DOI https://doi.org/10.30525/978-9934-588-63-1.22

# ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЗАКЛАДАХ ВИЩОЇ ОСВІТИ УКРАЇНИ

**Нашинець-Наумова А. Ю.**

## ВСТУП

Нині в умовах широкої доступності інтернету і стрімкого розвитку засобів зв'язку залишається помітним розрив між очікуваннями студентів і тими можливостями, які можуть запропонувати їм заклади вищої освіти (ЗВО). Форми та методи роботи в ЗВО мають постійно генерувати залежно від інформаційних потреб та технологічного розвитку суспільства. При цьому не останнє місце відводиться забезпеченню інформаційної безпеки як освітніх матеріалів та іншої інформації обмеженого доступу, так і самої ІТ-інфраструктури від випадкових або спрямованих атак. Заклад вищої освіти України переживає період адаптації не тільки щодо об'єктивних процесів інформаційного суспільства, а й щодо нових соціально-політичних умов із різноплановими проявами конкурентної боротьби. Створення ефективних механізмів управління інформаційними ресурсами системи вищої освіти в сучасних умовах неможливе без наукового обґрунтування та практичної реалізації збалансованої політики інформаційної безпеки ЗВО, яка може бути сформована на основі вирішення таких завдань[1]:

– аналіз процесів інформаційної взаємодії в усіх сферах основної діяльності ЗВО: інформаційних потоків, їх масштабу і якості, протиріч, конкурентної боротьби з виявленням власників і суперників;

– визначення ролі і місця політики інформаційної безпеки в управлінні інформаційними ресурсами ЗВО та вироблення узгоджуючих принципів і підходів;

– формулювання основних складників політики інформаційної безпеки: цілей, завдань, принципів і ключових напрямів забезпечення безпеки інформації ЗВО;

– розробка базових методик управління процесом забезпечення політики інформаційної безпеки;

– підготовка проектів нормативно-правових документів.

[1] Бєляков К. Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення. Київ, Україна : КВІЦ, 2008. С. 34.

Проблемам правового забезпечення інформаційної безпеки загалом та в закладах вищої освіти зокрема присвячені роботи К. Бєлякова, В. Богуша, Ю. Борсуковського, В. Борсуковської, О. Будіка, В. Бурячка, А. Зінюка, Л. Змія, О. Ільїна, О. Матвійчук-Юдіна, Л. Суркової, С. Сєрих, В. Чекуріна, О. Юдіна, О. Яковенка та інших.

Особливий інтерес становить монографія О.В. Олійника «Теоретико-методологічні засади адміністративно-правового забезпечення інформаційної безпеки України», в якій висвітлена генеза понять «інформаційна безпека», «інформаційні інтереси», подано категоріальний апарат проблем забезпечення інформаційної безпеки людини[2]. Ще одна монографія, на яку варто звернути увагу, присвячена адміністративно-правовим, психологічним і технологічним прийомам забезпечення інформаційної безпеки: автори В.Я. Настюк, В.В. Бєлєвцева характеризують поняття і зміст інформації, розглядають об'єкт адміністративно-правового захисту інформації, його особливості, на основі аналізу національного законодавства висвітлюють комплекс питань щодо проблем забезпечення правового захисту інформації в установах, а також подають пропозиції та рекомендації, спрямовані на вдосконалення цих законодавчих засад[3].

Окреме місце в системі правових досліджень інформаційної безпеки посідають теоретико-правові дослідження, покликані сформувати цілісну систему правових поглядів на вирішення проблем інформаційної безпеки. До завдань таких досліджень входить правове осмислення інформаційної безпеки як явища загалом і кожного з його складників окремо, визначення шляхів правового впливу на інформаційну безпеку та особливостей правових форм її забезпечення. Необхідно зазначити, що до правових досліджень згадуваної сфери належить і з'ясування взаємозв'язку інформаційної безпеки з іншими правовими явищами, вироблення концептуальних рекомендацій щодо вдосконалення інформаційного законодавства загалом і нормативно-правових актів, що визначають фундаментальні основи державної політики забезпечення інформаційної безпеки закладів вищої освіти зокрема.

Мета дослідження – створення ефективних механізмів щодо забезпечення інформаційної безпеки в закладах вищої освіти, а також управління інформаційними ресурсами системи вищої освіти.

