основі кількості практичних механізмів боротьби з кібербезпекою, адже без відповідних технічних навичок для виявлення і реагування на кібератаки держави залишаються вразливими;

— *організаційні структури* оцінюються наявністю інституцій координації політики і стратегій розвитку кібербезпеки на національному рівні. Важливість цього показника зумовлена тим, що без національної стратегії, моделі управління та наглядового органу зусилля з кібербезпеки у різних секторах стають конфліктними і малоефективними;

— *нарощування потенціалу* – заходи, що ґрунтуються на існуванні досліджень і розробок, освітніх програм, сертифікованих фахівців і державних установ, які сприяють розвитку спроможності розроблення ефективних заходів з оптимізації системи кібербезпеки держави. Такими заходами можуть бути: кампанії з інформування громадськості, сертифікація та акредитація фахівців з кібербезпеки, курси професійної підготовки з кібербезпеки тощо;

— *національне і міжнародне співробітництво* – заходи з партнерських відносин, структур співпраці та мереж обміну інформацією, оскільки кіберзлочинність є глобальною проблемою і не обмежується національними кордонами або галузевими відмінностями.

Відповідно до даних рейтингу GCI-2018 Україна посіла 54 місце з-посеред 193 країн, піднявшись за останній рік на 5 позицій [4]. Фахівці відзначили прогресивні кроки у побудові законодавчої бази для забезпечення кібербезпеки держави, стійкість державних ініціатив щодо підвищення кібербезпеки у сфері ІКТ, значне покращення кіберстійкості організацій за останній рік, незважаючи на збільшення більш ніж удвічі цілеспрямованих кібератак.

Проте, якщо порівнювати показники України у цьому рейтингу з показниками, наприклад, інших країн пострадянського простору, то стає зрозуміло, що деякі з них провели набагато кращу роботу з побудови своєї кіберстійкості, позаяк вони суттєво випередили нас у GCI-2018. Так, Литва вийшла на 4 позицію загального рейтингу, Естонія – 5, Грузія – 18, Російська Федерація – 26, Казахстан – 40, Латвія – 44, Молдова – 53 і випередили нас у рейтингу.

Глобальний індекс NCSI проводиться та розробляється Академією електронного управління (e-Governance Academy). Цей інструмент вимірює готовність країн до запобігання кіберзагрозам та керування

кіберінцидентами і може бути використаний для вдосконалення національних можливостей кібербезпеки. Відповідно до показників рейтингу NCSI-2018 Україна посіла 27 місце. Країни пострадянського простору, які випередили нас у цьому рейтингу, заробили такі позиції: Естонія – 3, Литва – 6, Латвія – 12, Грузія – 18, а Російська Федерація – 22 [5].

Експерти рейтингу NCSI зосереджувались на вимірюванні аспектів кібербезпеки, впроваджених центральними урядами країн. Щодо нашої країни було відзначено гарні напрацювання у сфері запровадження політики кібербезпеки, захисту персональних даних, боротьби з кіберзлочинністю. Проте слабкими є позиції управління інцидентами та кризовими ситуаціями у сфері кібербезпеки, захисту електронних сервісів, аналізу та інформування громадськості про кіберзагрози.

Вітчизняні реалії кібербезпекової сфери свідчать про важливість підвищення рівня обізнаності щодо кібербезпеки на всіх рівнях: від діючих центрів комп'ютерної безпеки до розгортання освітніх програм з комп'ютерної безпеки. Особливої уваги за умов, що склалися, потребує розроблення ефективного плану заходів для здійснення «стрибка вперед» у сфері захисту як урядових, так і приватних комп'ютерних і телекомунікаційних мереж від внутрішніх і зовнішніх нападів, запобігання нанесенню збитків населенню та інфраструктурі від кібернетичних атак, створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Для покращення рівня управління кіберкризами уряд має створити план врегулювання кризових ситуацій для масштабних кіберінцидентів, проводити навчання з управління кіберкризами і врегулювання кризових ситуацій на національному рівні, брати участь у міжнародних заходах з управління кіберкризами, передбачити законодавчі процедури використання волонтерів у сфері кібербезпеки.

Задля розвитку національних можливостей з кібербезпеки державі треба докласти політичних, економічних і соціальних зусиль. До цього слід залучати правоохоронні органи, департаменти юстиції, освітні установи, міністерства, приватний сектор, розробників ІКТ, організовувати державно-приватне партнерство і внутрішньодержавне співробітництво з урахуванням довгострокової мети – збільшення зусиль щодо гарантування кібербезпеки в глобальному масштабі.

Список використаної літератури:

1. Трофименко О.Г. Щодо правового потенціалу безпечного функціонування кіберпростору / Трофименко О.Г., Дубовой Я.В. // Кібербезпека в Україні: правові та організаційні питання: матер. III всеукраїнської наук.-практ. конф. (30 листопада 2018 р.). – Одеса: ОДУВС. – С. 5–7.
2. Трофименко О.Г. Законодавча база забезпечення кібербезпеки держави / О.Г Трофименко // Кібербезпека в Україні: правові та організаційні питання: матер. II всеукр. наук.-практ. конф. (17 листопада 2017 р.). – Одеса: ОДУВС. С. 55–56.
3. Трофименко О.Г. Еволюція поглядів на інформаційні війни в епоху інформаційного суспільства / Трофименко О.Г., Дубовой Я.В. // Порівня-

льно-аналітичне право: електронне наукове фахове видання. – Ужгород, 2017. – № 1. – С. 189–192.
4. Global Cybersecurity Index (GCI) 2018. [Електронний ресурс] – Режим доступу: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf.
5. National Cyber Security Index (NCSI) 2018. [Електронний ресурс] – Режим доступу: https://www.ncsi.ega.ee/country/ua/.

Ключові слова: кібербезпека, кіберзагроза, кіберінцидент, кіберпростір.
Ключевые слова: кибербезопасность, киберугроза, киберинцидент, киберпространство.
Key words: cyber security, cyber threat, cyber incident, cyberspace.

ЧАНЫШЕВ РАШИД ИБРАГИМОВИЧ

Национальный университет «Одесская юридическая академия»,
доцент кафедры информационных технологий,
кандидат юридических наук, доцент

ПСИХОЛОГИЯ ИНТЕРНЕТА

Сравнительно недавно в научный обиход вошло новое понятие «Internet psychology» (Психология Интернета) или «Cyberpsychology» (Киберпсихология). Оно объединяет такие, казалось бы, далекие друг от друга понятия как «информационные технологии, информационная безопасность» и «психология» [1].

За последние 20 лет информационные технологии, связанные с использованием компьютерной техники, кардинально изменили жизнь значительной части человечества, почти вытеснив традиционные способы получения и обмена информацией, такие как печатные СМИ и телевидение. Не менее существенным стало и повсеместное использование облачных технологий, сделавшее возможным получение к личной информации с любого устройства в любой точке планеты, где существует возможность подключения к сети Интернет.

Эти изменения носят как позитивный, так и негативный характер. С одной стороны, доступ к информации стал легким как никогда в истории человечества, с другой стороны – именно эта легкость доступа привела к некоторой деградации, которую психологи обозначают термином «Google Syndrome» (Синдром Гугла) [2].

Если раньше, при чтении книг, человек старался запомнить получаемую им информацию, так как повторный доступ к ней был затруднен, то сегодня такой доступ можно получить за считанные секунды путем запроса в поисковой системе или путем перехода по сохранённой ссылке. В результате мозг человека не получает необходимой тренировки, что постепенно приводит к ослаблению памяти. Еще большую угрозу синдром Гугла представляет для подрастающего поколения, теряющего все психо-