DOI 10.20535/2411-1031.2021.9.1.249805
УДК 004.056.53::[303.43::65(012.2+012.8)]

ЮЛІЯ КОЖЕДУБ,
АНДРІЙ МАКСИМЕЦЬ,
ВІРА ГИРДА

ПРОЄКТУВАННЯ СТРАТЕГІЇ ЗАХИСТУ ДАНИХ ЯК КОМПОНЕНТА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Проведено ґрунтовний аналіз проблеми захисту даних, зокрема початкового етапу – проєктування. Показано як застосування теорій ризиків і управління може використовуватися для досягнення цілей інформаційної безпеки. Відображено напрями розроблення та механізми впровадженням відповідних заходів та/або засобів, зокрема, через процедури авторизації, аутентифікації, ідентифікації. Запропоновано послідовність дій з проєктування стратегії захисту даних. Вона охоплює загальний і недеталізований план протягом довготривалого проміжку часу – так званого життєвого циклу інформації. Проаналізовано вихідні умови проєктування стратегії захисту даних та основні вимоги до оцінювання ефективності засобів захисту комп'ютерних систем. Виокремлено компоненти для функціонування стратегії захисту з акцентом на зменшення ризиків інформаційної безпеки. Оскільки відомо, що оптимальним підходом до забезпечення інформаційної безпеки є ризик-орієнтовний. Обирання теорії ризиків обумовлено своєю придатністю до всіх сфер діяльності людей і, зазвичай, саме на ризик-орієнтовний підхід спираються розробники сучасних технічних систем, зокрема й комп'ютерних. Доведено, що для досягнення цілей інформаційної безпеки стосовно захисту даних, застосування теорії ризиків є переважальним. Керування ризиками для навмисного й ненавмисного завдання шкоди дає змогу відслідковувати реалізацію вразливостей, спричинених антропогенним впливом. Встановлено, що завданням розроблюваної стратегії захисту даних є ефективне використання наявних ресурсів. Виділено відкриті науково-дослідницькі виклики та майбутні напрями у сфері захисту даних, особливо з огляду на те, що захист даних потребує міждисциплінарних досліджень та поєднання наукових підходів і теорій. Визначено важливість завдання захисту даних у зв'язку з пріоритетністю цього питання для сучасних інформаційних систем, де комп'ютерні системи і мережі є головними носіями критично чутливої інформації. Зосереджено увагу на прийнятті ефективних стратегій забезпечення комплексного захисту даних. Такі стратегії основані на різноманітних технологіях захисту даних у комп'ютерних системах і мережах. Проте основним чинником стратегії захисту даних, що розробляється, є встановлення балансу між вартістю впроваджених заходів та/або засобів забезпечення інформаційної безпеки і досягнутим станом інформаційної безпеки.

Ключові слова: комп'ютерна система, стратегія, проєктування, захист даних, ризики, забезпечення інформаційної безпеки.

Постановка проблеми. Термін "забезпечення інформаційної безпеки" (далі – ЗІБ) було вперше введено Генштабом США в 1998 році в Спільній доктрині інформаційних операцій [1]. Цим документом уперше визначається поняття ЗІБ. У 2000 році його було включено до Глосарію безпеки національних інформаційних систем США. За десятиріччя визначення змінилось, тому дефініція відноситься тепер до заходів [2]:

Забезпечення інформаційної безпеки – це заходи, якими охороняється і/або захищається інформація та інформаційні системи, забезпечуючи їхню доступність, цілісність, автентифікацію, конфіденційність та безвідмовність. Ці заходи охоплюють забезпечення відновлення інформаційних систем шляхом об'єднання можливостей захисту, виявлення і реагування.

Подане Комітетом з систем національної безпеки (КСНБ; англ. Committee on National Security Systems, CNSS) вищезазначене визначення, побудоване на п'яти так званих "стовпах", що залишається єдиним строгим визначенням ЗІБ і до теперішнього часу. Визначенням ЗІБ КСНБ встановлюються цілі безпеки, але не вказано на методи, що можуть бути застосовано для їх досягнення. Згодом була прийнята концепція поглибленого захисту щодо ЗІБ [3], що охоплює такі аспекти як менеджмент ризиків; навчання, освіта та професіоналізм персоналу; програмні, тематичні та системні політики; моніторинг, керування і адміністрування; оцінка та аудит. Виходячи з цього, стає зрозуміло, що належний стан ЗІБ підтримується завдяки менеджменту ризиками, а також оцінкою щодо впровадження необхідних заходів із ЗІБ.

Видані Організацією економічного співробітництва та розвитку (ОЕСР, англ. Organization for Economic Co-operation and Development (OECD) Настанови щодо безпеки інформаційних систем та мереж пропонують дев'ять загальних принципів діяльності у сфері інформаційної безпеки: усвідомлення небезпеки; відповідальність; реагування; етика; демократія; оцінка ризику; проєктування безпеки та його впровадження; керування безпекою; постійне оновлення й оцінювання [4].

ЗІБ – це багатопрофільна область навчання і професійної діяльності, яка спрямована на захист даних організації шляхом оброблення ризиків, пов'язаних з інформацією та інформаційними системами, за допомогою комплексного і систематичного керування контрзаходами забезпечення безпеки, що зумовлюється оцінюванням ризиків та економічною ефективністю від упроваджених заходів.

Таким чином, вищевказане визначення передбачає необхідність всебічного та систематичного керування контрзаходами безпеки. Всеосяжне керування означає, що механізми безпеки всіх доступних типів повинні використовуватися й охоплювати як організаційні заходи безпеки, так і технічні. Під систематичним керуванням розуміють, що ЗІБ повинно забезпечуватись послідовно на кожному етапі життєвого циклу інформації чи інформаційної системи. Відповідно комплексний підхід до менеджменту ризиків повинен інтегруватись в загальну систему керування організацією.

Крім того у визначенні поняття ЗІБ вказано два основних компонента [5]:

1. Менеджмент ризиків – ризики повинні бути ранжованими відповідно до встановленого прийнятного рівня для конкретної організації та/чи сфери діяльності організації, а після того – обробленими.
2. Оцінювання економічної ефективності – потрібно знати розрахунки вартості усіх заходів щодо ЗІБ, щоб досягнути цього стану найбільш ефективним і економічно виправданим способом.

В Україні термін ЗІБ має широке значення:

Забезпечення інформаційної безпеки – діяльність, спрямована на запобігання, своєчасне виявлення, припинення чи нейтралізацію реальних і потенційних загроз інформаційній безпеці України [6].

Таке тлумачення цього терміну дало змогу застосовувати його до різних сфер діяльності, так у [7] дано таке визначення:

– забезпечення інформаційної безпеки підприємництва – це сукупність методів і засобів, спрямованих на всебічне системне підтримання необхідного рівня захисту інформаційних ресурсів шляхом виконання відповідними підрозділами системи безпеки господарюючого суб'єкта завдань щодо:

- захисту інтелектуальної власності та комерційних секретів;
- захисту від незаконного проникнення в комп'ютерні системи і мережі, автоматизовані системи;
- захисту права суб'єктів господарювання на інформацію;
- розробки організаційних механізмів з технічного захисту інформації від зовнішніх і внутрішніх загроз і для перекриття можливих каналів відтоку інформації в процесі використання засобів зв'язку, передачі та обробки інформації;

- захисту інформації шляхом збереження важливої інформації через шифрування невеликих за обсягом відомостей, що містять друковані документи, або перетворення повідомлень, які надсилають за допомогою засобів телефонування.

Подолання проблеми ЗІБ в Україні стало надзвичайно актуальним, але на сьогодні воно, у зв'язку з цифровими трансформаціями суспільства і світу, дещо звузилось та відбулась підміна термінів. Ось, наприклад, в [8] надано визначення для фінансової організації (банку):

Інформаційна безпека або кібербезпека (ІБ) – це діяльність, як сукупність організаційно-технічних заходів і засобів спрямованих на захист інформації від широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації ризиків бізнеспроцесів і отримання максимальної рентабельності інвестицій та бізнес-можливостей. ІБ спрямована на забезпечення конфіденційності, цілісності та доступності інформації, а також автентичності, неспростовності та надійності процедур автентифікації користувачів і інформаційних ресурсів Банку.

І далі:

Система інформаційної безпеки (або кіберзахист) – сукупність (комплекс) спеціальних заходів правового (законодавчого) і адміністративного характеру, організаційних заходів, фізичних і технічних (програмних і апаратних) засобів захисту, а також спеціального персоналу, призначених для забезпечення інформаційної безпеки Банку.