Для розв'язання завдань дослідження здійснено аналіз наукового доробку публікацій вітчизняних та зарубіжних дослідників у сфері інформаційної безпеки. Дослідження пов'язане з виконанням завдань

[2] Олійник О. Теоретико-методологічні засади адміністративно-правового забезпечення інформаційної безпеки України. Київ : Укр. пріоритет, 2012. С. 56.

[3] Настюк В., Бєлєвцева В. Адміністративно-правовий захист інформації: проблеми та шляхи вирішення. Харків : Право, 2013. С. 88.

науково-дослідної індивідуальної теми «Концептуальні засади інформаційної безпеки в Україні як умови інноваційного розвитку держави та сучасного тренду суспільства», що виконується на кафедрі публічного та приватного права Факультету права та міжнародних відносин Київського університету імені Бориса Грінченка протягом 2019–2021 рр.

## 1. Заклад вищої освіти як об'єкт інформатизації

У сучасному закладі вищої освіти зберігається і обробляється величезна кількість різних даних, пов'язаних не тільки із забезпеченням навчального процесу, а й з науково-дослідними і проектно-конструкторськими розробками, персональні дані студентів і співробітників, службова, комерційна та інша конфіденційна інформація.

Зростання кількості злочинів у сфері високих технологій диктує свої вимоги до захисту ресурсів обчислювальних мереж навчальних закладів і ставить завдання побудови власної інтегрованої системи безпеки. Її рішення припускає наявність нормативно-правової бази, формування концепції безпеки, розробку заходів, планів і процедур щодо безпечної роботи, проектування, реалізацію і супровід технічних засобів захисту інформації в рамках закладу освіти. Ці складники визначають єдину політику забезпечення безпеки інформації у ЗВО.

Специфіка захисту інформації в освітній системі полягає в тому, що заклад вищої освіти – це публічний заклад із непостійною аудиторією, а також місце підвищеної активності «джуніорів» початківців-кіберзлочинців».

Основну групу потенційних порушників у ЗВО становлять студенти, низка мають досить високий рівень підготовки. Вік від 18 до 23 років та юнацький максималізм спонукають таких людей блиснути знаннями перед однокурсниками: влаштувати вірусну епідемію, отримати адміністративний доступ і «покарати» викладача, заблокувати вихід в інтернет тощо. Досить згадати, що перші комп'ютерні правопорушення народилися саме в закладі освіти (хробак Морріса)[4].

Особливості ЗВО як об'єкта інформатизації пов'язані також з багатопрофільним характером діяльності, великою кількістю форм і методів навчальної роботи, просторової розгалуженої інфраструктури (філії, представництва). Сюди ж можна зарахувати і різноманіття джерел фінансування, наявність розвиненої структури допоміжних підрозділів і служб (будівельна, виробнича, господарська діяльність), необхідність адаптації до мінливого ринку освітніх послуг, потреба в аналізі ринку праці, відсутність загальноприйнятої формалізації ділових процесів,

[4] История компьютерных вирусов. URL: http://ru.wikipedia.org/wiki/.

необхідність електронної взаємодії з вищими органами, часта зміна статусу співробітників та студентів.

Полегшує проблему те, що ЗВО має стабільну, ієрархічну за функціями управління систему, що володіє всіма необхідними умовами життєдіяльності і діє на принципах централізованого управління (останнє означає, що в управлінні завданнями інформатизації може активно використовуватися адміністративний ресурс).

Зазначені вище особливості зумовлюють необхідність дотримання вимог:

– комплексна проробка завдань інформаційної безпеки, починаючи з концепції і закінчуючи супроводом програмно-технічних рішень;

– залучення великої кількості фахівців, які володіють змістовною частиною ділових процесів;

– використання модульної структури корпоративних додатків, коли кожен модуль покриває взаємопов'язану групу ділових процедур або інформаційних сервісів при забезпеченні єдиних вимог до безпеки;

– застосування обґрунтованої послідовності етапів у вирішенні завдань інформаційної безпеки;

– документування розробок на базі раціонального використання стандартів, що гарантує створення успішної системи;

– використання надійних і масштабованих апаратно-програмних платформ і технологій різного призначення, що забезпечують необхідний рівень безпеки.

З точки зору архітектури в корпоративному інформаційному середовищі можна виділити три позиції, які необхідні для забезпечення безпечного функціонування ЗВО:

– обладнання обчислювальної мережі, каналів і ліній передачі даних, робочих місць користувачів, системи зберігання даних;

– операційні системи, мережеві служби і сервіси з управління доступом до ресурсів, програмне забезпечення середнього шару;

– прикладне програмне забезпечення, інформаційні сервіси і середовища, орієнтовані на користувачів.

