УДК 378.091(477):004.05

Нашинець-Наумова Анфіса Юріївна
доктор юридичних наук, доцент, заступниця декана з науково-методичної
та навчальної роботи Факультету права та міжнародних відносин
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID 0000-0002-5811-7733
a.nashynets-naumova@kubg.edu.ua

Бурячок Володимир Леонідович
доктор технічних наук, професор, завідувач кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID 0000-0002-4055-1494
v.buriachok@kubg.edu.ua

Коршун Наталія Володимирівна
доктор технічних наук, доцент, професор кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID 0000-0003-2908-970X
n.korshun@kubg.edu.ua

Жильцов Олексій Борисович
кандидат педагогічних наук, доцент, професор кафедри комп'ютерних наук та математики
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID 0000-0002-7253-5990
o.zhyltsov@kubg.edu.ua

Складанний Павло Миколайович
старший викладач кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Кузьменко Лідія Володимирівна
методист ІІ категорії центру перспективного планування та моніторингу освітньої діяльності
Національна академія Служби безпеки України, м. Київ, Україна
ORCID ID 0000-0001-7392-0324
lido4ok@gmail.com

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ І КІБЕРБЕЗПЕКИ В ЗАКЛАДАХ ВИЩОЇ ОСВІТИ УКРАЇНИ

Анотація. Зі збільшенням доступності Інтернету і стрімкого розвитку засобів комунікації, потреби в доступності до інформаційно-телекомунікаційних ресурсів, незалежно від місця їх надходження, постійно зростають. Одними з осередків таких ресурсів є заклади вищої освіти (ЗВО). Сучасні ЗВО і їх корпоративні мережі – це багаторівневе ієрархічне середовище, у якому стикаються інтереси і дані різних груп користувачів: студентів, науково-педагогічних працівників, адміністрації тощо. Оскільки периметр класичної корпоративної інформаційної мережі ЗВО продовжує розвиватися, саме застосування смартфонів, планшетів та інших кінцевих пристроїв з вебдодатками або спеціалізованими АРМ-ами сприяє невідворотній зміні освітнього процесу. Це, своєю чергою, надає користувачам можливість отримувати доступ до навчальних сервісів ЗВО знаходячись як в освітньому закладі, так і поза його межами. Разом з тим при впровадженні концепції доступу до інформації виникає цілий ряд завдань, які необхідно вирішити в процесі забезпечення інформаційної та кібербезпеки ЗВО, а саме: забезпечити: запобігання несанкціонованого доступу до приміщень ЗВО та його локальної мережі; виконання вимог і рекомендацій існуючих політик інформаційної та кібербезпеки; контроль підключених до корпоративної мережі пристроїв на предмет відповідності діючим політикам; логічний поділ корпоративної мережі на зони безпеки без зміни існуючої інфраструктури тощо. Крім захисту інформації обмеженого доступу, необхідно також забезпечити безпеку інформаційних систем ЗВО, зокрема, наприклад, такої системи, як «Електронний Університет». Випадкове або цілеспрямоване виведення цих

© А. Ю. Нашинець-Наумова, В. Л. Бурячок, Н. В. Коршун,
О. Б. Жильцов, П. М. Складанний, Л. В. Кузьменко, 2020.

систем з ладу може зупинити процес навчання і порушити договірні умови між навчальним закладом та студентом (у разі оплати освітніх послуг), нанести матеріальний, моральний та інший збиток громаді навчального закладу та ЗВО в цілому внаслідок проєктно-технологічної та/або інформаційної діяльності. Саме тому питання забезпечення інформаційної і кібербезпеки ЗВО нині є надзвичайно актуальним.

Ключові слова: інформаційна безпека; заклад вищої освіти; безпека інформаційних систем; інформаційно-телекомунікаційна система; кібербезпека; об’єкт інформаційної діяльності.

1. ВСТУП

Постановка проблеми. Сьогодні, в умовах широкої доступності Інтернету і стрімкого розвитку засобів зв'язку, існує дуже помітний розрив в очікуваннях студентів і тими можливостями, що можуть запропонувати їм заклади вищої освіти (ЗВО) України. За цих умов форми та методи освітньої діяльності у вітчизняних ЗВО повинні постійно оновлюватись залежно від інформаційних потреб та технологічного розвитку суспільства. Водночас не останнє місце в цьому процесі має займати забезпечення інформаційної та кібербезпеки як освітніх матеріалів та іншої інформації обмеженого доступу, так і самої ІТ-інфраструктури від випадкових або спрямованих атак.

Реалізація зазначених завдань ускладнюється тим, що ЗВО України переживають нині період адаптації не тільки до об’єктивних процесів інформаційного суспільства, а й до нових соціально-політичних умов з різноплановими проявами конкурентної боротьби. За таких умов створення ефективних механізмів управління інформаційними та ІТ-ресурсами ЗВО в сучасних умовах неможливо без [1, с. 34]:

- вироблення і вдосконалення комплексу узгоджених організаційних, нормативно-правових та технологічних заходів, спрямованих на захист інформації;
- формування і забезпечення системи інформаційної та кібербезпеки (ІКБ);
- координації діяльності структурних підрозділів при проведенні робіт щодо дотримання вимог забезпечення інформаційної та кібербезпеки.

Для їх практичної реалізації в ЗВО має бути:

по-перше, проведено комплекс превентивних заходів із захисту інформації, зокрема конфіденційних та персональних даних [2] з урахуванням рекомендацій загального регламенту про захист даних у країнах Євросоюзу щодо законності, обмеженості мети, мінімізації даних та їх точності, обмеження терміну зберігання даних, їх цілісності та підзвітності [3], а також інформаційних процесів, які містять вимоги до персоналу, менеджерів і технічних служб, аналіз інформаційних потоків, ризиків та оцінки захищеності інформації тощо;

по-друге, побудовано систему інформаційної і кібербезпеки з підсистемою управління, яка відповідатиме вимогам нормативно-правових документів та рекомендацій міжнародних стандартів у сфері захисту інформації, а також результатам інформаційного і технічного обстеження системи управління інформаційними та ІТ-ресурсами ЗВО тощо.

Аналіз останніх досліджень і публікацій. Проблемам організаційного, нормативно-правового та науково-техічного забезпечення інформаційної і кібербезпеки в цілому та в ЗВО зокрема присвячені роботи К.І. Бєлякова, В.М. Богуша, Ю.В. Борсуковського, О.О. Будіка, В.Л. Бурячка, А.В. Зінюка, Л.М. Змія, О.О. Ільїна, О.В. Матвійчук-Юдіна, Л.М. Суркової, С.О. Сєрих, В.Ф. Чекуріна, О.В. Юдіна, О.Г. Яковенка та інших [4-9].

Значну увагу фахівців привернула до себе монографія О.В. Олійника «Теоретико-методологічні засади адміністративно-правового забезпечення інформаційної безпеки

України», у якій висвітлена ґенеза поняття «інформаційна безпека», «інформаційні інтереси», подано категоріальний апарат проблем забезпечення інформаційної безпеки людини [10]. Організаційні, психологічні та технологічні прийоми забезпечення інформаційної безпеки розглянуто в монографії В.Я. Настюк та В.В. Бєлєвцева [9]. Автори цієї монографії характеризують поняття та зміст інформації, розкривають сутність інформаційної безпеки та її складових, розглядають види інформаційних правопорушень. Аналізуючи національне законодавство, вони висвітлюють комплекс питань щодо проблем забезпечення організаційного-правового захисту інформації в установах, а також надають пропозиції та рекомендації, спрямовані на вдосконалення цих законодавчих засад [11].