Отже, актуальним завданням є проєктування стратегії захисту даних, на основі пошуку заходів та/чи засобів досягнення ЗІБ через дослідження можливості використання сукупності загальновідомих наукових теорій, поєднання яких дасть розв'язок поставленого завдання.

Аналіз останніх досліджень і публікацій. У 2006 році британський математик Клайв Хамбі (Clive Humby) запропонував фразу "дані – це нова нафта" ("data is the new oil"). Ця теза точно відображає властивість даних бути ключовим елементом для керування, швидкого зростання та досягнення успіху в діяльності організації. Оскільки основою кожної функції діяльності організації є дані [9]: інформація про співробітників, уподобання клієнтів, прогнози продажів, замовлення постачальників, кредиторська заборгованість та дебіторська заборгованість, вебсайт організації, патенти, оренда, записи технічного обслуговування обладнання, маркетингові матеріали, – то викликає занепокоєння питання: як вплине на діяльність організації, якщо змінять, знищать чи вкрадуть дані. Вплив порушення властивостей даних може бути значним: втрата репутації та значні збитки.

Наприклад, за даними [10], де зібрано статистику починаючи з 2019 року:

– середня вартість збитків від втрати даних становить 3,9 мільйона доларів (за даними IBM) [11];

– кібератака відбувається кожні 39 секунди – це 2244 рази на день (за даними Університету штату Меріленд) [12];

– рівень безробіття в сфері кібербезпеки становить 0 % і понад один мільйон робочих місць не зайнято [13].

За прогнозами Cybersecurity Ventures [14] очікується, що глобальні витрати на кіберзлочинність досягнуть 10,5 трлн. дол. США щорічно до 2025 р. Оцінка вартості збитків базується на історичних цифрах кіберзлочинності, включаючи нещодавні темпи зростання за минулі роки; відбудеться різке збільшення кількості створюваних злочинних груп – їх буде на порядок більше в 2025 р., ніж сьогодні.

Витрати на кіберзлочинність включають: пошкодження та знищення даних, викрадені гроші, втрату продуктивності, крадіжку інтелектуальної власності, крадіжку персональних та фінансових даних, розкрадання, шахрайство, зрив звичного бізнесу, судово-медичне розслідування, відновлення та видалення зламаних даних та систем, і шкоду репутації.

За інформацією Cybersecurity Ventures [15], до 2025 року у світі буде зберігатись 200 цетабайт даних, вони зберігаються в приватній та державній IT-інфраструктурах, в комунальних інфраструктурах, в приватних та публічних хмарних центрах обробки даних, на

персональних обчислювальних пристроях – персональних комп'ютерах, ноутбуках, планшетах, смартфонах, а також на "розумних" пристроях (англ. Internet of Things, IoT).

У результаті пандемії COVID-19 майже половина робітників США працює на дому (за даними Стенфордського університету [16]): співробітники генерують, отримують доступ і обмінюються більшою кількістю даних віддалено за допомогою хмарних застосунків, – це загальнодоступні хмари, що експлуатуються постачальниками та компаніями соціальних медіа (Apple, Facebook, Google, Microsoft, Twitter тощо); державні хмари, доступні громадянам та організаціям; приватні хмари, що належать корпораціям середнього та великого розміру, або постачальники хмарних сховищ [17].

У [18] було оприлюднено дослідження проблеми захисту даних на трьох рівнях: керування, системи і штучного інтелекту.

У [19] показано ефективні методи захисту даних від інсайдерів.

Захист даних окремими громадянами або захист даних "зроби сам" (від анг. do-it-yourself, DIY), що розглянуто в [20], – є важливою частиною проблеми захисту даних. У цій статті розглядається так званий "парадокс конфіденційності" або сприяння захисту приватності людини, що полягає в: ефективному захисті своїх даних, з однієї сторони, а з іншої – у швидко розвиваючому ринку надання цифрових послуг.

У [21] досліджено питання збирання та оброблення великих даних (Big Data), і, відповідно, розглянуто моделі щодо права на захист даних (the right to data protection). Ці моделі пов'язані з властивостями великих даних: величезним обсягом даних, швидкістю, з якою їх збирають, зростанням кількості пристроїв, що їх збирають, різноманітністю даних і їхнім реляційним характером (можливістю встановлювати зв'язки між різними наборами даних) тощо.

Комісія з кіберпростору Solarium (Cyberspace Solarium Commission) у новаторському звіті за 2020 рік пропонує стратегію шаруватого кібер стримування, щоб захистити організації США від кіберзлочинів та навіть кібервійни [22]. Цей звіт складається з понад 80 рекомендацій щодо реалізації зазначеної стратегії. Ці рекомендації організовано як шість основних стовпів:

- реформування структури й організація урядового кіберпростору США;
- посилення норм та розвиток невійськових засобів протидії;
- підвищення національної стійкості;
- змінення форми кібер-екосистеми;
- операціоналізування співпраці в сфері кібербезпеки з приватним сектором;
- збереження та використання силових державних інструментів влади.

Метою статті є підвищення ефективності проєктування стратегії захисту даних, що полягає у відображенні послідовних і скоординованих заходів та/або засобів забезпечення інформаційної безпеки.

Виклад основного матеріалу досліджень. Інформація вважається одним із найцінніших ресурсів людства на всіх етапах його розвитку. Незалежно від того, про що йдеться: місцезнаходження багатого мисливського угіддя, технологія виготовлення зброї чи знання про створення Всесвіту, – вона мала цінність і потребувала захисту. Від знеособлюваної інформації сучасний світ перейшов до формації, що має виняткову цінність для конкретної людини: грошовий і майновий стан, персональні дані, особистісні уподобання, інформація про стан здоров'я. Це пов'язано перш за все зі стрімким розвитком інформаційних технологій, що роблять можливим доступ до великих масивів персоналізованих даних.

Інформація може як давати перевагу її власнику, так і призводити до колосальних збитків для організації в разі потрапляння до рук зловмисників. ЗІБ організації – одна з найбільш важливих задач, покладених на керівництво і від вирішення якої залежить безпосередня діяльність та успішність організації.

Це досягається розробленням і впровадженням заходів (технічні, організаційні, правові) та/або засобів забезпечення безпеки з метою збереження інформації усередині організації та поза її межами [5]. ЗІБ для КС, де інформація створюється, обробляється, зберігається, передається та знищується, – це комплекс заходів та засобів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, неправомірних дій щодо використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення інформації. Набір цілей забезпечення безпеки для ЗІБ, що визначають на основі ризик-орієнтовного підходу, слід періодично переглядати, щоб забезпечити їх адекватність та відповідність умовам, що динамічно змінюються. Поточний набір цілей безпеки зазвичай відповідає забезпеченню збереженості конфіденційності, цілісності, доступності та інших властивостей інформації.

Захист інформації щодо персональних даних фізичних осіб під час їх опрацювання є фундаментальним правом будь-якої людини, так як це визначено в ст. 8(1) Хартії фундаментальних прав Європейського Союзу. В Україні чинним є Закон України "Про захист персональних даних" [23], що регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних.

Сформована у США концепція права на приватність особистого життя людини зробила великий внесок у становлення сучасної системи прав і свобод людини [24]. Юридично першу спробу визначити поняття "приватність" було зроблено у 1890 р. американськими юристами, випускниками Гарвардської школи права Луїсом Брандайзом і Семюелем Уорреном, які сформулювали його як "право бути залишеним у спокої" ("the right to be left alone") [25]. Можна сказати, що американські правники суттєво випередили свій час, адже у своїй відомій статті "Право на приватність" у Гарвардському правовому журналі вони зазначали [25], що нові методи та засоби ведення бізнесу можуть завдати шкоди приватності особи, а також обґрунтовували необхідність створення окремого "права приватності". Оскільки у подальшому така позиція Луїса Брандайза і Семюела Уоррена отримала своє закріплення у прецедентній практиці Верховного Суду США, зокрема у 1928 році у справі "Олмстед проти США", "Olmstead v. the United States", 277 U.S. 438 (1928) [26], то можна стверджувати, що саме ця стаття гарвардських юристів заклала основи формування права на невтручання в особисте життя, в тому числі у зв'язку з обробкою персональних даних.