У процесі створення комплексної інформаційної мережі (КІМ) необхідно забезпечити міжрівневе погодження розбіжностей між вимогами з безпеки до кінцевого рішення. Так, на другій позиції архітектура КІМ багатьох закладів освіти є розрізненою і слабо пов'язаною підсистемою з різними операційними середовищами, узгодженою одна з одною тільки на рівні закріплення IP-адресу або обміну повідомленнями. Причинами поганої системної організації КІМ є відсутність затвердженої архітектури КІМ, наявність кількох центрів відповідальності за розвиток технологій,

які діють неузгоджено. Проблеми починаються з небажання управляти вибором операційних середовищ у підрозділах, коли ключові технологічні рішення повністю децентралізовані, що різко знижує рівень безпеки системи. Нормативно-правовим підґрунтям створення такої системи мають бути закони України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», «Про доступ до публічної інформації», «Про основні засади забезпечення кібербезпеки України», «Про науково-технічну інформацію», «Про авторське право і суміжні права» тощо.

Заклади вищої освіти, які мають чітку стратегію розвитку інформаційних технологій, єдині вимоги до інформаційної інфраструктури, політику інформаційної безпеки і затверджені регламенти на основні компоненти КІМ, відрізняються, як правило, сильним адміністративним ядром в управлінні і високим авторитетом керівника ІТ-служби[5]. У таких ЗВО можуть, звичайно, використовуватися різні операційні середовища або системи середнього шару, але це зумовлено організаційно-технічними або економічними причинами, і не перешкоджають розгортанню КІМ закладу освіти, а також впровадженню уніфікованих принципів безпечного доступу до інформаційних ресурсів.

Стан розвитку у ЗВО третьої позиції архітектури КІМ можна охарактеризувати таким чином: в основному завершено перехід від локальних програмних додатків до корпоративних клієнт-серверних інформаційних систем, які забезпечують доступ користувачів до оперативних баз даних закладу освіти. У тому чи іншому вигляді вирішена задача інтеграції даних, породжених різними інформаційними системами, що дає змогу вдосконалити бізнес-процеси, підвищити якість управління і прийняття рішень.

Якщо на початку 90-х рр. XX ст. був високий попит на бухгалтерське програмне забезпечення і програмне забезпечення управлінського обліку (облік кадрів, звітність тощо), нині цей попит здебільшого задоволено.

## 2. Корпоративна мережа закладу вищої освіти

Активне впровадження інтернету та нових інформаційних технологій в освітній процес і систему управління ЗВО створило передумови до появи корпоративних мереж.

Корпоративна мережа ЗВО – це інформаційна система, що включає комп’ютери, сервери, мережеве обладнання, засоби зв’язку і

[5] Крюков В., Шахгельдян К. Информационные технологии в университете: стратегия, тенденции, опыт. *Университетское управление: практика и анализ*. 2012. № 4. С. 101–112.

телекомунікації, систему програмного забезпечення, призначену для вирішення завдань управління вузом і ведення освітньої діяльності.

Корпоративна мережа зазвичай об'єднує не тільки структурні підрозділи ЗВО, а й їх регіональні представництва. Раніше недоступні для ЗВО, нині ці мережі стали активно впроваджуватися в освітні структури у зв'язку з масовим поширенням інтернету та його доступністю[6].

Комплексна інформаційна безпека ЗВО – це система збереження, обмеження і авторизованого доступу до інформації, що міститься на серверах у корпоративних мережах навчального закладу, а також передана по телекомунікаційних каналах зв'язку в системах дистанційного навчання.

У ширшому сенсі термін «комплексна інформаційна безпека ЗВО» включає в себе два аспекти: систему захисту інтелектуальної інформаційної власності навчального закладу від зовнішніх і внутрішніх агресивних впливів і систему управління доступом до інформації та захисту від агресивних інформаційних просторів. Останнім часом, у зв'язку з неконтрольованим масовим розвитком інтернету, останній аспект безпеки стає особливо актуальним. Під терміном «інформаційний простір» розуміється інформація, що міститься на серверах у корпоративних мережах навчальних закладів, установ, бібліотек і в глобальній мережі Інтернет, на електронних носіях інформації, а також передана по телевізійних каналах зв'язку або телебаченню.