Окремої уваги в системі організаційних та нормативно-правових досліджень інформаційної і кібербезпеки заслуговують результати, покликані сформувати цілісну систему поглядів на вирішення проблем ІКБ. До головних напрямів таких досліджень належить правове осмислення інформаційної безпеки як явища загалом і кожної з його складників зокрема, визначення шляхів правового впливу на ІКБ та особливостей організаційних і правових форм її забезпечення. Необхідно зазначити, що до правових досліджень згадуваної сфери належить і з'ясування взаємозв'язку ІКБ з іншими правовими явищами, вироблення концептуальних рекомендацій щодо вдосконалення інформаційного законодавства загалом і нормативно-правових актів, які визначають фундаментальні основи державної політики забезпечення ІКБ ЗВО, зокрема.

Мета дослідження – розробка технології створення в закладах вищої освіти України системи інформаційної та кібербезпеки, спрямованої на комплексне управління станом захисту інформаційних та ІТ-ресурсів ЗВО, а також її всебічного забезпечення.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

У сучасному ЗВО зберігається і обробляється величезна кількість різних даних, пов'язаних не тільки із забезпеченням освітнього процесу, а й з науково-дослідними і проєктно-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 ЗВО і ставить завдання щодо побудови ними власної інтегрованої системи безпеки. Вирішення цього завдання потребує наявності нормативно-правової бази, формування концепції безпеки, розробки заходів, планів і процедур щодо безпечної роботи, проєктування, реалізації і супроводу технічних засобів захисту інформації в рамках закладу освіти. Ці складові визначають єдину політику забезпечення безпеки інформації в ЗВО.

Специфіка захисту інформації в освітній системі полягає в тому, що ЗВО, по-перше, це публічний заклад з непостійною аудиторією й, по-друге, це місце підвищеної активності «джуніорів» – «початківців кіберзлочинців», спроможних вчинити комп'ютерне правопорушення. Комп'ютерне (інформаційне) правопорушення – це суспільно небезпечне протиправне, винне діяння (дія або бездіяльність) деліктоздатної особи, що посягає на встановлений порядок в інформаційній сфері з використанням інформаційних засобів і інформаційних технологій. В Україні покарання в зазначеній сфері як міри адміністративної відповідальності мають різні форми – від морального попередження до адміністративного арешту. Основну групу потенційних порушників у ЗВО становлять студенти, певна частина яких має досить високий рівень практичної 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) [12].

Не менш важливою особливістю ЗВО є їх просторово-розгалужена інфраструктура (філії, представництва) та багатопрофільний характер їх діяльності, що супроводжується великою кількістю форм і методів навчальної роботи. Сюди ж можна віднести 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, необхідність електронної взаємодії з вищими органами, часта зміна статусу співробітників та студентів.

Зазначені вище особливості обумовлюють необхідність дотримання:

– принципу «рольового розподілу функцій» між користувачами і обслуговуючим персоналом, наприклад, табл.1;

Таблиця 1

Стислий перелік ролей, що належать до зони дії політики безпеки ЗВО

№	Найменування ролі	Опис функціональних обов'язків ролей
1	Адміністратор	Виконання налаштувань різних параметрів системи. Управління правами доступу до функцій і об'єктів системи. Моніторинг роботи користувачів і системи в цілому.
2	Студент	Доступ до тестових питань під час сесії. Перегляд особистої інформації.
3	Співробітник	Виконання доручень, резолюцій тощо. Підписання документів організації.
4	Викладач	Розробка і завантаження списку вибіркових дисциплін та тестових питань. Розробка і завантаження електронних навчальних курсів. Завантаження бакалаврських і магістерських випускових робіт.
5	Відповідальна особа	Доступ до інформації про (більш детальна інформація у табл.2): ведення ЗВО науково-дослідної роботи та про зміст такої роботи; створення в ЗВО нових технологічних апаратних, програмних, програмно-апаратних та топологічних рішень; проведення нарад, семінарів, конференцій та зустрічей з керівним складом підприємств-партнерів, замовників; стан охорони праці, держтехнагляду та техніки безпеки ЗВО; укладення договорів (контрактів) з юридичними та/або фізичними особами; захист інформації в ЗВО тощо.

– доступності оброблюваної інформації для зареєстрованих користувачів;

– конфіденційності інформації, що накопичується, зберігається та оброблюється на засобах обчислювальної техніки і передається каналами зв'язку, її цілісності та автентичності.

Водночас слід враховувати, що безпека ЗВО як об'єкта інформаційної діяльності (ОІД) не існує у виділеному середовищі та/або у відриві від життєдіяльності самого об'єкта – окремих корпусів ЗВО в межах контрольованих зон їх діяльності. Безпека ЗВО як об'єкта інформаційної діяльності має бути щільно інтегрованою до цього об'єкта.

Подоланню цих проблем може сприяти створення в ЗВО системи інформаційної та кібернетичної безпеки (СІКБ), яка була б здатна забезпечити ідентифікацію та автентифікацію користувачів, управляти їх доступом до інформації та ресурсів інформаційно-телекомунікаційної системи (ІТС) ЗВО, блокувати несанкціоновані дії та запобігати можливостям реалізації загроз порушення конфіденційності, цілісності та доступності інформації, запобігати інфікування АРМ ІТС комп'ютерними вірусами

тощо. Це передбачає наявність у корпоративному інформаційному середовищі ЗВО таких основних компонентів, необхідних для забезпечення його безпечного функціонування, як-от [13]:

- 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, програмного забезпечення середнього шару;
- прикладне програмне забезпечення, інформаційні сервіси і середовища, орієнтовані на користувачів.

Цілісна система управління зазначеними ресурсами в існуючій ІТС ЗВО або такій, що створюється, має будуватися на концепції єдиного системного підходу, який забезпечуватиме політика інформаційної та кібербезпеки (ПІКБ ЗВО), розроблена і затверджена ЗВО. 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.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Не зважаючи на те, що ІТС ЗВО будуються на концепціях системного підходу, вони за умов «мізерного фінансування» не мають, як правило, стратегічних цілей розвитку. Для вирішення таких глобальних задач, як забезпечення освітньої і наукової діяльності, а також управління освітнім і науковим процесами в ІТС ЗВО наявні декілька автоматизованих підсистем, які одночасно працюють у межах однієї системи управління. Такими підсистемами ІТС ЗВО можуть бути:

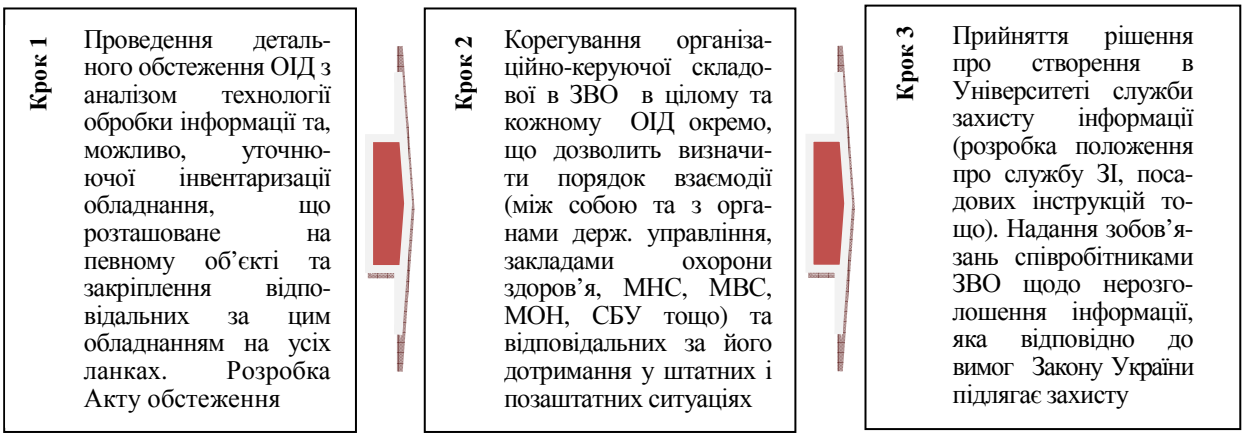
- підсистема авторизації користувачів в ІТС ЗВО для доступу до Інтернету;
- підсистема електронного документообігу ЗВО;
- підсистема бухгалтерського та планово-фінансового обліку ЗВО;
- підсистема організації дистанційного навчання та тестування студентів тощо.