У сьогоднішньому мінливому світі персональні дані людини обробляються щосекунди – на роботі, державними інституціями, у сфері охорони здоров'я, під час використання мережі Інтернет, при наданні різноманітних послуг, включаючи банківські, супермаркетів, кафе та ресторанів, кінотеатрів, самозайнятих осіб, операторів мобільного зв'язку [27]. Тому більшість країн (і об'єднання країн) закріпила законодавчо вимоги щодо збереження (захисту) даних. Відомими і визначними нормативно-правовими актами в сфері захисту даних є такі: General Data Protection Regulation (GDPR) і California Consumer Privacy Act (CCPA). Даними документами суттєво підвищено рівень вимог щодо забезпечення захисту персональних даних [28]. Закон України [23] гармонізовано з "Конвенцією про захист осіб у зв'язку з автоматизованою обробкою персональних даних" [29].

Ключові відмінності між GDPR і CCPA [27]:

- сфера застосування та територіальне охоплення;
- визначення, що стосуються захищеної інформації;
- рівні специфічності та право відмовитись від продажу особистої інформації.

Так за CCPA загальнодоступна інформація (наприклад, профіль соціальної мережі можуть бути вигаданими) не є особистою. Винятками є інформація про особисте здоров'я, що підпадає під дію Акту про переносимість та підзвітність медичного страхування, інакше відомого як HIPAA (Health Insurance Portability and Accountability Act), а також інформація, яку збирають фінансові установи.

Сучасним підходом до захисту даних є концепція “потрійного А” [30]:

1. Аутентифікація. Користувачу потрібно підтвердити свою особу перед тим, як отримати доступ до систем або записів. Як правило, автентифікація здійснюється за допомогою пароля, але деякі системи можуть використовувати й інші технології, такі, як: код маркера, картка доступу, відбиток пальця або розпізнавання обличчя. Найважливішою властивістю автентифікації є можливість відстежувати дії до конкретної людини.

2. Авторизація. Хоча автентифікація підтверджує особу, авторизація визначає, що ця особа можете робити з цією системою та записами, що зберігаються в ній. Авторизація – це ролі або дозволи, які має користувач. Чи можливе редагування даних? Чи мають вони можливість видаляти дані? Чи можуть вони скопіювати або експортувати всю базу даних?

3. Аудит. Більшістю сучасних систем управління записами відслідковуються дії користувачів у системі. Це потрібно для відстеження використання даних, і щоб слідкувати за тим, звідки дані надходять і що саме пересилають. Потужна система аудиту виходить за рамки притягнення людей до відповідальності за внесення змін, додавання або видалення записів або внесення інших модифікацій – вона може надати цінну інформацію про найбільш часто використовувані, а, отже, найбільш цінні набори (колекції, рубрики) даних.

Розглядаючи питання ЗІБ в комп’ютерних системах (КС), перш за все, вводять їх абстрактну модель, якою відображаються наявні передбачувані стани цієї КС. Ці стани (в термінах моделі самої КС) описують її захищеність. Поняття “захищеності” принципово не відрізняється від будь-яких інших властивостей КС, наприклад, “надійної роботи”, і є для неї зовнішнім, апріорно заданим. Поняття “захищеності” взаємопов’язане з трьома поняттями [30]:

“джерело загрози” – позначення зовнішньої причини для виведення КС із стану “захищеності”;

“загроза” – вказує на причину виведення КС із захищеного стану через дії джерела загрози;

“уразливість” – означення властивості елементу КС, за допомогою якого реалізується загроза.

Інтегральною характеристикою захищуваної системи, є політика безпеки (ПБ) – це якісний або якісно-кількісний опис властивостей захищеності, що описують КС [31]. ПБ має описувати в загальному випадку нестаціонарний (динамічний) стан захищеності відповідного об’єкта захисту. Дійсно, система, що захищається, може змінюватись, доповнюватись новими компонентами (суб’єктами, об’єктами, операціями суб’єктів над об’єктами), відповідно, що і ПБ повинна підтримуватись в часі, цим самим і досягається управління безпекою об’єкта захисту. Змінюваність захищуваної КС в часі, а також питання реалізації ПБ щодо конкретних елементів захищуваної системи, зумовлюють необхідність розв’язання завдання: як гарантує задана ПБ досягнення встановленого рівня захисту.

Захист даних – пріоритетне завдання будь-якої організації. В світових масштабах не вирішення цієї проблеми набуває максимально небезпечного характеру. Тому різні технології ЗІБ розроблялись спеціально, щоб допомогти користувачам (організації та/чи людині) досягнути ефективного ступеню захисту. Отже, такими технологіями є:

– мережева безпека, щоб запобігти проникненню в мережу неавторизованих користувачів або зловмисників. Цей тип безпеки необхідний для захисту даних усередині мережі;

– Інтернет-безпека – охоплює захист інформації, що відправляється і отримується в браузерах, а також опікується питаннями безпеки мережі з використанням вебзастосунків. Дана технологія призначена для моніторингу вхідного інтернет-трафіку і перегляду на наявність шкідливих програм;

– кінцева точка безпеки, щоб забезпечити захист на рівні пристроїв, які можуть бути захищені системою безпеки кінцевих точок (мобільні телефони, планшети і ноутбуки). Безпека кінцевих точок запобігає доступу пристроїв до мереж, які представляють загрозу як для організації, так і для особи;

– хмарна безпека. Для забезпечення захисту даних в хмарі часто використовують брокер безпеки хмарного доступу (CASB), безпечний інтернет-шлюз (SIG) і хмарне спеціалізоване управління загрозами (UTM), це потрібно, оскільки користувачі підключаються безпосередньо до інтернету і не захищені традиційним способом.

– безпека застосунків, де додатки спеціально кодують під час створення, щоб гарантувати максимальний захист користувачам.

Захист даних – це спільні зусилля усіх складових процесу, динамічного за своєю природою, захисту інформації. Розпочати роботу та спланувати підхід потрібно з урахуванням того, що є найважливішим в організації, – це є початкова точка проєктування. Також може бути потрібно врахувати інші чинники як от нормативно-правові документи, що сприятимуть встановленню рамкових вимог щодо захисту даних [9].

Отже, головною метою практичного застосування стратегії інформаційної безпеки щодо захисту даних, – це надання можливості організації виконувати свої функції, враховуючи можливі інформаційні ризики для неї, її партнерів і споживачів. Цієї мети досягають за допомогою вирішення п’яти задач забезпечення безпеки, що відповідають чотирьом властивостям інформації (доступності, конфіденційності, цілісності, спостережності) та п’ятої – гарантії того, що заходи безпеки ефективно реалізовано [32], а саме забезпечення:

1. Доступності (лише ресурсів, призначених для використання). Авторизовані користувачі мають доступ до відповідних ресурсів КС. Ця задача направлена на запобігання навмисному чи ненавмисному видаленню даних, необґрунтованої відмови в доступі до ресурсу, спроб використання КС чи даних в несанкціонованих цілях.
2. Цілісності (даних і КС). Цілісність має два аспекти:
   – цілісність даних – дані не можуть бути несанкціоновано модифіковані під час їх зберігання, передачі і обробки;
   – цілісність КС – функціонування системи без втручання в її роботу і несанкціонованих маніпуляцій.
3. Конфіденційності (даних і системної інформації). Конфіденційна інформація не може бути доступна для неавторизованого користувача під час її зберігання, обробки і передачі.
4. Спостереженості. Здатність вибіркового спостереження (фіксації) за діями об’єктів і суб’єктів у КС.

Спостереженість – це організаційна вимога ПБ, що забезпечується механізмами причетності, примушення, локалізації несправностей, виявлення і запобігання вторгненням, відновлення, дотримання упроваджених правових заходів.

5. Гарантій (адекватна реалізація попередніх чотирьох завдань). Підстава довіряти, що механізми безпеки реалізовані і функціонують відповідно до розробленого проєкту захищеної КС. Перші чотири задачі забезпечення безпеки (цілісність, доступність, конфіденційність і спостережність) адекватно реалізовані, якщо [32]:
   – функціональні вимоги сформульовано і коректно реалізовано;
   – забезпечено достатній захист від навмисних помилок користувачів або помилок програмного забезпечення;
   – забезпечено достатню стійкість від навмисного проникнення.

Забезпечення гарантій – це загальна задача, де всі задачі є взаємозалежними і не можуть бути вирішені окремо (рис. 1).