Агресивний інформаційний простір – це інформаційний простір, зміст якого може викликати прояви агресії в користувача як відразу ж після інформаційного впливу, так і через деякий час (віддалений ефект). Термін заснований на гіпотезі, що інформація в певних формах і змісті може викликати певні ефекти з проявом агресії і ворожості[7]. Проблеми комплексної інформаційної безпеки корпоративних мереж ЗВО набагато ширші, різноманітніші і гостріші, ніж в інших системах. Це пов'язано з такими особливостями:

– корпоративна мережа ЗВО будується зазвичай на концепції «мізерне фінансування»;

– як правило, корпоративні мережі не мають стратегічних цілей розвитку. Це означає, що топологія мереж, їх технічне і програмне забезпечення розглядаються з позицій поточних завдань;

– в одній корпоративній мережі ЗВО вирішуються дві основні задачі: забезпечення освітньої та наукової діяльності, а також вирішення завдання

[6] Минзов А. Особенности комплексной информационной безопасности корпоративных сетей вузов. URL: http://tolerance.mubiu.ru/base/Minzov(2).htm#top.

[7] Минзов А. Особенности комплексной информационной безопасности корпоративных сетей вузов. URL: http://tolerance.mubiu.ru/base/Minzov(2).htm#top.

управління освітнім і науковим процесами. Це означає, що одночасно в цій мережі працює кілька автоматизованих систем або підсистем у рамках однієї системи управління (АСУ «Студент», АСУ «Відділ кадрів», АСУ «Навчальний процес», АСУ «Бібліотека», АСУ «Бухгалтерія» тощо);

– корпоративні мережі гетерогенні як за обладнанням, так і програмним забезпеченням у зв'язку з тим, що створювалися протягом тривалого часу для різних завдань;

– плани комплексної інформаційної безпеки, як правило, або відсутні, або не відповідають сучасним вимогам.

У такій мережі можливі як внутрішні, так і зовнішні загрози безпеки інформації:

– спроби несанкціонованого адміністрування баз даних;

– дослідження мереж, несанкціонований запуск програм з аудиту мереж;

– видалення інформації;

– запуск ігрових програм;

– встановлення вірусних програм і троянських коней;

– спроби злому АСУ «ЗВО»;

– сканування мереж, в тому числі інших організацій, через інтернет;

– несанкціоноване відкачування з інтернету неліцензійного софту та встановлення його на робочі станції;

– спроби проникнення в системи бухгалтерського обліку;

– спроби несанкціонованого віддаленого адміністрування ОС;

– сканування портів тощо.

Джерелами можливих загроз інформації є:

– комп'ютеризовані навчальні аудиторії, в яких проходить навчальний процес;

– інтернет;

– робочі станції некваліфікованих у сфері інформаційної безпеки працівників навчального закладу.

Аналіз інформаційних ризиків можна розділити на етапи:

– класифікація об'єктів, які підлягають захисту;

– визначення привабливості об'єктів захисту для зломщиків;

– визначення можливих загроз і ймовірних каналів доступу на об'єкти;

– оцінка заходів безпеки;

– складання рангового списку загроз;

– оцінка збитку від несанкціонованого доступу, атак у відмові обслуговування, збоїв у роботі обладнання.

Основні об'єкти, які потребують захисту від несанкціонованого доступу:

– бухгалтерські дані, дані планово-фінансового відділу, а також статистичні і архівні дані;

– сервери баз даних;
– консоль управління обліковими записами;
– сервери дослідних проектів.

Необхідно зазначити, що зв'язок з інтернетом здійснюється відразу по кількох лініях зв'язку. Окремі канали надаються для зв'язку з іншими університетами або для безпечного обміну даними.