Разом з цим, враховуючи, що створюються такі системи протягом тривалого часу й призначені для вирішення різних завдань, технології забезпечення безпеки в них або взагалі відсутні, або ж є занадто застарілими. Зважаючи на це, ЗВО прагне до створення надійної і ефективної системи захисту власних ресурсів. До системи захисту ЗВО передусім належать інформаційні ресурси, зокрема й такі, що надходять з мережі Інтернет. Водночас ЗВО прагне до створення ефективної системи захисту інформації, що накопичується, оброблюється й зберігається з використанням технічних можливостей ІТС ЗВО і підлягає захисту відповідно до вимог чинного законодавства України (наприклад, персональних даних науково-педагогічних працівників, обслуговуючого персоналу та студентів від несанкціонованих дій). Із врахуванням цього технологія створення в ЗВО України системи ІКБ, на наш погляд, має поєднувати такі основні етапи:

- *по-перше,* проведення обстеження ЗВО як об’єкту інформаційної діяльності;
- *по-друге,* розроблення технороботочого проєкту СІКБ ЗВО;
- *по-третє,* створення комплексу технічного захисту інформації, проведення попередніх випробувань та дослідної експлуатації СІКБ ЗВО;
- *по-четверте,* проведення державної експертизи СІКБ ЗВО (як для АС класу “3”) та супроводження СІКБ ЗВО протягом її життєвого циклу.

Розглянемо зазначені етапи більш детально.

Етап №1. Обстеження ЗВО, як ОІД.



Обстеження ЗВО, як ОІД проводиться з метою перевірки їх на предмет наявності:

– *планів ОІД з елементами електроживлення, заземлення, розміщення АТС, телефонних кабелів і апаратів, пожежної і охоронної сигналізації по поверхах;*

– *документів щодо системи охорони та контролю доступу до ОІД;*

– *документів, які містять опис загальної структурної схеми ІТС ЗВО: перелік і склад обладнання, технічних і програмних засобів; зв'язки обладнання, технічних і програмних засобів; особливості конфігурації, архітектури й топології ІТС; таблиці адресації ресурсів і компонент ІТС, таблиці маршрутизації та комутації;*

– *документів, які визначають види і характеристики каналів зв'язку ІТС;*

– *документів, які визначають особливості взаємодії окремих компонентів ІТС (взаємний вплив один на одного, взаємний вплив при взаємодії з ресурсами глобальної мережі Інтернет);*

– *документів на існуючі засоби контролю доступу до приміщень, де циркулює (знаходиться) інформація, яка підлягає захисту, а також на системи та технології, що обмежують доступ користувачів ІТС до певних ресурсів ІТС та зовнішніх мереж;*

– *документів на підсистеми та компоненти ІТС (технічні, програмні, програмно-апаратні тощо), які є засобами захисту інформації та/або містять механізми захисту інформації, потенційні можливості цих засобів і механізмів, їхні властивості і характеристики;*

– *документів, які регламентують схеми інформаційних потоків кожного елементу ІТС, склад інформаційних об'єктів, режим доступу до них, можливий вплив на нього елементів середовища користувачів, фізичного середовища;*

– *документів щодо обліку та порядку використання носіїв інформації в ІТС;*

– *опису спеціальних програмних засобів (підсистеми антивірусного захисту, підсистеми електронного документообігу тощо) щодо регламенту технології обробки інформації в ІТС та обігу електронних документів;*

– *діючих ліцензій на програмні засоби, які використовуються в ІТС;*

– *проєктної та експлуатаційної документації на ІТС, зокрема на встановлене гетерогенне мережеве обладнання та системи його захисту (міжмережеві екрани), а також інші програмно-апаратні засоби системи.*

За результатами обстеження має бути:

1) відновлено відсутні/втрачені документи, плани та описи або ж внесено зміни у застарілі;

2) сформовано «Перелік відомостей, що підлягають автоматизованому обробленню та відповідно норм права потребує захисту». Приклад такого переліку наведено у табл.2;
3) сформовано «Перелік службової інформації, персональних даних та відкритої інформації, яка накопичується, обробляється та зберігається в структурних підрозділах ЗВО»;
4) сформовано «Перелік загроз інформації, що обробляється в ІТС ЗВО».

Таблиця 2

Перелік відомостей, що повинні підлягати захисту у ЗВО

№ з/п	Найменування інформації	Гриф обмеж. доступу
1	Відомості про склад робіт, які виконуються ЗВО	
2	Відомості щодо ведення ЗВО науково-дослідної роботи та про зміст такої роботи	
3	Відомості про наукові, технічні та технологічні рішення, які є основними при виконанні робіт, що виконуються ЗВО	
4	Відомості про конкурентні наукові, технічні та технологічні рішення, які є результатом виконання науково-дослідних робіт та робіт по створенню в ЗВО нових технологічних апаратних, програмних, програмно-апаратних та топологічних рішень	
5	Відомості щодо проведення нарад, семінарів, конференцій та зустрічей з керівним складом підприємств-партнерів, замовників тощо	
6	Відомості, що отримуються або відправляються електронною поштою	
7	Оперативний аналіз стану працездатності технічних, програмних, програмно-апаратних засобів ЗВО	
8	Оперативний аналіз стану працездатності засобів енергопостачання ЗВО	
9	Оперативний аналіз стану охорони праці, держтехнагляду та техніки безпеки ЗВО	
10	Відомості щодо ведення раціоналізаторської та винахідницької роботи в ЗВО	
11	Відомості щодо ведення робіт режимно-секретним відділом ЗВО	
12	Відомості щодо змісту та результатів робіт, які виконуються за напрямом інформаційної та кібербезпеки, крім обумовлених окремими угодами та такими, що не підпадають під ЗВДТ	
13	Відомості щодо ведення в ЗВО кадрової роботи	
14	Відомості щодо проведення в ЗВО організаційно-штатних заходів	
15	Відомості щодо ведення обліку персоналу ЗВО	
16	Відомості, які пов’язані з укладанням договорів (контрактів) з юридичними та/або фізичними особами	
17	Відомості щодо звітності ЗВО до податкової інспекції та державних фондів	
18	Відомості щодо фінансово-господарської діяльності ЗВО	
19	Відомості щодо організації роботи локальної обчислювальної мережі ЗВО та технології її взаємодії з іншими обчислювальними мережами	
20	Відомості щодо порядку забезпечення цілодобового функціонування технологічного обладнання ЗВО	
21	Відомості щодо ведення баз даних систем обліку наданих послуг та автоматизованої бухгалтерії ЗВО	
22	Відомості про розробку та вдосконалення підрозділами ЗВО спеціального програмно-математичного забезпечення	
23	Відомості про результати іспитів створеного в ЗВО ПЗ та ПЗ сторонніх виробників	
24	Відомості щодо розробки документів, публікацій, методик з науково-дослідної роботи, експлуатації, функціонування обчислювальної техніки	
25	Накази та розпорядження адміністрації, керівна та плануюча документація ЗВО	
26	Відомості щодо захисту інформації в ЗВО	

5) формалізовано вимоги до перспективної СІКБ ЗВО. Визначено умови та шляхи реалізації: оперативно-тактичних і системотехнічних вимог до СІКБ ЗВО в цілому, а також вимог до підсистем СІКБ ЗВО;
6) розроблено проєкт варіанту Концепції СІКБ ЗВО, ключовими елементами якого мають бути:

по-перше, вимоги щодо базового забезпечення ІКБ в ЗВО, а саме до:

- *авторизованих і неавторизованих програмно-апаратних засобів та засобів управління вразливостями;*
- *захищених конфігурацій мобільних пристроїв, ноутбуків, робочих станцій і серверів тощо;*

по-друге, вимоги щодо застосування кращих практик в сфері ІКБ стосовно:

- *захисту електронної пошти та Webбраузеру;*
- *захисту від впливу шкідливих програм;*
- *обстеження і контролю мережевих портів;*
- *можливості відновлення втрачених даних;*
- *захищених конфігурацій для мережевих пристроїв (файєрволів, роутерів, комутаторів);*
- *захисту периметру і даних;*
- *контролю доступу та контролю облікових записів тощо;*

по-третє, вимоги щодо організаційних процесів і адміністративних заходів, пов'язаних із забезпеченням інформаційної та кібербезпеки ЗВО, а саме до:

- *процедур контролю рівня обізнаності персоналу та прикладного програмного забезпечення;*
- *технологій реагування на інциденти та процедур тестування на проникнення тощо.*

Алгоритм визначення вимог щодо забезпечення безпеки інформації в СІКБ ЗВО викладено на рис.1.