Захист даних стосується набору практичних інструментів та стандартних механізмів, що їх використовують для недопущення несанкціонованого доступу, змін та розголошення протягом її життєвого циклу. Цей набір охоплює політики, чинні нормативно-правові документи та сучасні інноваційні технології, які можуть захистити дані організації від зловмисних вторгнень або ненавмисних витоків.

Практичні механізми зазвичай також охоплюють фізичну безпеку обладнання та мережеві активи, що містять захищені дані, адміністративні засоби контролю та політики, логічний механізм захисту доступу до програмного забезпечення [11].

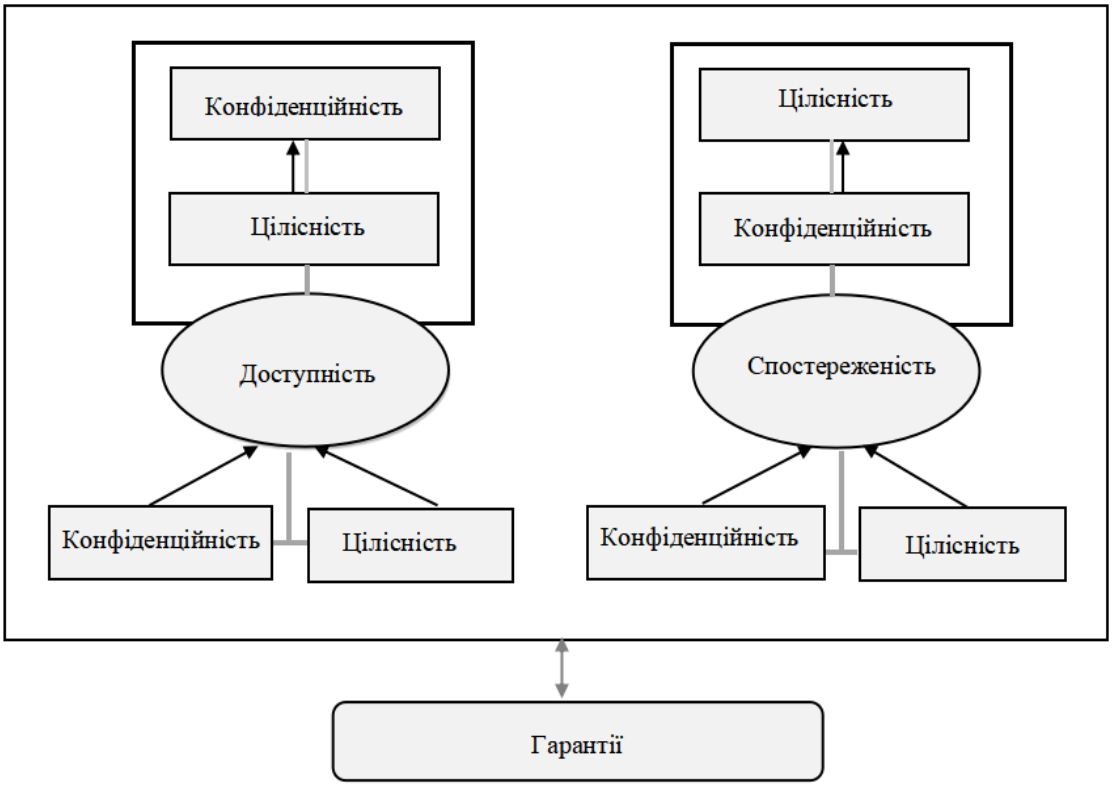

Рисунок 1 – Взаємозв'язок задач забезпечення безпеки

Під час проєктування стратегії захисту даних слід дотримуватись такої послідовності дій (рис. 2) [11]:

1. Постійно переглядати цілі організації відповідно до затвердженої ПБ.
2. Ідентифікувати загрози безпеці та кількісно оцінити вплив основних (ранжованих) ризиків на діяльність організації.
3. Створити надійні можливості реалізування заходів, зазначені в процедурах оброблення ризиків, які можуть допомогти організації зменшити ризики, враховуючи мінливу динаміку сфери діяльності організації, масштаби операцій, використовувані технології та глобальний ландшафт ризиків кібербезпеки.
4. Знайти оптимальний баланс між інвестиціями в процеси та технології, спрямованими на підвищення рівня захисту, – і збитками від реалізації загроз. Окрім того працездатність удосконалених рішень щодо безпеки залежить від культури обізнаності персоналу стосовно заходів безпеки, а також достатнього контролю за управлінням застосованих заходів безпеки та наявністю в організації необхідних кваліфікованих спеціалістів, які виконують нагляд за дотриманням застосованих заходів.

Апріорі відомо [33] - [34], що практичні інструменти захисту даних можуть бути нівельовано наявністю людського компоненту – це найслабша ланка для сталого й безпечного функціонування КС. Згідно з дослідженням IBM [10] - [11], людський елемент відповідає за 95% від усіх випадків порушення безпеки, а тому одним із способів зміцнити систему захисту даних, – це підвищити культуру й обізнаність співробітників організації. Для цього провадять навчання з широкого кола питань ЗІБ, незалежно від технічного чи професійного рівня їх підготовки й досвіду. Крім того, слід дотримуватись принципу найменших прав доступу як елемента ПБ організації. Не менш значущим є наймання й залучення спеціалістів з безпеки, особливо для роботи в управлінських відділах, наприклад, що займаються плануванням. Освіченість і навченість персоналу основам ЗІБ дозволить зменшити кількість інцидентів інформаційної безпеки і, відповідно, збитки через їх дію [35].

Рисунок 2 – Компоненти стратегії захисту даних

Наступне покоління рішень щодо захисту даних покладається на розширені можливості штучного інтелекту для створення активної та інтелектуальної системи захисту, розуміння динамічного характеру оточення КС та навантаження на такі системи під час виявлення потенційно аномальних дій у КС (рис. 3) [11].

Рисунок 3 – Ризик через поєднання загрози та вразливості

Одне з ключових понять в оцінці ефективності заходів та/чи засобів для ЗІБ – це збиток, що наноситься організації в результаті впливу загроз на інформацію та/чи КС. За своєю суттю будь-який збиток, його визначення й оцінка мають економічну основу для аналізування питання із ЗІБ [36] щодо недоотримання вигоди через перевищення витрат організації.

З позиції функціонально-вартісного аналізу, загальний збиток організації складається з двох складових частин: безпосереднього і опосередкованого. Безпосередній збиток виникає внаслідок порушення властивостей інформації. Опосередкований – це втрати, які матиме організація у зв'язку з обмеженнями на поширення інформації, яку в установленому порядку віднесено до категорії чутливої, що потребує захисту. Описування збитку, що наноситься організації в результаті витоку інформації, ґрунтується на його кількісних і якісних показниках. Ці показники базуються на одному з принципів захисту інформації – принципі обґрунтованості. Він полягає у встановленні, зазвичай шляхом експертних оцінок, доцільності обмеження в доступі і, відповідно до цього, захисту конкретних відомостей, а також імовірних наслідків цих дій, з урахуванням завдань і поставлених цілей організації, що закріплено в затвердженій ПБ [36].

Основними принципами ЗІБ є такі [36]: системність; комплексність; безперервність; розумна достатність; гнучкість управління і застосування; відкритість, зрозумілість і простота застосування заходів та/чи засобів захисту, тому під час розроблення необхідних механізмів, процедур, алгоритмів для ЗІБ, необхідно враховувати велику кількість різних чинників.

Проєкт стратегії захисту даних також повинен містити процедуру зменшення ризиків інформаційної безпеки (рис. 4-5).

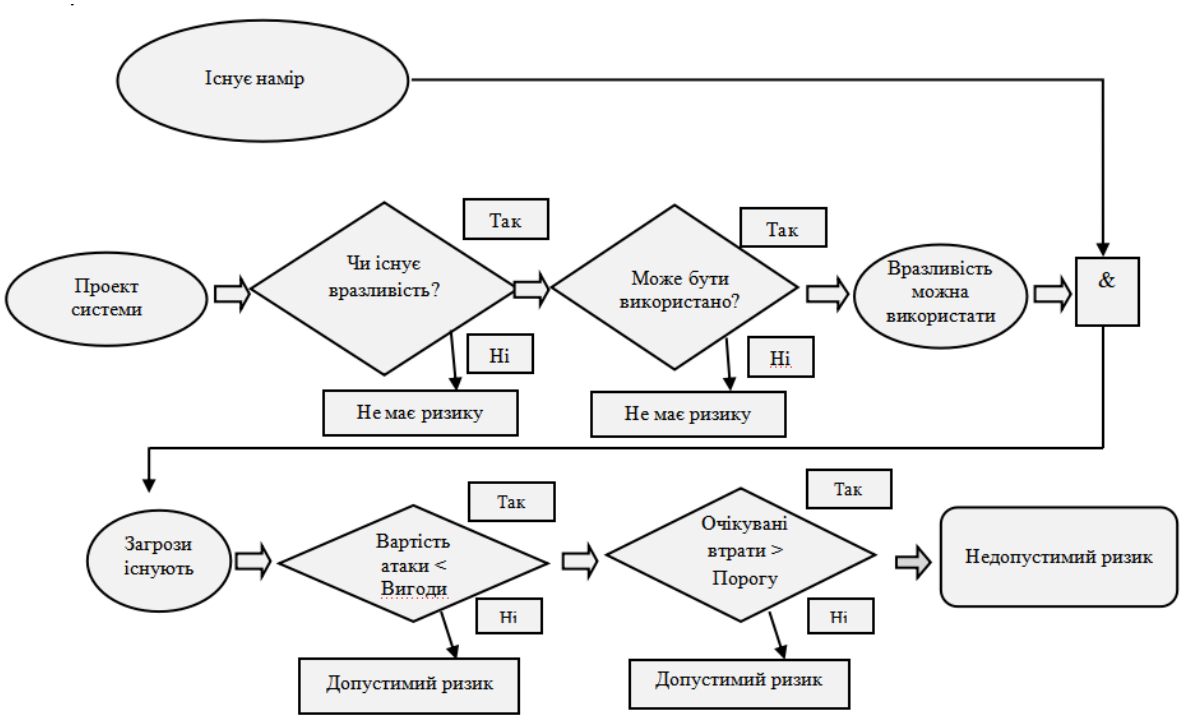

Рисунок 4 – Схема зменшення ризиків інформаційної безпеки за наявності навмисних джерел загроз

У разі наявності антропогенних джерел загроз, точками прийняття рішень [37] - [38] у алгоритмі зменшення ризиків є (рис. 4):

– вразливості є. Рішення: запровадити методи і засоби, що зменшать нездатність КС протистояти загрозам;

– вразливості можуть бути використанні. Рішення: застосувати багаторівневий захист, щоб запобігти їх використанню;

– орієнтовна вартість реалізації загрози (розрахована на основі експертної оцінки) менша за можливу вигоду від зламу КС (й отримання інформації). Рішення: застосувати захист, який збільшить вартість “атаки” (це можуть бути організаційні методи захисту, такі як обмеження в обробці інформації, що суттєво зменшить можливу вигоду для порушника інформаційної безпеки);

– втрати дуже великі. Рішення: застосувати необхідні підходи в проєктуванні, архітектурне планування та технічні методи захисту, що зменшать очікуванні втрати (зокрема, управління доступом може забезпечити найбільш ефективне зменшення ризиків).

Схема зменшення ризиків за наявності таких джерел загроз як помилки в КС системі та дії користувачів, які ненавмисно порушують встановлену ПБ (рис. 5), мало відрізняється від схеми зменшення ризиків за наявності навмисних (здебільшого антропогенного походження) джерел загроз (рис.4).

Захист даних для спеціалістів з інформаційної безпеки особливо є важливим завданням для тих сфер діяльності, де зроблено акцент на забезпечення конфіденційності даних через крадіжки персональних даних.

Щоденна боротьба зі глобальними викликами як у державному, так і у приватному секторах економіки спричинила зростання ринку, пов’язаного з надання професійних послуг зі створення систем захисту даних, закупівлі спеціального програмного забезпечення. Крім того, ця діяльність потребує збільшення інвестицій, щоб протистояти Інтернет шахрайству,

крадіжками і витокам даних, що спричинені порушенням інформаційної безпеки. Фахівці у сфері інформаційних технологій повинні мати необхідну освіту, підготовку та/чи перепідготовку, сертифікацію, у разі необхідності. Організації мають більш серйозно ставитись до загроз, вкладаючи більше ресурсів у створення ефективної системи захисту. Організаціям життєво необхідно приділяти більше уваги підвищенню обізнаності фахівців. Для цього важливо підвищувати поінформованість персоналу організацій щодо ризиків інформаційної безпеки, проводити тренінги, використовувати відповідні симуляції, в результаті чого зміцниться захист життєво важливої інформації організації [39].

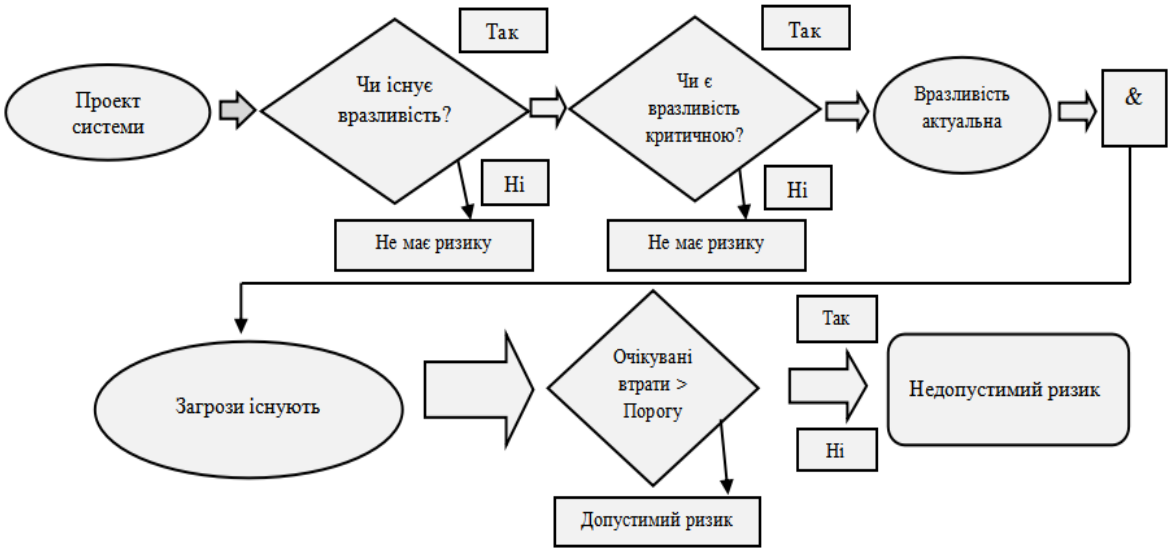

Рисунок 5 – Схема зменшення ризиків інформаційної безпеки за наявності ненавмисних джерел загроз

Щоб забезпечити максимальний рівень захисту даних під час процедури обміну, можна використати моделювання загроз, що допоможе визначити проблемні місця в безпеці організації, пов’язані з архітектурним проєктуванням КС, наприклад за допомогою тестування на проникнення [40].

Під час планування систем безпеки потрібно знати про те, кого і яка саме інформація може цікавити, яка її цінність і на які фінансові витрати заради неї здатен піти порушник. Створена система безпеки має бути адекватною потенційним загрозам щодо даних. Важливу роль у цьому відіграють організаційні заходи, такі, наприклад, як регулярна зміна паролів і ключів, суворий порядок їх зберігання, аналіз журналів реєстрації подій у системі, правильний розподіл повноважень користувачів [40].

Для комп’ютерної мережі, що об’єднує КС, де циркулює інформація, у багато разів збільшується й ризик несанкціонованого доступу до інформації. Важливими напрямами, які необхідно реалізувати – є комплекс заходів щодо захисту даних, що мають на меті врахувати так звані людиноорієнтовані аспекти безпеки:

1) коло службових осіб, які мають доступ до КС, перелік інформації, до якої їх допущено, а також вид дозволу на доступ залежно від безпосередніх функціональних обов’язків;

2) осіб, які відповідальні за збереження та уповноважені надавати доступ до інформаційних ресурсів;

3) контроль за результатами виконання впроваджених заходів (шляхом проведення планових перевірочних робіт як особою, відповідальною за безпеку в організації, так і з залученням компетентних спеціалістів інших організацій);

4) перелік інформації, ранжованої відповідно до її важливості і застосування заходів щодо її захисту;

5) порядок доступу до інформації (даних), а також порядок її захисту та знищення;

6) охорона та контроль за доступом до КС, приміщень і комунікацій від проникнення осіб, які не мають доступу до інформації.