Щоб виключити ризики, пов'язані з витоком і псуванням переданої інформації, такі мережі не мають підключатися до глобальних мереж та загальної корпоративної мережі ЗВО. Критично важливі вузли для обміну даними ЗВО (наприклад, дані планово-фінансового відділу) також мають існувати окремо. Ризики стосуються і системи комплексної інформаційної безпеки. Вона має включати в себе вироблення наступних, не менш важливих політик. Перш за все, це фінансова політика розгортання, розвитку та підтримки в актуальному стані корпоративної мережі ЗВО. Вона є домінуючою, і її можна розділити на три напрями: мізерне фінансування, фінансування з розумною достатністю і пріоритетне фінансування. Друга політика визначається рівнем організації розгортання та супроводу корпоративної мережі ЗВО. Третя політика належить до кадрового складу інформаційного центру. Для навчального закладу вона особливо актуальна у зв'язку з підвищеною затребуваністю досвідчених системних адміністративістів. Політика технічного забезпечення може бути не цілком актуальна в умовах достатнього фінансування. Але завжди є проблема оновлення застарілого обладнання. Зрештою, остання політика пов'язана з формуванням морально-етичних норм толерантної поведінки в інформаційних системах і розумного обмеження від відвідувань агресивних інформаційних просторів. Недооцінка цих напрямів буде компенсуватися підвищеними фінансовими витратами на супровід корпоративних мереж ЗВО[8].

У процесі розгляду змісту забезпечення інформаційної безпеки в закладах вищої освіти нам не уникнути питань щодо впливу інформаційної безпеки на навчальний процес:

1) на рівні оцінки ризику безпеки загалом інформаційної інфраструктури навчального процесу ЗВО, коли оцінюється стан (ситуація) окремих груп компонентів інформаційної інфраструктури навчального процесу вузу, його вплив на вихідний продукт організації, і, відповідно, рекомендується фінансування того чи іншого напряму інформаційної інфраструктури навчального процесу. Така оцінка зазвичай проводиться один раз на рік під

[8] Юдін О., Матвійчук-Юдіна О., Яковенко О. Методи розробки та впровадження комплексної інформаційно-довідкової системи підтримки навчального процесу. Київ : ІПМЕ НАН України, 2007. С. 121.

час складання бюджету витрат із вдосконалення безпеки інформаційної інфраструктури навчального процесу ЗВО;

2) на рівні виконання навчального процесу. На цьому рівні необхідно проводити моніторинг інформаційної безпеки навчального процесу, виявляти ситуації порушення інформаційної безпеки навчального процесу, вимірювати вплив порушення інформаційної безпеки навчального процесу на вихідний продукт, а конкретніше, на знання студентів. За результатами таких вимірювань необхідно вживати оперативних заходів з усунення порушень інформаційної безпеки. Якість навчального процесу залежить від оперативності виправлення цих порушень, відповідно, необхідно вибрати період моніторингу та оперативного реагування на порушення нормативного, необхідного стану навчального процесу. Відповідним періодом із точки зору максимальної ефективності навчального процесу є академічна година. Однак можливий розгляд і інших періодів моніторингу і реагування: півдня, один день тощо. Вибір періоду моніторингу і реагування на порушення інформаційної безпеки навчального процесу залежить також від планованих витрат на систему моніторингу і реагування на порушення інформаційної безпеки навчального процесу: чим оперативніше реагування, тим більше воно вимагає витрат на створення і супровід системи моніторингу і реагування на порушення інформаційної безпеки навчального процесу. Таким чином, можна говорити про два типи ситуацій об’єкта дослідження, а саме інформаційної безпеки навчального процесу:

– ситуації стану безпеки інформаційної інфраструктури навчального процесу ЗВО, за якої оцінюється рівень можливих порушень інформаційної безпеки навчального процесу;

– ситуації порушення інформаційної безпеки навчального процесу, які оперативно виявляються під час навчального процесу.

У разі оцінки ситуації стану інформаційної інфраструктури навчального процесу ЗВО необхідна відповідна система реагування, спрямована на підвищення рівня безпеки інформаційної інфраструктури навчального процесу. У разі ситуації порушення інформаційної безпеки навчального процесу необхідна система оперативного ситуаційного управління забезпеченням інформаційної безпеки навчального процесу ЗВО.

## ВИСНОВКИ

Враховуючи вищевказане, пропонуємо вирішувати висвітлені проблеми в основних напрямах:

1) організація захищеного доступу до освітніх матеріалів і систем ЗВО з будь-якої точки світу;

2) захист інформації обмеженого доступу (персональні дані, комерційна таємниця тощо) і захист інтелектуальної власності;

3) виконання вимог законодавства в галузі інформаційної безпеки (захист персональних даних, захист прав на інтелектуальну власність).

Для цього необхідно врахувати наведене нижче.