Рис.1. Алгоритм визначення вимог щодо забезпечення безпеки інформації в СІКБ ЗВО

Загрози інформації в ІТС ЗВО можуть мати як суб'єктивну, так і об'єктивну природу. Джерелом загроз суб'єктивного характеру можуть бути навмисні чи ненавмисні дії осіб (табл.3), які можуть мати віддалений доступ до ресурсів ІТС з використанням каналу доступу до мережі Інтернет або фізичний доступ у приміщення, де розміщена ІТС чи до її машинних носіїв інформації.

До загроз об'єктивного характеру належать:

– зміна умов фізичного середовища (вологість, запиленість, коливання температури). Джерело загрози – природні явища. Наслідки – порушення цілісності, доступності;

– збої і відмови в роботі обладнання та технічних засобів. Джерело загрози – апаратура. Наслідки – порушення цілісності, доступності, спостереження.

Таблиця 3

Джерела загроз інформації суб'єктивного характеру

Навмисні загрози	Ненавмисні загрози
✓ порушення фізичної цілісності ІТС (окремих компонентів, пристроїв, обладнання, носіїв інформації). Джерело загрози – люди. Наслідки – порушення цілісності, доступності, спостереження; ✓ порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ІТС (електроживлення або заземлення). Джерело загрози – люди. Наслідки – порушення цілісності, доступності; ✓ порушення режимів функціонування ІТС (обладнання і програмного забезпечення). Джерело загрози – люди, програми. Наслідки – порушення цілісності, доступності, спостереження; ✓ застосування комп'ютерних вірусів. Джерело загрози – люди, програми. Наслідки – порушення цілісності, доступності, спостереження; ✓ впровадження програмних закладок. Джерело загрози – люди, програми. Наслідки – порушення цілісності, доступності, спостереження; ✓ одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача ("маскарад"). Джерело загрози – люди, програми. Наслідки – порушення цілісності, доступності, спостереження; ✓ впровадження і використання забороненого політикою безпеки програмного забезпечення (неліцензійного) або несанкціоноване використання ПЗ. Джерело загрози – люди, програми. Наслідки – порушення цілісності, доступності, спостереження; ✓ навмисне пошкодження носіїв інформації. Джерело загрози – люди. Наслідки – порушення цілісності, доступності, спостереження; ✓ неправомірна зміна режимів роботи ІТС (окремих компонентів, обладнання, ПЗ тощо), ініціювання процесів тестування або технологічних, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації). Джерело загрози – люди, програми. Наслідки – порушення цілісності, доступності, спостереження; ✓ невиконання організаційних вимог розпорядчих документів, чинних для ЗВО Джерело загрози – люди. Наслідки – порушення цілісності, доступності, спостереження.	✓ ненавмисне ураження ПЗ комп'ютерними вірусами. Джерело загрози – люди, програми. Наслідки – порушення цілісності, доступності, спостереження; ✓ ненавмисне пошкодження машинних носіїв інформації. Помилки при введенні даних в ІТС. Джерело загрози – люди. Наслідки – порушення цілісності, доступності; ✓ ненавмисні дії, що можуть призвести до розголошення паролю адміністратора, втрати паролю тощо. Джерело загрози – люди. Наслідки – порушення цілісності, доступності, спостереження; ✓ ненавмисні дії, що можуть призвести до розголошення паролів користувачів, втрати паролів тощо. Джерело загрози – люди. Наслідки – порушення цілісності, доступності файлів користувачів; ✓ некомпетентне застосування засобів захисту. Джерело загрози – люди. Наслідки – порушення цілісності, доступності, спостереження.

Співвідношення можливих загроз з потенційно необхідними послугами безпеки на прикладі застосування неліцензійного ПЗ показано у таблиці 4.

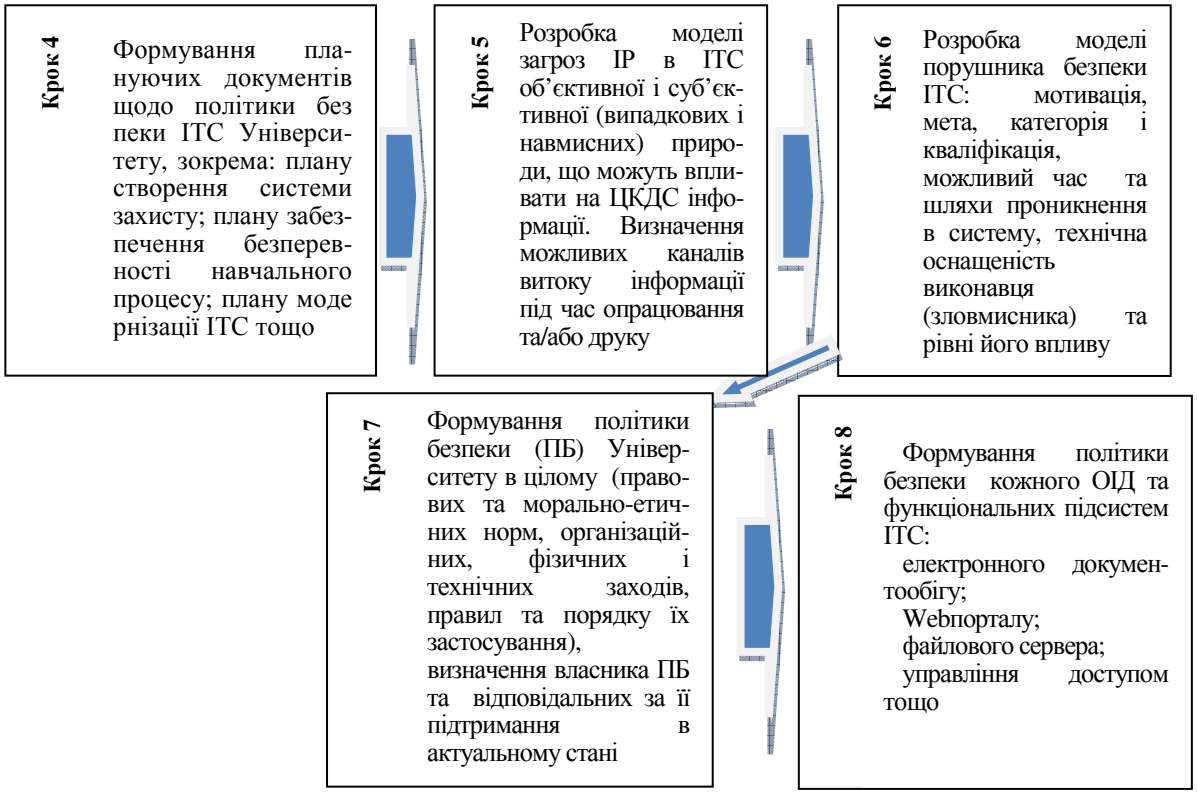
Таблиця 4

Співвідношення загроз і послуг безпеки на прикладі застосування неліцензійного програмного забезпечення

Послуги безпеки	Загрози безпеки				
	Знищення інформації та/або інших ресурсів	Викривлення та/або змінювання інформації	Крадіжка, видалення або втрата інформації	Розкриття інформації	Переривання обслуговування
Контроль доступу	так	так	так	так	
Аутентифікація			так	так	
Відмовостійкість	так	так	так	так	так
Конфіденційність			так	так	
Безпечність			так	так	
Цілісність	так	так			
Доступність	так				так
Секретність				так	

Етап №2. Розробка техноробочого проєкту СІКБ ЗВО.