Заходи ЗІБ повинні мати комплексний і системний характер та виконуватись на всіх етапах життєвого циклу інформації.

Заходи ЗІБ щодо захисту даних передбачають:

– захист інформації під час її передачі каналами зв'язку "користувач – комп'ютер", "комп'ютер – комп'ютер";

– забезпечення доступу до даних за процедурами управління доступом і виконання допустимих операцій над ними.

Усі процедури з управління доступом до інформації функціонують за принципом відповіді на запитання: хто може здійснювати доступ до інформації в КС і які операції з цією інформацією вони можуть виконувати? Об'єктом захисту, доступ до якого контролюється, може бути файл, запис у файлі або окреме поле запису файлу, а чинником, що впливає на прийняття рішення про доступ – зовнішня подія, значення даних, стан КС, повноваження користувача, причина звертання, перехресні посилання і пов'язані між собою документи. Виходячи з цього, доступ може бути визначено як:

– загальний (надається кожному користувачеві безумовно);

– залежний від події (керується подією). Передбачає блокування звертання користувача у певні інтервали часу чи під час звертання до КС з певного терміналу;

– залежний від змісту даних (наприклад, конкретному користувачеві заборонено знайомитись зі змістом певних документів);

– залежний від динамічного стану КС (наприклад, може бути заборонено доступ до файлу, якщо носій інформації не перебуває в стані "тільки читання" або закритий логічний диск, що містить цей файл);

– частково-залежний (наприклад, користувачеві дозволено доступ лише встановлену кількість разів). Це дає можливість уникнути можливості динамічного управління подіями;

– залежний від певного віку, імені користувача (наприклад, користувач має бути старшим 18 років);

– залежний від повноважень (наприклад, може бути дозволено "тільки читання", "читання і запис", "тільки виконання");

– залежний від дозволу (за паролем або іншим ідентифікатором).

Висновки. Початковий етап створення систем захисту – проєктування – має враховувати визначену множину чинників, які безпосередньо й опосередковано впливають на досягнення мети забезпечення інформаційної безпеки. Застосування інструментів системного і комплексного підходів, теорій ризиків, управління, прийняття рішень та функціонально-вартісного аналізу можуть ефективніше задовольняти в досягненні стану забезпечення інформаційної безпеки. Під час розгляду проблеми інформаційної безпеки завжди акцентується необхідність захисту інформації, що, як правило, виникає при роботі з конфіденційними документами і відомостями в процесі традиційного документообігу, або під час передавання інформації каналами зв'язку, або під час ведення конфіденційних переговорів. Проте у зв'язку з наростаючою діджиталізацією й можливістю, а, інколи, і необхідністю дистанційної роботи, ця проблема дещо змінилась. Наразі проблема інформаційної безпеки і, зокрема, захист даних стосується вже кіберпростору, а це спонукає фахівців з інформаційної безпеки розглядати комплексно й системно передавання, зберігання, оброблення інформації в КС. Проєктування стратегії захисту даних на основі ризик-орієнтовного підходу є саме тим підходом за допомогою якого досягають ефективного результату. Покращення процесу проєктування стратегії захисту даних для забезпечення інформаційної безпеки полягає у відображенні послідовних і скоординованих заходів та/чи засобів. Показано послідовність дій під час проєктування стратегії захисту даних. Нею відображаються шляхи розробки та механізми впровадження заходів та/або засобів забезпечення безпеки. Так, це реалізовано через процедури авторизації, аутентифікації,

ідентифікації. Вони є інструментами захисту інформації в КС. Проаналізовано вихідні умови побудови проєкту стратегії захисту даних та основні вимоги до оцінки ефективності засобів безпеки КС. Встановлено функційні компоненти для систем захисту даних з акцентом на зменшення ризиків інформаційної безпеки. Алгоритми управління ризиками дають змогу відслідковувати реалізацію вразливостей, спричинених людиноорієнтовним впливом. Завданням спроєктованої стратегії захисту даних є ефективне використання наявних ресурсів для досягнення основної мети – захист інформації в КС, що наразі широко поширені й у майбутньому стануть всеохопними. Показано важливість цього завдання для сучасних КС, що містять і обробляють критично чутливу інформацію. Розроблення результативної і ефективної стратегії досягається балансом між вартістю впроваджених заходів та/або засобів захисту даних і цінністю інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Joint Pub 3-13. Joint Doctrine for Information Operations. USA, 1998. [Online]. Available: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf. Accessed on: Febr. 11, 2021.

[2] National Information Systems Security (INFOSEC) Glossary. [Online]. Available: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. Accessed on: Febr. 11, 2021.

[3] Information Assurance through Defense in Depth. [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA377569.pdf. Accessed on: Febr. 11, 2021.

[4] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. [Online]. Available: https://www.oecd.org/sti/ieconomy/15582260.pdf. Accessed on: Febr. 11, 2021.

[5] Yu. Cherdantseva, and J. Hilton, “Understanding information assurance and security, in “Secure*BPMN – a graphical extension for BPMN 2.0 based on a Reference Model of Information Assurance & Security”, PhD Thesis, Cardiff University, UK, 2014. [Online]. Available: http://users.cs.cf.ac.uk/Y.V.Cherdantseva/UnderstandingIAS.pdf. Accessed on: Feb. 15, 2021.

[6] Верховна Рада України. 4 сесія. (2014, Трав. 28). *Проект № 4949 Закону України, Про засади інформаційної безпеки України*. [Електронний ресурс]. Доступно: https://ips.ligazakon.net/document/JG3TH00A?an=11. Дата звертання: Лют. 11, 2021.

[7] Е. Низенко, та В. Каленяк, *Забезпечення інформаційної безпеки підприємництва.* Київ, Україна: МАУП, 2006.

[8] Політика інформаційної безпеки АТ “АЙБОКС БАНК’. [Електронний ресурс]. Доступно: https://app.iboxbank.online/api/file/open/677. Дата звертання: Лют. 11, 2021.

[9] K. McCartney, “5 Essential Elements Of A Data Protection Plan”. [Online]. Available: https://www.zenefits.com/company-blog/5-essential-elements-of-a-data-protection-plan. Accessed on: Febr. 11, 2021.

[10] R. Sobers, “81 Ransomware Statistics, Data, Trends and Facts for 2021”. [Online]. Available: https://www.varonis.com/blog/ransomware-statistics-2021/. Accessed on: Febr. 11, 2021.

[11] M. Raza, “Introduction To Data Security”. [Online]. Available: https://www.bmc.com/blogs/data-security. Accessed on: Febr. 11, 2021.

[12] S. Morgan, “Zero-percent cybersecurity unemployment, 1 million jobs unfilled”. [Online]. Available: https://www.csoonline.com. Accessed on: Febr. 11, 2021.

[13] U.S. Bureau of labor statistics. Summary. Information Security Analysts. [Online]. Available: https://www.bls.gov. Accessed on: Febr. 11, 2021.

[14] S. Morgan, “Cybercrime To Cost The World $10.5 Trillion Annually By 2025”. Cybersecurity Ventures. [Online]. Available: https://cybersecurityventures.com/hackerpocalypse- cybercrime-report-2016/. Accessed on: Febr. 11, 2021.

[15] S. Morgan, “The World Will Store 200 Zettabytes of Data by 2025”. [Online]. Available: https://cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/. Accessed on: Febr. 11, 2021.

[16] N. Bloom, and M. Wong, “Stanford research provides a snapshot of a new working-from-home economy”. [Online]. Available: https://news.stanford.edu/2020/06/29/snapshot-new-working-home-economy. Accessed on: Febr. 11, 2021.
[17] Cross-media consumption patterns over pandemic. Temporary peaks or new trends? [Online]. Available: https://www.gemius.com/all-reader-news/cross-media-consumption-patterns-over-pandemic-temporary-peaks-or-new-trends.html. Accessed on: Febr. 11, 2021.
[18] C. Meurisch, and M. Mühlhäus, “Data Protection in AI Services: A Survey”, *ACM Computing Surveys*, vol. 54, iss. 2, pp. 1-38, 2021, doi: https://doi.org/10.1145/3440754.
[19] E. Bertino, “Data Protection from Insider Threats”, *Synthesis Lectures on Data Management*. [Online]. Available: https://doi.org/10.2200/S00431ED1V01Y201207DTM028. Accessed on: Febr. 11, 2021.
[20] T. Matzner, P. K. Masur, C. Ochs, and T. von Pape, “Do-It-Yourself Data Protection – Empowerment or Burden?”, *Data Protection on the Move. Law, Governance and Technology*, vol. 24, 2016. [Online]. Available: https://doi.org/10.1007/978-94-017-7376-8_11. Accessed on: Febr. 11, 2021.
[21] Y. McDermott, “Conceptualising the right to data protection in an era of Big Data”, *Big Data & Society*, 2017. [Online]. Available: https://doi.org/10.1177/ 2053951716686994. Accessed on: Febr. 11, 2021.
[22] United States of America, Cyberspace Solarium Commission (CSC). [Online]. Available: https://www.solarium.gov/. Accessed on: Febr. 11, 2021.
[23] Верховна Рада України. 5 сесія. (2010, Черв. 10). Закон, *Про захист персональних даних*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/2297-17#Text. Дата звертання: Лют. 15, 2021.
[24] Yu. Cherdantseva, and J. Hilton, “Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals” in *Organizational, Legal, and Technological Dimensions of Information System Administrator*, F. Almeida and I. Portela, Eds. IGI Global Publishing, 2013.
[25] S. D. Warren, and L. D. Brandeis, “The Right to Privacy”, *Harvard Law Review*, vol. 4, no. 5, pp. 193-220, 1890.
[26] US Supreme Court (Vol. 277), Olmstead v. United States, 277 U.S. 438 (1928). [Online]. Available: https://supreme.justia.com/cases/federal/us/277/438/. Accessed on: Febr. 11, 2021.
[27] 28 січня – Міжнародний День захисту персональних даних. [Електронний ресурс]. Доступно: https://monrda.gov.ua/index.php/9-uncategorised/8633-28-sichnya-mizhnarodnij-den-zakhistu-personalnikh-danikh. Дата звертання: Лют. 11, 2021.
[28] Європейський Союз. *Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/984_008-16#Text. Дата звертання: Лют. 11, 2021.
[29] Європейський Союз. *Конвенція про захист осіб у зв’язку з автоматизованою обробкою персональних даних*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/994_326#Text. Дата звертання: Лют. 11, 2021.
[30] V. Basani, “9 Important Elements to Corporate Data Security Policies that Protect Data Privacy”. [Online]. Available: https://www.securitymagazine.com/articles/87113-important-elements-to-corporate-data-security-policies-that-protect-data-privacy. Accessed on: Febr. 11, 2021.
[31] National Institute of Standards and Technology. (2001, Dec. 01). *NIST Special Publication 800-33, Underlying Technical Models for Information Technology Security*. Gary Stoneburner (ed.). [Online]. Available: http://csrc.nist.gov/publications/ nistpubs/800-33/sp800-33.pdf. Accessed on: Febr. 11, 2021.
[32] International Organization for Standardization. (2009, Dec. 03). ISO/IEC 15408-1, *Information technology. Security techniques. Evaluation criteria for IT security. Part 1*. [Online]. Available: https://www.iso.org/standard/ 50341.html. Accessed on: Febr. 11, 2021.

[33] Reuters Institute for the Study of Journalism. Digital News Report 2020. [Online]. Available: https://www.digitalnewsreport.org/survey/2020/. Accessed on: Febr. 11, 2021.
[34] International Telecommunication Union. Development (ITU-D). E-Strategies, 2015. Global Cybersecurity Index & Cyberwellness Profiles. [Online]. Available: http://handle.itu.int/11.1002/pub/80c63097-en. Accessed on: Febr. 11, 2021.
[35] В. Богуш, В. Бровко, та В. Настрадін. *Основи кіберпростору, кібербезпеки та кіберзахисту*. Київ, Україна: Ліра, 2020.
[36] A. Cherevko, "The theoretical basis of the concept of information security threats and classification of information security", *Efektyvna ekonomika*, no. 5, 2014. [Online]. Available: http://www.economy.nayka.com.ua/?op=1&z=3304. Accessed on: Febr. 11, 2021.
[37] В. Циганок, О. Андрійчук, С. Каденко, та О. Карабчук, "Підтримка прийняття рішень при побудові стратегії підвищення безпеки дорожнього руху та розвитку міської транспортної інфраструктури", *Реєстрація, зберігання і обробка даних*, т. 21, № 4, с.76-89, 2019, doi: https://doi.org/ 10.35681/1560-9189.2019.21.4.199489.
[38] S. Kadenko, V. Tsyganok, O. Andriichuk, A. Karabchuk, and M. Fu, "An Overview of Decision Support Software: Strategic Planning Perspective", *CEUR Workshop Proceedings*, Vol. 2859, pp. 142-156.
[39] А. Слободяник. *Кіберзахист для CFO: 10 трендів + 10 рекомендацій*. [Електронний ресурс]. Доступно: https://www.bdo.ua/uk-ua/blog-2/consulting/march-2020/cybersecurity-for-ceo. Дата звертання: Лют. 11, 2021.
[40] D. Bulatovych. *Core Elements of Data Security*. [Online]. Available: https://yalantis.com/blog/core-data-security-elements. Accessed on: Febr. 11, 2021.

Стаття надійшла до редакції 15.02.2021.

REFERENCE

[1] Joint Pub 3-13. Joint Doctrine for Information Operations. USA, 1998. [Online]. Available: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf. Accessed on: Febr. 11, 2021.
[2] National Information Systems Security (INFOSEC) Glossary. [Online]. Available: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. Accessed on: Febr. 11, 2021.
[3] Information Assurance through Defense in Depth. [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA377569.pdf. Accessed on: Febr. 11, 2021.
[4] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. [Online]. Available: https://www.oecd.org/sti/ieconomy/15582260.pdf. Accessed on: Febr. 11, 2021.
[5] Yu. Cherdantseva, and J. Hilton, "Understanding information assurance and security, in "Secure*BPMN – a graphical extension for BPMN 2.0 based on a Reference Model of Information Assurance & Security", PhD Thesis, Cardiff University, UK, 2014. [Online]. Available: http://users.cs.cf.ac.uk/Y.V.Cherdantseva/UnderstandingIAS.pdf. Accessed on: Feb. 15, 2021.
[6] Verkhovna Rada of Ukraine. 4th Session. (2014, May 28). *Draft № 4949 of the Law of Ukraine, On the Principles of Information Security of Ukraine*. [Online]. Available: https://ips.ligazakon.net/document/JG3TH00A?an=11. Accessed on: Febr. 11, 2021.
[7] E. Nizenko, and V. Kalenyak, *Ensuring information security of entrepreneurship*. Kyiv, Ukraine: MAUP, 2006.
[8] Information security policy of JSC "IBOX BANK". [Online]. Available: https://app.iboxbank.online/api/file/open/677. Accessed on: Febr. 11, 2021.
[9] K. McCartney, "5 Essential Elements Of A Data Protection Plan". [Online]. Available: https://www.zenefits.com/company-blog/5-essential-elements-of-a-data-protection-plan. Accessed on: Febr. 11, 2021.

[10] R. Sobers, "81 Ransomware Statistics, Data, Trends and Facts for 2021". [Online]. Available: https://www.varonis.com/blog/ransomware-statistics-2021/. Accessed on: Febr. 11, 2021.
[11] M. Raza, "Introduction To Data Security". [Online]. Available: https://www.bmc.com/ blogs/data-security. Accessed on: Febr. 11, 2021.
[12] S. Morgan, "Zero-percent cybersecurity unemployment, 1 million jobs unfilled". [Online]. Available: https://www.csoonline.com. Accessed on: Febr. 11, 2021.
[13] U.S. Bureau of labor statistics. Summary. Information Security Analysts. [Online]. Available: https://www.bls.gov. Accessed on: Febr. 11, 2021.
[14] S. Morgan, "Cybercrime to Cost The World $10.5 Trillion Annually by 2025". Cybersecurity Ventures. [Online]. Available: https://cybersecurityventures.com/hackerpocalypse- cybercrime-report-2016/. Accessed on: Febr. 11, 2021.
[15] S. Morgan, "The World Will Store 200 Zettabytes of Data by 2025". [Online]. Available: https://cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/. Accessed on: Febr. 11, 2021.
[16] N. Bloom, and M. Wong, "Stanford research provides a snapshot of a new working-from-home economy". [Online]. Available: https://news.stanford.edu/2020/06/29/snapshot-new-working-home-economy. Accessed on: Febr. 11, 2021.
[17] Cross-media consumption patterns over pandemic. Temporary peaks or new trends? [Online]. Available: https://www.gemius.com/all-reader-news/cross-media-consumption-patterns-over-pandemic-temporary-peaks-or-new-trends.html. Accessed on: Febr. 11, 2021.
[18] C. Meurisch, and M. Mühlhäus, "Data Protection in AI Services: A Survey", *ACM Computing Surveys*, vol. 54, iss. 2, pp. 1-38, 2021, doi: https://doi.org/10.1145/3440754.
[19] E. Bertino, "Data Protection from Insider Threats", *Synthesis Lectures on Data Management*. [Online]. Available: https://doi.org/10.2200/S00431ED1V01Y201207DTM028. Accessed on: Febr. 11, 2021.
[20] T. Matzner, P. K. Masur, C. Ochs, and T. von Pape, "Do-It-Yourself Data Protection – Empowerment or Burden?", *Data Protection on the Move. Law, Governance and Technology*, vol. 24, 2016. [Online]. Available: https://doi.org/10.1007/978-94-017-7376-8_11. Accessed on: Febr. 11, 2021.
[21] Y. McDermott, "Conceptualising the right to data protection in an era of Big Data", *Big Data & Society*, 2017. [Online]. Available: https://doi.org/10.1177/ 2053951716686994. Accessed on: Febr. 11, 2021.
[22] United States of America, Cyberspace Solarium Commission (CSC). [Online]. Available: https://www.solarium.gov/. Accessed on: Febr. 11, 2021.
[23] Verkhovna Rada of Ukraine. 5th Session. (2010, June 10). Law, *About personal data protection.* [Online]. Available: https://zakon.rada.gov.ua/laws/show/2297-17#Text. Accessed on: Febr. 11, 2021.
[24] Yu. Cherdantseva, and J. Hilton, "Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals" in *Organizational, Legal, and Technological Dimensions of Information System Administrator*, F. Almeida and I. Portela, Eds. IGI Global Publishing, 2013.
[25] S. D. Warren, and L. D. Brandeis, "The Right to Privacy", *Harvard Law Review*, vol. 4, no. 5, pp. 193-220, 1890.
[26] US Supreme Court (Vol. 277), Olmstead v. United States, 277 U.S. 438 (1928). [Online]. Available: https://supreme.justia.com/cases/federal/us/277/438/. Accessed on: Febr. 11, 2021.
[27] January 28 – International Day for Personal Data Protection. [Online]. Available: https://monrda.gov.ua/index.php/9-uncategorised/8633-28-sichnya-mizhnarodnij-den-zakhistu-personalnikh-danikh. Accessed on: Febr. 11, 2021.
[28] European Union. *Regulation (EC) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC*

(General Data Protection Regulation). [Online]. Available: https://zakon.rada.gov.ua/laws/show/984_008-16#Text. Accessed on: Febr. 11, 2021.

[29] European Union. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.* [Online]. Available: https://zakon.rada.gov.ua/laws/show/994_326#Text. Accessed on: Febr. 11, 2021.

[30] V. Basani, "9 Important Elements to Corporate Data Security Policies that Protect Data Privacy". [Online]. Available: https://www.securitymagazine.com/articles/87113-important-elements-to-corporate-data-security-policies-that-protect-data-privacy. Accessed on: Febr. 11, 2021.

[31] National Institute of Standards and Technology. (2001, Dec. 01). *NIST Special Publication 800-33, Underlying Technical Models for Information Technology Security*. Gary Stoneburner (ed.). [Online]. Available: http://csrc.nist.gov/publications/ nistpubs/800-33/sp800-33.pdf. Accessed on: Febr. 11, 2021.

[32] International Organization for Standardization. (2009, Dec. 03). ISO/IEC 15408-1, *Information technology. Security techniques. Evaluation criteria for IT security. Part 1*. [Online]. Available: https://www.iso.org/standard/ 50341.html. Accessed on: Febr. 11, 2021.

[33] Reuters Institute for the Study of Journalism. Digital News Report 2020. [Online]. Available: https://www.digitalnewsreport.org/survey/2020/. Accessed on: Febr. 11, 2021.

[34] International Telecommunication Union. Development (ITU-D). E-Strategies, 2015. Global Cybersecurity Index & Cyberwellness Profiles. [Online]. Available: http://handle.itu.int/11.1002/pub/80c63097-en. Accessed on: Febr. 11, 2021.

[35] V. Bogush, V. Brovko, and V. Nastradin. *Fundamentals of cyberspace, cybersecurity and cybersecurity*. Kyiv, Ukraine: Lira, 2020.

[36] A. Cherevko, "The theoretical basis of the concept of information security threats and classification of information security", *Efektyvna ekonomika*, no. 5, 2014. [Online]. Available: http://www.economy.nayka.com.ua/?op=1&z=3304. Accessed on: Febr. 11, 2021.

[37] V. Tsyganok, O. Andriychuk, S. Kadenko, and O. Karabchuk, "Decision support in building a strategy to improve road safety and development of urban transport infrastructure", *Data Recording, Storage & Processing*, vol. 21, no. 4. pp. 76-89, 2019, doi: https://doi.org/10.35681/1560-9189.2019.21.4.199489.

[38] S. Kadenko, V. Tsyganok, O. Andriichuk, A. Karabchuk, and M. Fu, "An Overview of Decision Support Software: Strategic Planning Perspective", *CEUR Workshop Proceedings*, Vol. 2859, pp. 142-156. [Online]. Available: http://ceur-ws.org/Vol-2859/paper12.pdf. Accessed on: Febr. 11, 2021.

[39] A. Slobodyanik. Cybersecurity for CFO: 10 trends + 10 recommendations. [Online]. Available: https://www.bdo.ua/uk-ua/blog-2/consulting/march-2020/cybersecurity-for-ceo. Accessed on: Febr. 11, 2021.

[40] D. Bulatovych. *Core Elements of Data Security*. [Online]. Available: https://yalantis.com/blog/core-data-security-elements. Accessed on: Febr. 11, 2021.

YULIIA KOZHEDUB,
ANDRII MAKSYMETS,
VIRA HYRDA

DESIGNING A DATA PROTECTION STRATEGY AS A COMPONENT OF PROVIDING INFORMATION SECURITY

A thorough analysis of the data protection problem, in particular the initial stage, was carried out. It is shown how the application of risk theories and management can be used to achieve information security goals. The directions of development and mechanisms for implementing appropriate measures and/or means through authorization, authentication, and identification

procedures are reflected. A sequence of actions for designing a data protection strategy is proposed. It covers a general and non-detailed plan over a long period of time – the so-called information life cycle. The initial conditions for designing a data protection strategy and the basic requirements for evaluating the effectiveness of computer systems protection are analyzed. Components for the functioning of the protection strategy with an emphasis on reducing information security risks have been identified. It is known that the optimal approach to information security is risk-based. The choice of risk theory is due to its suitability for all spheres of human activity, and usually, the developers of modern technical systems, including computer ones, rely on a risk-oriented approach. It has been proven that to achieve information security goals regarding data protection, the application of risk theory is predominant. Risk management for intentional and unintentional damage allows you to monitor the implementation of vulnerabilities caused by anthropogenic impacts. It is established that the task of the developed data protection strategy is the efficient use of available resources. Open research challenges and future directions in the field of data protection are highlighted, especially given that data protection requires interdisciplinary research and a combination of scientific approaches and theories. The importance of data protection is determined in connection with the priority of this issue for modern information systems, where computer systems and networks are the main carriers of critically sensitive information. The focus is on the adoption of effective strategies to ensure comprehensive data protection. Such strategies are based on a variety of data protection technologies in computer systems and networks. However, the main factor in the developed data protection strategy is to establish a balance between the cost of implemented measures and/or means of information security and the achieved state of information security.

Keywords: computer system, strategy, designing, data protection, risks, providing information security.

Кожедуб Юлія Василівна, кандидат технічних наук, старший науковий співробітник, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0001-6181-5519, JuliaKozhedub@email.ua.

Максимець Андрій Володимирович, старший інженер, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0003-3551-0628, andy.west.corp@gmail.com.

Гирда Віра Анатоліївна, старший інженер, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-3858-4086, gidraponka@ukr.net.

Kozhedub Yuliia, candidate of technical sciences, senior research, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Maksymets Andrii, senior engineer, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Hyrda Vira, senior engineer, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.