I. Є різні групи користувачів.

Сучасний великий навчальний заклад і його корпоративна мережа – це багаторівневе ієрархічне середовище, в якому стикаються інтереси і дані різних груп користувачів. У навчальному закладі зустрічаються такі категорії користувачів: студенти університету та студенти, які приїхали в університет за обміном; професорсько-викладацький склад, співробітники та адміністрація; школярі, які відвідують підготовчі курси перед вступом до навчального закладу; відвідувачі платних курсів і курсів підвищення кваліфікації, що пропонуються навчальним закладом із метою отримання додаткових джерел доходів, а також представники організацій, що забезпечують навчальний заклад комерційними замовленнями, наприклад, НДР.

II. Є трансформація способів доступу.

Оскільки периметр класичної корпоративної інформаційної мережі навчального закладу продовжує розвиватися, смартфони, планшети та інші кінцеві пристрої з вебдодатками або спеціалізованими АРМа-ми невідворотно змінюють освітній процес, надаючи змогу отримувати доступ до навчальних сервісів за межами навчального закладу: з бібліотеки, гуртожитку, іншого навчального закладу тощо. Разом із тим у процесі впровадження концепції доступу до інформації виникає низка завдань, які необхідно вирішити в процесі забезпечення інформаційної безпеки. У такому разі треба забезпечити: запобігання несанкціонованого доступу пристроїв у захищений периметр навчального закладу, виконання вимог і рекомендацій політик інформаційної безпеки, забезпечення можливості контролю підключених до корпоративної мережі пристроїв на предмет відповідності чинним політикам інформаційної безпеки, забезпечення організацією логічного поділу корпоративної мережі на зони безпеки без зміни інфраструктури. Крім захисту інформації обмеженого доступу, необхідно забезпечувати безпеку інформаційних систем освітнього процесу. Випадкове або цілеспрямоване виведення цих систем із ладу може зупинити процес навчання і порушити договірні умови між навчальним закладом та студентом (у разі оплати освітніх послуг). Усе це підтримує або збільшує рівень конкурентоспроможності, продуктивності і безпеки навчального закладу. При цьому виникає низка завдань інформаційної безпеки, які необхідно вирішити:

– запобігання несанкціонованого підключення мережевих абонентських пристроїв: стаціонарних комп'ютерів, ноутбуків, мобільних пристроїв, мережевих принтерів і IP-телефонів до університетської мережі;

– виконання вимог і рекомендацій діючих політик інформаційної безпеки, а також забезпечення можливості віддаленого контролю;

– організація логічного поділу корпоративної мережі ЗВО на зони безпеки, без необхідності зміни інфраструктури, з метою виділення гостьових зон і зон обмеженого доступу для підключення абонентських пристроїв різних груп користувачів, а також мобільних пристроїв користувачів.

III. Є захист інформаційних систем та захист інформації обмеженого доступу.

Сучасний заклад вищої освіти – це джерело різноманітної інформації, яка потребує захисту. Це можуть бути персональні дані студентів, викладачів, адміністрації та інших категорій користувачів. Це можуть бути відомості, що становлять комерційну таємницю навчального закладу і дають йому змогу випереджати інші ЗВО у сфері надання більш якісної освіти, більш прогресивних методів навчання, кращих освітніх програм. Це можуть бути освітні матеріали, створені навчальним закладом, доступ до яких має бути або обмеженим, або контрольованим, тому що він являє собою інтелектуальну власність. Це можуть бути придбані навчальним закладом програмне забезпечення або ліцензії, крадіжка яких може погіршити становище закладу в конкурентній боротьбі або спричинити настання кримінальної або адміністративної відповідальності. Зрештою, захисту підлягають і результати тих НДР, які університет може проводити на замовлення комерційних або державних замовників. Крім захисту інформації обмеженого доступу, має бути забезпечена безпека інформаційних систем освітнього процесу, випадкове або цілеспрямоване виведення з ладу яких може зірвати як процес навчання, так і порушення договірних умов у разі платного навчання або реалізації різних НДР.

IV. Є законодавчі обмеження.

Крім захисту інформаційних систем та інформації, що дарують ЗВО конкурентні переваги, система забезпечення інформаційної безпеки має давати змогу виконувати і законодавчі ініціативи, спрямовані на захист прав та інтересів різних груп громадян і бізнес-організацій. До таких нормативно-правових актів, виконання яких вимагається від закладу вищої освіти насамперед належать закони України «Про доступ до публічної інформації», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних» та інші.