Підетап №2.1. Розробка документації на СІКБ ЗВО.



Політика безпеки повинна доказово давати гарантії того, що в ЗВО забезпечується:

- адекватність рівня захисту інформації рівню її критичності;
- рентабельність реалізації заходів захисту інформації;
- оцінка та перевірка рівня захищеності інформації;
- персоніфікація положень політики безпеки (стосовно суб'єктів ЗВО);
- звітність (реєстрація, аудит) для всіх критичних з точки зору безпеки ресурсів;
- доступ персоналу і користувачів до всіх документів, які регламентують порядок захисту інформації та забезпечують їх суворе дотримання;
- неперервна робота засобів ІТС та можливість її поновлення в разі виникнення непередбачуваних ситуацій.

Політика інформаційної безпеки є частиною загальної ПБ ЗВО. Її побудова передбачає визначення структури цінностей і проведення аналізу ризику інформації, а також визначення правил для будь-якого процесу користування певним видом доступу до елементів інформації, які охоплюють коло питань, пов'язаних з оцінкою цінностей.

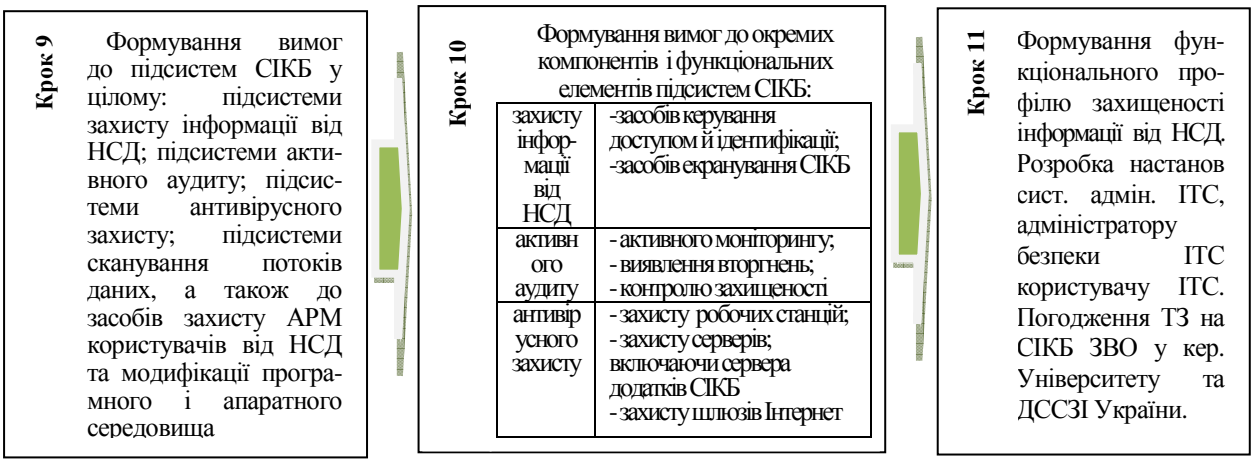
Підетап №2.2. Розробка Технічного завдання на створення СІКБ ЗВО.

Технічне завдання повинно визначати вимоги:

1) до організаційних заходів та комплексу засобів захисту (КЗЗ) ІТС ЗВО, що забезпечують безпеку інформації на всіх етапах її життєвого циклу, а також вимоги до порядку їх розробки, створення та впровадження;

2) стосовно розробки та реалізації політики інформаційної безпеки в ІТС ЗВО, тобто такого функціонального профілю захищеності інформації від НСД, який за рахунок застосування КЗЗ і набору певних правил *відповідатиме критеріям гарантій*, наприклад, на рівні Г-2 та *забезпечить на ОІД необхідний та/або достатній рівень*

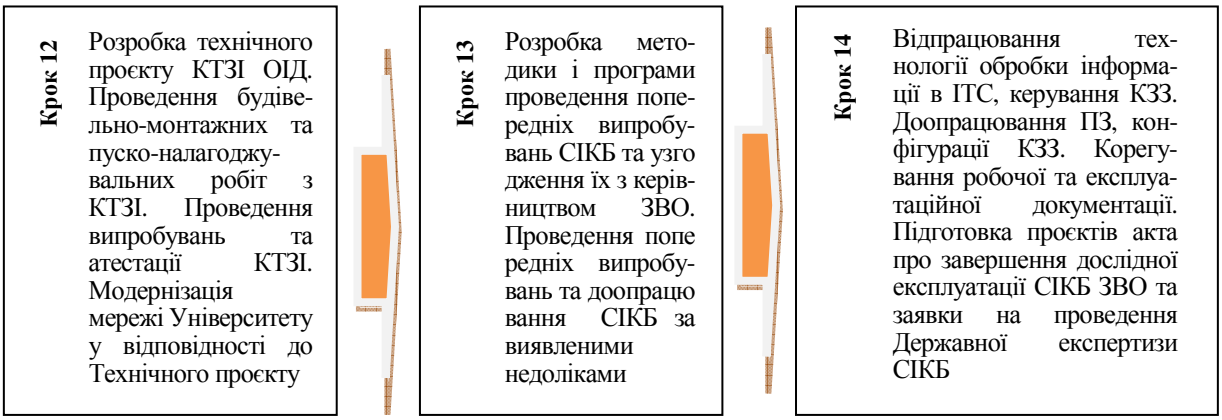
послуг щодо конфіденційності інформації в ІТС Університету, її цілісності та доступності, наприклад,



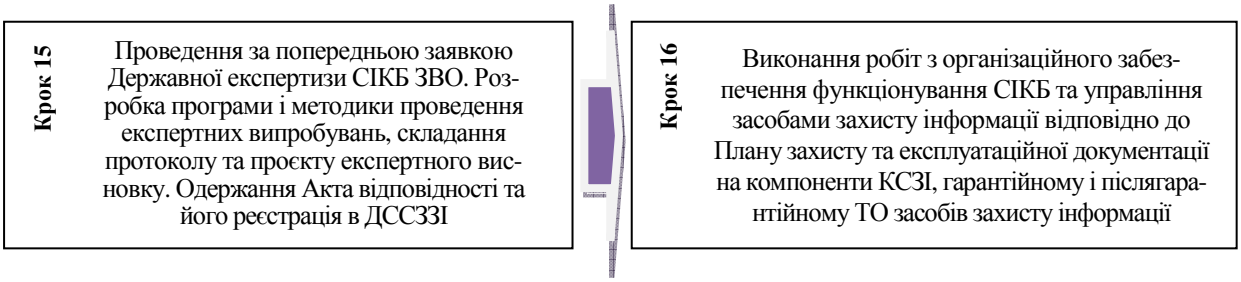
КД-2, ЦД-1, ЦО-1, ЦВ-1, ДЗ-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1

де КД-2 – базова довірча конфіденційність; ЦД-1 – мінімальна довірча цілісність; ЦО-1 – обмежений відкат; ЦВ-1 – мінімальна цілісність при обміні; ДЗ-1 – модернізація; ДВ-1 – ручне відновлення після збоїв; НР-2 – "Реєстрація" на рівні "Захищений журнал"; НИ-2 – одиночна ідентифікація і автентифікація користувачів; НК-1 – однонаправлений достовірний канал; НО-1 – виділення адміністратора; НЦ-1 – КЗЗ з контролем цілісності; НТ-1 – самотестування за запитом.

Етапи №3 - №5. Створення комплексу технічного захисту інформації, проведення попередніх випробувань, дослідної експлуатації та державної експертизи СІКБ ЗВО (як для АС класу "3")



Етапи №6 - №7. Проведення державної експертизи СІКБ ЗВО (як для АС класу "3") та її супроводження протягом життєвого циклу.



Календарний план щодо створення системи інформаційної та кібербезпеки в АС класу 3 довільного ЗВО наведено в табл.5.

Таблиця 5

Календарний план щодо створення СІКБ ЗВО за запропонованою технологією

№ етапу	Найменування етапу / підетапу створення СІКБ ЗВО	Виконавці	Вид продукції, кому подається	Термін
1	**ОБСТЕЖЕННЯ ЗВО як ОІД**	Замовник	1) Акт обстеження 2) Перелік інформації, що підлягає автоматизованій обробці та згідно з законодавством України потребує захисту 3) Положення про службу ЗІ та посадові інструкції її співробітників	
2	**ТЕХНОРОБОЧИЙ ПРОЄКТ СІКБ ЗВО**		Пояснювальна записка до технороботого проєкту	
2.1	Розробка документації на СІКБ ЗВО	Виконавець	1)План захисту інформації в ІТС 2) модель загроз 3) модель порушника 4) політика безпеки ЗВО 5) політика інформаційної безпеки 6) ПБ функціональних підсистем ОІД: електронного документообігу; Webпорталу; файлового сервера; управління доступом тощо	
2.2	Розробка Технічного завдання на створення СІКБ ЗВО	Виконавець	1) вимоги до підсистем СІКБ: підсистеми захисту інформації від НСД; підсистеми активного аудиту; підсистеми антивірусного захисту; підсистеми сканування потоків даних; захисту АРМ користувачів від НСД та модифікації програмного і апаратного середовища тощо; 2) вимоги до компонентів та функціональних елементів підсистем СІКБ: засобу керування доступом й ідентифікації; засобу екранування СІКБ. компоненти активного моніторингу; компоненти виявлення вторгнень; компоненти контролю захищеності. компоненти антивірусного захисту робочих станцій, серверів (разом із сервером додатків СІКБ) та шлюзів Інтернет 3) функціонального профілю захищеності інформації від НСД в ІТС Університету 4) ТЗ на створення СІКБ ЗВО, узгодженого з ДССЗЗІ України 5) Настанова системному адміністратору ІТС 6) Настанова адміністратору безпеки ІТС з інсталяції та ініціалізації ІТС Університету та конфігурування параметрів безпеки ІТС 7) Настанова користувачу ІТС з послуг безпеки	

3	**СТВОРЕННЯ КОМПЛЕКСУ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ КТЗІ СІКБ ЗВО**		Пояснювальна записка до технічного проєкту створення КТЗІ	
3.1	Будівельно-монтажні роботи	Виконавець	Акт виконаних робіт	
3.2	Встановлення та налагодження технічних засобів. Пусконалагоджувальні роботи	Виконавець	1) Акт встановлення категорій технічних засобів. 2) Паспорт на КТЗІ	
3.3	Розробка Програми та методики випробувань КТЗІ	Виконавець	1) Програма та методика випробувань КТЗІ 2) Акти інсталяції програмного забезпечення	
3.4	Проведення випробувань КТЗІ	Виконавець	Протокол випробувань КТЗІ	
3.5	Проведення атестації КТЗІ	Виконавець	Акт атестації КТЗІ	
4	**ПОПЕРЕДНІ ВИПРОБУВАННЯ СІКБ ЗВО**		Протокол попередніх випробувань СІКБ	
4.1	Розробка методики проведення попередніх випробувань СІКБ ЗВО та її узгодження із Замовником.	Виконавець	Методика проведення попередніх випробувань СІКБ	
4.2	Розробка Програми проведення випробувань СІКБ ЗВО	Виконавець	Програма проведення попередніх випробувань СІКБ	
4.3	Випробування СІКБ ЗВО та її доопрацювання за виявленими недоліками	Замовник Виконавець	Протокол випробувань	
4.4	Підготовка проєкту акта приймання СІКБ ЗВО у дослідну експлуатацію	Замовник	Акт приймання СІКБ у дослідну експлуатацію	
5	**ДОСЛІДНА ЕКСПЛУАТАЦІЯ СІКБ ЗВО**		Акт про завершення дослідної експлуатації СІКБ	
5.1	Відпрацювання технології обробки інформації в ІТС, керування КЗЗ	Замовник	Наказ про проведення дослідної експлуатації ІТС СІКБ	
5.2	Доопрацювання ПЗ, конфігурації КЗЗ	Виконавець		
5.3	Корегування робочої та експлуатаційної документації	Замовник Виконавець	1) Інструкція щодо забезпечення безпеки інформації в ІТС 2) Інструкція щодо порядку забезпечення антивірусного захисту інформації в ІТС 3) Журнал обліку роботи на ПЕОМ 4) Журнал обліку копіювання інформації на ПЕОМ 5) Журнал обліку стирання інформації на ПЕОМ	

5.4	Підготовка проєктів актів про завершення дослідної експлуатації СІКБ та заявки на проведення Державної експертизи СІКБ	Замовник	Заявка на проведення Державної експертизи СІКБ	
6	**ДЕРЖАВНА ЕКСПЕРТИЗА СІКБ ЗВО**	Експертів визначає організатор екс-пертизи	1) Атестат відповідності. Його реєстрація в Адміністрації Держспецзв'язку України 2) Акт приймання – передавання послуг	
7	**СУПРОВОДЖЕННЯ СІКБ ЗВО**	Виконавець	Виконання робіт з організаційного забезпечення функціонування СІКБ та управління засобами захисту інформації відповідно до Плану захисту та експлуатаційної документації на компоненти СІКБ, гарантійному і післягарантійному технічному обслуговуванню засобів захисту інформації	

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті розглянуто технологію створення в ЗВО системи ІКБ, спрямованої на комплексне управління станом захисту інформаційних та ІТ-ресурсів ЗВО від несанкціонованих дій, які можуть призвести до порушення їх цілісності та доступності, зокрема з використанням комп'ютерних вірусів, а також всебічного забезпечення процесу функціонування системи. З цією метою в роботі запропоновано:

- *по-перше*, проводити обстеження ЗВО як об'єкта інформаційної діяльності;
- *по-друге*, розробляти техноробочий проєкт СІКБ ЗВО;
- *по-третє*, створювати комплекс технічного захисту інформації, проводити попередні випробування та дослідну експлуатацію СІКБ ЗВО;
- *по-четверте*, проводити державну експертизу СІКБ ЗВО (як для АС класу "3") та супроводжувати СІКБ ЗВО протягом її життєвого циклу.

Система інформаційної та кібербезпеки ЗВО, створена з дотриманням запропонованої технології [14-19], забезпечить: ідентифікацію та автентифікацію користувачів; керування та контроль доступу користувачів до ресурсів ІТС ЗВО; блокування несанкціонованих дій та запобігання можливостям реалізації загроз порушення цілісності та доступності інформації; запобігання інфікування АРМ ІТС ЗВО комп'ютерними вірусами та їх подальшого розповсюдження з використанням знімних носів інформації; забезпечення реєстрації даних про події, що відбуваються в системі і стосуються безпеки інформації. Певні аспекти запропонованої технології було досліджено в науково-дослідних роботах «Сучасні тенденції розвитку національної правової системи» (Державний реєстраційний номер: 0116U004626) та «Методи та засоби забезпечення функціональної та кібербезпеки програмно-технічних систем критичного застосування в умовах впливу інформаційних загроз, ризиків та невизначеностей», що протягом останніх років виконуються в Київському університеті імені Бориса Грінченка.

Подальші дослідження будуть орієнтовані на формування загальної моделі побудови системи ІКБ ЗВО з урахуванням: рекомендацій GDPR як стандарту ЄС щодо захисту персональних даних; організаційно-технічних аспектів взаємодії елементів системи ІКБ ЗВО щодо доступу до авторизованих та Webресурсів; ротації контингенту студентів і співробітників ЗВО; необхідності захисту критично важливих сегментів ЗВО, передусім таких, як бухгалтерія, відділ кадрів, режимно-секретний орган тощо;

необхідності моніторингу нових загроз, визначення ризиків та рівнів їх інтенсивності. Разом з цим планується розглянути можливість адаптації до застосування в системі ІКБ ЗВО підсистеми передачі та архівації зображень PACS (Picture Archiving and Communication System) як потенційно можливого запобіжника несанкціонованого доступу до мережі на території ЗВО.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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

[2] Закон України «Про захист персональних даних», від 01.06.2010 № 2297-VI. [Електронний ресурс]. Доступно: https://www.kadrovik01.com.ua/article/3659-qqq-17-m4-normativna-baza-ta-termnologya-u-sfer-zahistu-personalnih-danih

[3] EU General Data Protection Regulation, EU GDPR. [Електронний ресурс].Доступно: https://www.kingston.com/ru/ solutions/data-security/eu-gdpr

[4] В. Бурячок, В. Богуш, Ю. Борсуковський, П. Складанний, та В. Борсуковська, "Модель підготовки фахівців у сфері інформаційної та кібернетичної безпеки в закладах вищої освіти України", *Інформаційні технології та засоби навчання,* т. 67, № 5, с. 277-291, 2018. [Електронний ресурс]. Доступно: http://nbuv.gov.ua/UJRN/ITZN_2018_67_5_24 Дата звернення: Тра. 20, 2019.

[5] В. Чекурін, та О. Будік, "Модель інформаційної системи ВНЗ та підхід до оцінювання її ризиків", *Вісник Національного університету "Львівська політехніка"*, № 665, с. 83-90, 2010.

[6] А. Зінюк, та Л. Змій, "Особливості забезпечення інформаційної безпеки в електронному навчанні", *Вісник Одеського національного університету. Соціологія і політичні науки,* Т. 21, Вип. 3. с. 33-40, 2016. [Електронний ресурс]. Доступно: http://nbuv.gov.ua/UJRN/Vonu_sip_2016_21_3_5 Дата звернення: Тра. 20, 2019.

[7] О. Ільїн, та С. Сєрих, "Когнітивна модель управління інформаційною безпекою вищого навчального закладу", *Сучасний захист інформації,* №2(30), с. 24-29. 2017.

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

[9] Л. Сєркова, "Інформаційна технологія моніторингу організації учбового процесу вищого навчального закладу", дис. канд. техн. наук., ЧДТУ, Черкаси, 2006.

[10] О. Олійник, *Теоретико-методологічні засади адміністративно-правового забезпечення інформаційної безпеки України*. Київ, Україна: Укр. пріоритет, 2012.

[11] В. Настюк, та В. Бєлєвцева, *Адміністративно-правовий захист інформації: проблеми та шляхи вирішення*. Харків, Україна: Право, 2013.

[12] История компьютерных вирусов. [Електронний ресурс]. Доступно: http://ru.wikipedia.org/wiki/. Дата звернення: Тра. 15, 2019.

[13] А. Минзов, *Особенности комплексной информационной безопасности корпоративных сетей вузов.* [Електронний ресурс]. Доступно: /http://tolerance.mubiu.ru/base/Minzov(2).htm#top. Дата звернення: Тра. 17, 2019.

[14] ДСТУ 3396.2-97 *Захист інформації. Технічний захист інформації. Терміни і визначення*. [Чинний від 1998-01-01]. Вид. офіц. Київ, Україна: Держстандарт України, 1997.

[15] ДСТУ 2938-94 *Система оброблення інформації. Основні поняття. Терміни і визначення*. [Чинний від 1996-01-01]. Вид. офіц. Київ, Україна: Держстандарт України, 1995.

[16] НД ТЗІ 1.1-003-99 *Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу*. [Чинний від 1999-07-01]. Вид. офіц. Київ, Україна: ДСТСЗІ СБ України, 1999.

[17] НД ТЗІ 2.5-004-99 *Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу*. [Чинний від 1999-04-28]. Вид. офіц. Київ, Україна: ДСТСЗІ СБ України, 1999.

[18] НД ТЗІ 2.5-010-03 *Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.* [Чинний від 2003-04-02]. Вид. офіц. Київ, Україна: ДСТСЗІ СБ України, 2003.

[19] НД ТЗІ 2.5-008-02 *Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу "2"*.[Чинний від 2002-13-12]. Вид. офіц. Київ, Україна: ДСТСЗІ СБ України, 2002.

Матеріал надійшов до редакції 01.10.2019р.

ТЕХНОЛОГИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ И КИБЕРБЕЗОПАСНОСТИ В УЧРЕЖДЕНИЯХ ВЫСШЕГО ОБРАЗОВАНИЯ УКРАИНЫ

Нашинец-Наумова Анфиса Юрьевна
доктор юридических наук, доцент, заместитель декана по научно-методической и учебной работе факультета права и международных отношений
Киевский университет имени Бориса Гринченко, г. Киев, Украина
ORCID ID 0000-0002-5811-7733
a.nashynets-naumova@kubg.edu.ua

Бурячок Владимир Леонидович
доктор технических наук, профессор, заведующий кафедрой информационной и кибернетической безопасности
Киевский университет имени Бориса Гринченко, г. Киев, Украина
ORCID ID 0000-0002-4055-1494
v.buriachok@kubg.edu.ua

Коршун Наталия Владимировна
доктор технических наук, доцент, профессор кафедры информационной и кибернетической безопасности
Киевский университет имени Бориса Гринченко, г. Киев, Украина
ORCID ID 0000-0003-2908-970X
n.korshun@kubg.edu.ua

Жильцов Алексей Борисович
кандидат педагогических наук, доцент, профессор кафедры компьютерных наук и математики
Киевский университет имени Бориса Гринченко, г. Киев, Украина
ORCID ID 0000-0002-7253-5990
o.zhyltsov@kubg.edu.ua

Складанный Павел Николаевич
старший преподаватель кафедры информационной и кибернетической безопасности
Киевский университет имени Бориса Гринченко, г. Киев, Украина
ORCID ID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Кузьменко Лидия Владимировна
методист II категории центра перспективного планирования и мониторинга образовательной деятельности,
Национальная академия Службы безопасности Украины, г. Киев, Украина
ORCID ID 0000-0001-7392-0324
lido4ok@gmail.com

Аннотация. С увеличением доступности Интернета и стремительного развития средств коммуникации, потребности в доступности информационно-телекоммуникационных ресурсов, независимо от места их поступлення, постоянно растут. Одними из ячеек таких ресурсов является учреждения высшего образования (УВО). Современные УВО и их корпоративные сети – это многоуровневое иерархическое окружение, в котором сталкиваются интересы и данные различных групп пользователей: студентов, научно-педагогических работников, администрации и т.п. Поскольку периметр классической корпоративной информационной сети УВО продолжает развиваться, именно применение смартфонов, планшетов и других конечных устройств с веб-приложениями или специализированными АРМ-ами способствует неотвратимому изменению образовательного процесса. Это, в свою очередь, предоставляет пользователям возможность получать доступ к учебным сервисам УВО находясь как в образовательном учреждении, так и за его пределами. Вместе с тем при внедрении концепции доступа к информации возникает целый ряд задач, которые необходимо решить в процессе обеспечения информационной и кибербезопасности УВО, а именно обеспечить: предотвращение несанкционированного доступа в помещения УВО и его локальные сети; выполнение требований и рекомендаций существующих политик информационной и кибербезопасности; контроль подключенных к корпоративной сети устройств на предмет соответствия действующим политикам; логическое разделение корпоративной сети на зоны безопасности без изменения существующей инфраструктуры и т.п. Кроме защиты информации ограниченного доступа, необходимо также обеспечить безопасность информационных систем УВО, в частности, например, такой системы, как «Электронный Университет». Случайное или целенаправленное выведение этих систем из строя может остановить процесс обучения и нарушить договорные условия между учебным заведением и студентом (в случае оплаты

образовательных услуг), нанести материальный, моральный и иной ущерб коллективу учебного заведения и УВО в целом вследствие проектно-технологической и / или информационной деятельности. Именно поэтому вопросы обеспечения информационной и кибербезопасности УВО сейчас являются чрезвычайно актуальными.

Ключевые слова: информационная безопасность; учреждение высшего образования; безопасность информационных систем; информационно-телекоммуникационная система; кибербезопасность; объект информационной деятельности.

TECHNOLOGY FOR INFORMATION AND CYBER SECURITY IN HIGHER EDUCATION INSTITUTIONS OF UKRAINE

Anfisa Yu. Nashynets-Naumova
Doctor of Law, Associate Professor, Deputy Dean of the Faculty of Law and International Relations
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID 0000-0002-5811-7733
a.nashynets-naumova@kubg.edu.ua

Volodymyr L. Buriachok
Doctor of Technical Sciences, Professor, Head of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID 0000-0002-4055-1494
v.buriachok@kubg.edu.ua

Natalia V. Korshun
Doctor of Technical Sciences,
Associate Professor, Professor at the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID 0000-0003-2908-970X
n.korshun@kubg.edu.ua

Oleksii B. Zhyltsov
PhD of Pedagogical Sciences,
Associate Professor, Professor at the Department of Information Technology and Mathematics
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID 0000-0002-7253-5990
o.zhyltsov@kubg.edu.ua

Pavlo M. Skladannyi
Senior Lecturer at the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Lidia V. Kuzmenko
Methodist of the second category at the Center for Advanced Planning and Monitoring of Educational Activities,
National Academy of Security Service of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0001-7392-0324
lido4ok@gmail.com

Abstract. With the increasing availability of the Internet and the rapid development of communication tools, the need for the availability of information and telecommunication resources, regardless of where they are received, is constantly growing. One of the cells of such resources is the institution of higher education (IHE). Modern IHE and their corporate networks are a multi-level hierarchical environment in which the interests and data of various user groups collide: students, research workers, administration, etc. As the perimeter of the classic corporate information network of IHE continues to evolve, it is the use of smartphones, tablets and other end devices with web applications or specialized workstations that contributes to the inevitable change in the educational process. This, in turn, provides users with the opportunity to access the training services of IHE while in the educational institution, and beyond. At the same time, when introducing the concept of access to information, a whole series of tasks arises that need to be solved in the process of ensuring information and cyber security of IHE, namely, to ensure: prevention of unauthorized access to IHE premises and its local networks; compliance with the requirements and recommendations of existing information and cybersecurity policies; Monitoring devices connected to the corporate network for compliance with applicable policies; logical division of the corporate network into security zones

without changing the existing infrastructure, etc. In addition to protecting information of limited access, it is also necessary to ensure the security of information systems of IHE, in particular, for example, of such a system as “Electronic University”. Accidental or deliberate disabling of these systems can stop the learning process and violate the contractual conditions between the educational institution and the student (in the case of payment for educational services), cause material, moral and other damage to the staff of the educational institution and IHE as a whole due to design and technological and / or information activities. That is why the issues of ensuring information and cybersecurity of IHE are now extremely relevant.

Keywords: information security; higher education institution; security of information systems; information and telecommunication system; cyber security; object of information activity.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] K. Belyakov, *Informatization in Ukraine: Problems of Organizational, Legal and Scientific Support.* Kyiv, Ukraine: KVIC, 2008. (in Ukrainian).

[2] Law of Ukraine «Protection of personal data», 01.06.2010 № 2297-VI. [Online]. Available: https://www.kadrovik01.com.ua/article/3659-qqq-17-m4-normativna-baza-ta-termnologya-u-sfer-zahistu-personalnih-danih . Accessed on: December 02, 2019 (in Ukrainian).

[3] EU General Data Protection Regulation, EU GDPR. [Online]. Available:: https://www.kingston.com/ru/solutions/data-security/eu-gdpr . Accessed on: December 02, 2019 (in Russian).

[4] V. Buriachok, V. Bogush, Y. Borsukovsky, P. Skladnannyi, and V. Borsukovskaya, "Model of training specialists in information and cyber security in higher education institutions of Ukraine", Information Technologies and Learning Tools, vol. 67, № 5, pp. 277-291, 2018. [Online]. Available: http://nbuv.gov.ua/UJRN/ITZN_2018_67_5_24 Accessed on: May 20, 2019. (in Ukrainian).

[5] V. Chekurin, and O. Budik, "Model of the University Information System and Approach to Assessing its Risks", *Visnyk Natsionalnoho universytetu "Lvivska politekhnika"*, № 665, pp. 83-90, 2010. (in Ukrainian).

[6] A. Zinyuk, and L. Zmij, "Features of Information Security in E-Learning", *Visnyk Odeskoho natsionalnoho universytetu. Sotsiolohiia i politychni nauky,* vol. 21, №. 3. pp. 33-40, 2016. [Online]. Available: http://nbuv.gov.ua/UJRN/Vonu_sip_2016_21_3_5 Accessed on: May 20, 2019. (in Ukrainian).

[7] O. Ilyin, and S. Serykh, "The Cognitive Model of Information Security Management at a Higher Education Institution", *Suchasnyi zakhyst informatsii*, № 2 (30), pp. 24-29. 2017. (in Ukrainian).

[8] O. Yudin, O. Matviychuk-Yudin, and O. Yakovenko, *Methods of development and implementation of a comprehensive information and reference system for supporting the educational process.* Kyiv, Ukraine: IPME NAS of Ukraine, 2007. (in Ukrainian).

[9] L. Serkova, "Information Technology of Monitoring the Organization of the Educational Process of Higher Education", (Master’s thesis). CHDTU, Cherkasy, 2006. (in Ukrainian).

[10] O. Oliynyk, *Theoretical and methodological principles of administrative and legal support of information security of Ukraine*. Kyiv, Ukraine: Ukr. priorytet, 2012. (in Ukrainian).

[11] V. Nastyuk, and V. Belevtseva, *Administrative and Legal Protection of Information: Problems and Solutions*. Kharkiv, Ukraine: Pravo, 2013. (in Ukrainian).

[12] History of computer viruses. [Online]. Available: http://en.wikipedia.org/wiki/. Accessed on: May 15, 2019. (in Russian).

[13] A. Minzov, *Features of complex information security of corporate networks of universities.* [Online]. Available: /http://tolerance.mubiu.ru/base/Minzov(2).htm#top. Accessed on: May 17, 2019. (in Russian).

[14] DSTU 3396.2-97 Protection of information. Technical protection of information. Terms and definitions. [Valid from 1998-01-01]. Kind. offic. Kyiv, Ukraine: Derzhstandart Ukrainy, 1997. (in Ukrainian).

[15] DSTU 2938-94 Information Processing System. Basic concepts. Terms and definitions. [Valid from 1996-01-01]. Kind. offic. Kiev, Ukraine: Derzhstandart Ukrainy, 1995. (in Ukrainian).

[16] NDI 1.1 003 99 Terminology for the protection of information on computer systems against unauthorized access. [Valid from 1999-07-01]. Kind. offic. Kiev, Ukraine: DSTSI SB of Ukraine, 1999. (in Ukrainian).

[17] NDI 2.5-004-99 *Criteria for evaluating the security of information on computer systems against unauthorized access*. [Valid from 1999-04-28]. Kind. offic. Kiev, Ukraine: DSTSI SB of Ukraine, 1999. (in Ukrainian).

[18] NDI 2.5-010-03 *Requirements for the protection of web site information from unauthorized access.* [Valid from 2003-04-02]. Kind. offic. Kiev, Ukraine: DSTSI SB of Ukraine, 2003. (in Ukrainian).

[19] NDI 2.5-008-02 *Requirements for the protection of sensitive information from unauthorized access during processing in automated Class “2” systems*.[Valid from 2002-13-12]. Kind. offic. Kiev, Ukraine: DSTSI SB of Ukraine, 2002. (in Ukrainian).

(cc) BY-NC-SA
This work is licensed under Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.