V. Є зростання числа загроз.

Середа загроз мережевої безпеки знаходиться в постійному розвитку. Варто зазначити, що лідируючі позиції в ній займають спеціально написані, приховані загрози, яким дедалі частіше вдається долати традиційні методи і засоби захисту. Ці загрози проникають усередину мережі, на рівень ядра, рівень поширення і рівень доступу користувачів, де захист від загроз і їх видимість знаходяться на мінімальному рівні. Звідти вони без проблем вибирають свої цілі – конкретні ресурси і навіть конкретних людей у навчальному закладі. Мета цих сучасних кіберзагроз полягає аж ніяк не в отриманні популярності і слави, і навіть не у створенні прибуткового ботнету, мета – в захопленні і крадіжці інтелектуальної власності або комерційних та інших таємниць для досягнення конкурентної переваги.

**АНОТАЦІЯ**

Нині проблеми правового забезпечення інформаційної безпеки в закладах вищої освіти дедалі частіше стають предметом обговорення в найширших наукових колах. При цьому, як правило, значна увага приділяється опису різних технічних рішень, аналізу переваг і недоліків відомих апаратних і програмних засобів та технологій захисту інформації і меншою мірою зачіпаються питання правового забезпечення інформаційної безпеки навчального закладу. У дослідженні проаналізовані особливості ЗВО як об’єкта інформатизації, специфіка захисту інформації в освітній системі, фактори ризику та погроз інформаційної безпеки в навчальних закладах. Розглянуто проблеми аналізу інформаційної структури корпоративної мережі ЗВО. Сформульовано основні принципи аналізу структури, внутрішні і зовнішні загрози безпеки інформації. Розкриті джерела можливих загроз інформації у структурі корпоративної мережі ЗВО. Запропоновано механізм захисту інформації в закладах вищої освіти, зокрема, враховуючи групи користувачів, трансформацію способу доступу до інформації, захист інформаційних систем та захист інформації обмеженого доступу.

**ЛІТЕРАТУРА**

1. Бєляков К. Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення. Київ : КВІЦ, 2008.

2. Бурячок В., Богуш В., Борсуковський Ю., Складанний П. Модель підготовки фахівців у сфері інформаційної та кібернетичної безпеки в закладах вищої освіти України. *Інформаційні технології та засоби навчання.* 2018. Т. 67, № 5. С. 277–291. URL: http://nbuv.gov.ua/UJRN/ITZN_2018_67_5_24.

3. Чекурін В., Будік О. Модель інформаційної системи ВНЗ та підхід до оцінювання її ризиків. *Вісник Національного університету «Львівська політехніка».* 2010. № 665. С. 83–90.

4. Зінюк А., Змій Л. Особливості забезпечення інформаційної безпеки в електронному навчанні. *Вісник Одеського національного університету. Соціологія і політичні науки.* 2016. Т. 21. Вип. 3. С. 33–40. URL: http://nbuv.gov.ua/UJRN/Vonu_sip_2016_21_3_5.

5. Ільїн О., Сєрих С. Когнітивна модель управління інформаційною безпекою вищого навчального закладу. *Сучасний захист інформації.* 2017. № 2(30). С. 24–29.

6. Юдін О., Матвійчук-Юдіна О., Яковенко О. Методи розробки та впровадження комплексної інформаційно-довідкової системи підтримки навчального процесу. Київ : ІПМЕ НАН України, 2007.

7. Сєркова Л. Інформаційна технологія моніторингу організації учбового процесу вищого навчального закладу : дис. … канд. техн. наук. ЧДТУ, Черкаси, 2006.

8. Олійник О. Теоретико-методологічні засади адміністративно-правового забезпечення інформаційної безпеки України. Київ : Укр. пріоритет, 2012.

9. Настюк В., Бєлєвцева В. Адміністративно-правовий захист інформації: проблеми та шляхи вирішення. Харків : Право, 2013.

10. История компьютерных вирусов. URL: http://ru.wikipedia.org/wiki/.

11. Крюков В., Шахгельдян К. Информационные технологии в университете: стратегия, тенденции, опыт. *Университетское управление: практика и анализ*. 2012. № 4. С. 101–112.

12. Минзов А. Особенности комплексной информационной безопасности корпоративных сетей вузов. URL: http://tolerance.mubiu.ru/base/Minzov(2).htm#top.

**Information about author:**
**Nashynets-Naumova A. Yu.,**
D.Sc. (Law), Associate Professor,
Deputy Dean of the Faculty of Law and International Relations
Borys Grinchenko Kyiv University
18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine