INFORMATION SECURITY

DOI 10.20535/2411-1031.2019.7.2.190555
УДК 004.056.53

НАТАЛІЯ КУХАРСЬКА,
ОРЕСТ ПОЛОТАЙ

АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УПРАВЛІННІ БЕЗПЕРЕРВНІСТЮ ДІЯЛЬНОСТІ ОРГАНІЗАЦІЇ

Переважна більшість сучасних підприємств для організації своєї діяльності використовує інформаційну інфраструктуру та корпоративні інформаційні системи. Від надійності і безпеки їх функціонування напряму залежать безперервність процесів, доступність і цілісність даних, а отже і діяльність організації в цілому. У статті розглянуто питання забезпечення стійкості основних процесів та інформаційної безпеки організацій до негативних впливів надзвичайних ситуацій природного, техногенного, економічного, соціального характеру, а також питання відновлення діяльності та необхідного рівня безперервності щодо інформаційної безпеки під час та після ситуацій, що перешкодили штатному функціонуванню організації, з урахуванням характеру та ступеня їх впливу. У першому випадку завдання управління безперервністю діяльності полягають у запобіганні ризикової події і виражаються в розробленні та впровадженні превентивних заходів. У другому випадку – у зменшенні наслідків негативних впливів, що спричинили переривання діяльності організації, скороченні часу вимушеної заміни активів і зменшенні розміру витрат, пов'язаних з цією заміною. Описано еволюцію підходів щодо забезпечення безперервності діяльності організацій. Зроблено огляд стандартів та інших нормативних документів, у яких знайшли своє відображення кращі світові практики побудови систем управління безперервністю діяльності. У контексті процесної моделі менеджменту розглянуто основні етапи управління безперервністю діяльності, які полягають у послідовній реалізації замкнутого циклу "Плануй – Виконуй – Перевіряй – Дій", а саме: процесів планування, впровадження, підтримування, моніторингу, аналізування та поліпшення результативності побудованої системи управління безперервністю діяльності. Акцентовано увагу на тому, що організації у рамках цієї системи повинні розробити, задокументувати, реалізувати та підтримувати процедури і заходи безпеки для гарантування необхідного рівня безперервності інформаційної безпеки в умовах впливу загроз і дестабілізуючих чинників різної природи. Зроблено висновки стосовно переваг, що отримують організації завдяки розробленій та впровадженій системі управління безперервністю діяльності, у якій інтегровано заходи щодо забезпечення інформаційної безпеки.

Ключові слова: інформаційна безпека; управління безперервністю діяльності; процесний підхід; оцінювання ризиків; максимально прийнятний період переривання; допустимий час відновлення; цільова точка відновлення.

Постановка проблеми. У сучасному менеджменті дедалі більшого значення набуває забезпечення стійкості і безперервності діяльності організацій. Це спричинено: по-перше, існуючою тенденцією розширення спектру загроз безпеці діяльності. По-друге, високою імовірністю виникнення позаштатних і надзвичайних ситуацій, що призводять до порушення нормальної діяльності організацій, до неможливості виконання покладених на них зобов'язань перед споживачами і контрагентами. По-третє, постійно зростаючою залежністю сучасних організацій від інформаційних технологій (ІТ), які в деяких галузях (телекомунікації, інтернет-комерція та ін.) є основою їх діяльності, а в багатьох інших важливим елементом управління основними процесами (транспорт, енергетика та інші

виробництва). Повсюдна інформатизація та автоматизація різноманітних сфер людської діяльності тягнуть за собою збільшення масштабів аварій, катастроф, а отже і збитків господарюючого суб'єкта.

У 2007 році для описання непередбачуваних подій на кшталт терористичного акту у США 11 вересня 2001 р., спалаху смертельно небезпечних захворювань, японського землетрусу 2011 р., цунамі та аварії на АЕС введено поняття "чорний лебідь" [1]. Однак, як показує практика, в організаціях здебільшого "трапляються" більш дрібні "чорні лебеді" (відмова комунальних мереж, часткове загоряння офісу, падіння сервера, обрив кабелю, відключення електроенергії), що здатні ускладнити, призупинити або навіть перервати нормальну діяльність організації.

За результатами досліджень Network Computing, the Meta Group and Contingency Planning Research встановлено, що одна година простою інформаційної системи обходиться інтернет-магазину в середньому в 1,1 млн. доларів. Для промислових підприємств середня годинна втрата становить близько 1,6 млн. доларів. Для комунальних підприємств, таких як телекомунікації та енергетика, потенційні втрати, викликані простоєм інформаційної системи, можуть досягти 2,8 млн. доларів на годину, це більше ніж 67 млн. доларів за добу [2]. Для окремих організацій даун-тайм закінчується фатально. 60 % компаній, що під час надзвичайної ситуації втратили свої дані, закриваються протягом шести місяців [3].

Загроза аварій не є чимось ефемерним, вона є реальною і може вдарити по будь-якій без винятку організації у найнесподіваніший для неї момент. Втім, негативні наслідки її впливу, у тому числі на інформаційну безпеку, мають бути зведені до мінімуму: дані повинні бути збережені, технічні засоби перебувати в робочому стані, люди – поза небезпекою, репутація організації має бути врятованою. Вирішення зазначених завдань є можливим завдяки управлінню безперервністю діяльності.

Управління безперервністю діяльності (Business Continuity Management, BCM) – це цілісний процес управління, в рамках якого ідентифікуються потенційні загрози діяльності організації, оцінюється можливий вплив на операції у разі реалізації цих загроз, а також створюються приписи для забезпечення здатності організації відновлювати свою діяльність і ефективно реагувати на інциденти, що дає змогу гарантувати дотримання інтересів зацікавлених сторін, забезпечити захист репутації, бренду й операцій, що мають цінність [4].

Аналіз останніх досліджень і публікацій. Історія управління безперервністю діяльності почалася у 50-х рр. XX ст. Саме тоді організаціями, які зіштовхнулися з проблемою відновлення діяльності після аварій, введено в практику зберігати дублікати критичних даних в електронній та паперовій формах у віддалених приміщеннях. Що стосується поняття "безперервність діяльності", то воно з'явилось дещо пізніше – у 90-х роках минулого століття.

У 1988 р. при Вашингтонському університеті заснований Міжнародний інститут аварійного відновлення (Disaster Recovery Institute International, DRII), а у 1994 р. у Великій Британії – Інститут безперервності діяльності (Business Continuity Institute, BCI). Нині кожен із згаданих інститутів об'єднує понад десяток тисяч сертифікованих фахівців у сфері забезпечення безперервності діяльності організацій у більш ніж ста країнах світу. Основний напрямок діяльності інститутів – поширення і просування кращих практик управління безперервністю діяльності та аварійного відновлення після надзвичайних ситуацій; експертиза відповідних стандартів і нормативних документів.

Проблеми, пов'язані з управлінням безперервності діяльності, і підходи до їх вирішення знайшли своє відображення у наукових працях зарубіжних та вітчизняних вчених з економіки, менеджменту, кібернетики та інформатики. Найбільша кількість досліджень з питань управління безперервністю діяльності проводиться для кредитно-фінансових організацій, визначаються можливість і здатність банківської сфери витримувати катастрофічні події як фінансового, юридичного, так і фізичного характеру.

Зарубіжний досвід у дослідженні питань планування безперервності діяльності представлений у роботах A. Hiles, S. Snedaker, J. Rittinghouse, J. Ransome, M. Wieczorek, U. Naujoks, B Bartlett, S. Akhtar, S. Afsar [5] - [9]. Ці та інші публікації [10] - [14] присвячені практиці впровадження системи управління безперервністю діяльності організації; використанню інтегрованих засобів автоматизації процесу управління; огляду нормативних документів і стандартів, які застосовуються в роботі з управління безперервністю діяльністю; управлінню ризиками, а також вимогам, що висуваються до організацій, щодо забезпечення безперервності діяльності організації та її відновлення після переривань.

Тим часом, у цих дослідженнях недостатньо уваги приділено питанням інтеграції безперервності інформаційної безпеки у систему управління безперервністю діяльності організації.

Мета статті є розглядання у контексті вимог міжнародного стандарту ISO/IEC 27001 основних аспектів залучення безперервності управління інформаційною безпекою в систему управління безперервністю діяльності організації на етапах її створення, впровадження, функціонування, моніторингу, аналізування та поліпшення.

Виклад основного матеріалу дослідження. Передовий досвід побудови ефективних систем управління безперервністю діяльності організації акумульовано у стандартах, нормативних документах, прийнятих у різних країнах: практиках британського інституту безперервності бізнесу (Business Continuity Institute, BCI), міжнародного інституту аварійного відновлення (Disaster Recovery Institute International, DRII) і американського інституту SANS (SysAdmin, Audit, Network, Security Institute), стандартах і специфікаціях Британського інституту стандартів (British Standard Institute, BSI), керівництвах Австралійського національного агентства аудиту (Australian National Audit Office, ANAO); у національних стандартах: Німеччини (BSI 100-4), США і Канади (NFPA 1600, NIST SP 800-34); у відповідному розділі міжнародного стандарту з інформаційної безпеки ISO/IEC 27001; а також у міжнародних стандартах ISO 22301, ISO 22313, ISO/IEC 27031; стандартах і бібліотеках COBIT, ITIL, MOF в частині безперервності діяльності, галузевих стандартах.

Розглянемо хронологію появи основоположних у цій сфері стандартів. Спочатку у полі зору управління безперервністю діяльності організації перебували, в основному, інформаційно-технологічні аспекти. У 1995 році на замовлення уряду Великобританії розроблено прародич міжнародних стандартів з управління інформаційною безпекою – британський стандарт BS 7799 (прообраз ISO/IEC 27001). Документ описував 127 необхідних для побудови системи управління інформаційною безпекою організації механізмів контролю, визначених на основі кращих прикладів світового досвіду в цій сфері. Цей стандарт багато в чому випередив свій час. В одному з його розділів інформаційна безпека розглядалась у взаємозв'язку з управлінням безперервністю діяльності.

У 2002 році Інститут безперервності діяльності опублікував першу версію "Настанов щодо найкращих практик" (Good Practice Guidelines), а через рік спільно з Британським інститутом стандартів на їх основі підготував загальнодоступну специфікацію Publicly Available Specification (PAS 56). У цьому документі подано термінологію, описано принципи та процеси менеджменту безперервності діяльності, а також критерії та техніки оцінювання. У PAS 56 вперше запропоновано п'яти ланкову схему проведення замкненого кола робіт з управління безперервністю діяльності.

У 2005 році британські інститути BCI та BSI почали працювати над стандартом BS 25999 з управління безперервністю діяльності. У 2006 році ними опубліковано першу його частину BS 25999-1 "Управління безперервністю діяльності. Частина 1: Практичні правила", а у 2007 році – другу частину BS 25999-2 "Управління безперервністю діяльності. Частина 2: Специфікація". Обидві частини внесли значний вклад в подоланні проблематики забезпечення безперервності діяльності та лягли в основу міжнародних і багатьох національних стандартів. У 2012 році на основі BS 25999-2 розроблено та опубліковано основний з управління безперервності діяльності міжнародний стандарт ISO 22301

“Соціальна безпека. Системи управління безперервністю бізнесу. Вимоги” [4], а на основі BS 25999-1 – міжнародний стандарт ISO 22313 “Соціальна безпека. Системи управління безперервністю бізнесу. Керівництво” [15]. Перший з них орієнтований на визначення вимог до систем управління безперервністю діяльності, другий надає стислі роз’яснення та коментарі з розроблення та впровадження таких систем. Стандарт ISO 22301 використовує відому модель PDCA – “plan – do – check – act” (ПВПД – “плануй – виконуй – перевіряй – дій”) стосовно процесів планування, впровадження, підтримки, моніторингу, аналізування і постійного поліпшення результативності системи управління безперервністю діяльності.

У 2012 році також опубліковано міжнародний стандарт ISO/IEC 27031:2011 “Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для забезпечення безперервності діяльності”. Як зазначається в анотації, “Стандарт ISO/IEC 27031:2011 описує концепції і принципи готовності інформаційно-комунікаційних технологій до забезпечення безперервності діяльності, і забезпечує систему методів і процесів для виявлення і визначення всіх аспектів (таких, як експлуатаційні характеристики, проектування і впровадження), з метою підвищення готовності інформаційно-комунікаційних технологій організації до забезпечення безперервності діяльності [16]”.

Готовність IT до забезпечення безперервності діяльності (ICT Readiness for Business Continuity, IRBC) – це важлива складова частина впровадження та функціонування системи управління безперервністю діяльності організацій [17].

Здебільшого концепцію управління безперервністю діяльності впроваджують як елемент корпоративного управління інформаційною структурою організації. У міжнародному стандарті ISO/IEC 27001:2013 забезпечення безперервності діяльності розглядається як одна з 14 областей управління інформаційною безпекою [18].

Дійсно, управління безперервністю діяльності “випливає” з системи управління інформаційною безпекою, успадковує її методологію та основні принципи:

– оцінювання ризиків виникнення і впливу надзвичайних ситуацій на ділові процеси і функції;

– контролювання і управління інцидентами;

– стратегічне і тактичне планування безперервністю інформаційно-комунікаційних технологій.

Водночас, управління безперервністю діяльності не можна ототожнювати з управлінням інформаційною безпекою. Управління безперервністю діяльності організації, взявши свій початок від резервного копіювання інформації, охопило, крім інформаційної безпеки, майже всі аспекти ділової активності і поступово перетворилось у цілісну структуру поглядів на методи забезпечення безперервності діяльності – стійкості організації до всіляких збоїв, руйнувань, втрат, у першу чергу – фінансових.

Загалом, процес управління безперервністю діяльності можна поділити на два напрями:

– забезпечення стійкості процесів організації до позаштатних та надзвичайних ситуацій;

– відновлення процесів, операцій і ресурсів організації після них.

У першому випадку завдання управління безперервністю діяльності полягають у зменшенні ймовірності ризикової події і виражаються у розробленні і впровадженні превентивних антикризових заходів. У другому випадку – у зменшенні негативного впливу надзвичайних чи кризових ситуацій, аварій.

Як процес управління безперервністю діяльності організації починається з аналізування процесів, а також ресурсів, що їх підтримують, оцінювання ризиків, їх впливу на діяльність організації з подальшим визначенням стратегій, сценаріїв і планів дій. Розглянемо ці етапи більш детальніше.

Аналізування процесів організації (Business Environment Analysis, BEA). На цьому етапі виокремлюють основні і допоміжні процеси, ранжують їх за ступенем впливу на

безперервність ділової активності організації, а також визначають ступінь залежності процесів від інформаційних технологій та зовнішніх сервісів. Наприклад, специфіка процесів медичної установи є такою, що відмова системи обліку пацієнтів не буде критичною, у той же час, збій в роботі високотехнологічного та реанімаційного обладнання призведе до непоправних наслідків.

Оцінювання ризиків (Risk Assessment, RA). З одного боку, управління безперервністю діяльності організації є частиною управління ризиками, з іншого – управління ризиками – складова управління безперервністю діяльності.

Оцінювання ризиків складається з окремих послідовних процесів [19]:

– ідентифікування ризиків – визначення елементів ризиків, описування кожного з них, складання їх переліку;

– аналізування ризиків – вимірювання їх рівня;

– порівняння рівня ризиків з критеріями оцінювання ризиків і критеріями прийняття ризиків, встановленими при визначенні області застосування менеджменту ризику.

Ідентифікуючи та аналізуючи ризики, вивчають загрози, що можуть призвести до порушення діяльності організації, аналізують сценарії їх реалізації та визначають можливі наслідки:

– несправність або недоступність обладнання;

– відсутність водопостачання, комунальних послуг, опалення, вентиляції, електроенергії;

– недоступність (неможливість використання) будівлі;

– недоступність (непрацездатність) критичного персоналу;

– недоступність (непрацездатність) виробників або постачальників послуг;

– пошкодження програмного забезпечення та/або даних та ін.

Аналізування впливу на діяльність (Business Impact Analysis, BIA). На основі даних, отриманих на попередніх двох етапах, складають карту ключових процесів та ймовірних порушень їх функціонування. Далі будують модель, у якій відображають зв’язки між порушеннями та категоріями (масштабами) потенційних втрат, що можуть бути зафіксовані як кількісно, так і якісно. Обов’язково враховують усі втрати: прямі і непрямі. Ними можуть бути: порушення інформаційної безпеки, втрата ділової репутації та довіри, зниження продуктивності, втрата доходів, збільшення операційних витрат, втрата конкурентних переваг, порушення законодавства та недотримання вимог регуляторів, штрафні санкції через невиконання контрактних зобов’язань.

Також на цьому етапі власники і керівництво організації разом з аналітиками повинні визначити, так звані, тайм-аути і продуктивну потужність для кожного виду діяльності (процесів, застосунків, сервісів), а саме:

– максимально прийнятний період переривання (Maximum Tolerable Period of Disruption, MTPD) – період часу, після закінчення якого несприятливі наслідки, що виникли в результаті переривання діяльності, стануть неприйнятними;

– допустимий час відновлення (Recovery Time Objective, RTO), або інтервал вимушеного простою – період часу після події переривання, впродовж якого повинні бути відновлені мінімальний рівень діяльності організації, підтримуючі його системи, застосунки та функції;

– цільова точка відновлення (Recovery Point Objective, RPO) – проміжок часу, що передує позаштатній ситуації, впродовж якого створені дані можуть бути втрачені. Для прикладу, якщо резервна копія даних створюється один раз на добу, то всі дані, які поступили після останнього створення резервної копії, у разі позаштатної ситуації будуть втрачені.

Проведення превентивних захисних заходів. Для зменшення рівня ризиків організації на цьому етапі необхідно обрати і реалізувати економічно вигідні контрзаходи, наприклад, такі як:

- укріплення будівлі, її конструкційних матеріалів;
- використання резервних серверів і комунікаційних каналів;
- електроживлення від різних трансформаторів;
- укладання угод з додатковими (надлишковими) постачальниками;
- страхування;
- встановлення джерел безперебійного живлення та електрогенераторів;
- впровадження технологій резервного копіювання даних;
- забезпечення захисту носіїв інформації;
- збільшення кількості запасних частин для критичного обладнання;
- впровадження систем виявлення і гасіння пожеж.

Резервне копіювання даних може бути повним, диференціальним чи інкрементним [20]. Зауважимо, яка б стратегія резервного копіювання не була обрана організацією, вона повинна враховувати ймовірність появи проблем на будь-якому кроці процесу створення резервної копії чи відновлення файлів з неї.

Чимраз більш широкого розповсюдження набувають “хмарні” послуги. Їх застосовують у тих випадках, коли необхідно забезпечити значення RTO і RPO на рівні не більше кількох хвилин. Для захисту даних та застосунків за допомогою “хмари” використовують технологію Disaster Recovery as a Service (DRaaS). У рамках послуги DRaaS організаціям надається інструментарій, за допомогою якого вони можуть проводити реплікацію даних в режимі реального часу, налаштовувати різні види бекапів, тестувати післяаварійне відновлення інформації. У цілому, застосування хмарних технологій дає можливість зменшити витрати на забезпечення безпеки, водночас, підтримуючи її на рівні стандартів, прийнятих в індустрії.

Розроблення стратегій безперервності діяльності (Business Continuity Strategy definition) – процес, який необхідний для обґрунтування технічних і організаційних рішень, що стосуються безпеки працівників, їх забезпечення робочими приміщеннями, технічними засобами і необхідними матеріалами; доступу до критично важливої інформації; безперешкодних комунікацій з партнерами, клієнтами, постачальниками і підрядниками.

На цьому етапі розробляють стратегії:

а) відновлення процесів;
б) відновлення будівель;
в) відновлення технічного середовища, зокрема:
   1) мережевого і комп’ютерного обладнання;
   2) комунікаційного обладнання для передачі голосу і даних;
   3) засобів для транспортування обладнання та персоналу;
   4) систем вентиляції, опалення та кондиціонування;
   5) систем забезпечення безпеки персоналу та даних;
   6) забезпечення різними витратними матеріалами (папір, бланки, кабелі);
   7) документації;
г) відновлення користувацького середовища;
д) відновлення даних.

Вибір організаційних і технічних рішень визначається стратегією управління безперервністю діяльності. На цьому етапі розробляють політики, які формалізують пріоритетні цілі і завдання підтримки безперервності діяльності, процедури реагування та області застосування системи управління безперервністю діяльності організації, здійснюють вибір технологій забезпечення доступності даних, визначають кадрові потреби та ступінь залучення персоналу до реалізації програми впровадження (проекту) управління безперервності діяльністю.

Розроблення і впровадження планів безперервності діяльності, зокрема плану забезпечення безперервності процесів (Business Continuity Planning, BCP) та плану їх відновлення у разі нештатних ситуацій (Disaster Recovery Plan, DRP). Специфіка планів залежить від типу організації, критичних для діяльності процесів та необхідного рівня їх стійкості до позаштатних ситуацій.

Враховуючи те, що основним пріоритетом забезпечення безпеки роботи будь-якої організації є люди, на цьому етапі розробляють чіткі інструкції, спрямовані на збереження їх життя, здоров'я під час та після надзвичайної ситуації.

Впровадження процесів управління безперервністю діяльності у корпоративну культуру передбачає інформування персоналу про заходи, які слід здійснювати у разі виникнення загроз з метою зменшення ризиків переривання діяльності, зменшення або нейтралізації негативних наслідків ризикових подій, а також про заходи необхідні для відновлення діяльності організації до прийнятного рівня у визначені терміни.

Всі працівники організації повинні знати: що і чому відбувається. Інакше надзвичайна подія викличе паніку, страх, домисли, що неодмінно позначиться на керованості організацією і це у кращому випадку, а в гіршому – призведе до занепаду організації протягом декількох днів. Яка би форс-мажорна обставина не мала місце, контроль над ситуацією повинен бути встановлений за лічені хвилини, максимум – години. Не пізніше трьох днів мають бути відновлені комунікації, після чого в організації починається кропітка робота по виходу її на колишній рівень, здійснюються заходи щодо трансформації нештатної ситуації в штатну. Зазвичай для відновлення діяльності потрібно кілька місяців. І саме від того наскільки добре підготовлений персонал залежить успіх цього процесу.

Перегляд і тестування розроблених планів, проведення тренінгів та навчань. З огляду на те, що організація, її оточення постійно змінюються, плани забезпечення безперервності забезпечення інформаційної безпеки та діяльності організації необхідно регулярно (не рідше одного разу на рік) переглядати та з метою перевірки їх працездатності тестувати. Як правило, під час тестування виявляють недоліки планування, які усувають на фазі "дій" циклу "плануй – виконуй – перевіряй – дій".

Є декілька підходів до проведення тестування планів та навчання персоналу: опитування методом анкетування, покрокове активне "читання" плану представниками окремих підрозділів організації, моделювання "віртуального" переривання тих чи інших процесів, паралельне тестування на альтернативних майданчиках, тестування на реальному об'єкті [21]. Вибір найбільш ефективного способу проведення тестувань та навчання залежить від типу організації і її цілей.

Висновки. Забезпечення безперервності інформаційної безпеки як і безперервності діяльності організації в цілому не є разовим проектом. Це складний, багатоетапний, циклічний процес управління, що вимагає компетентних працівників, відповідної підтримки керівництва і працездатних структур. Однак, коли безперервність управління інформаційною безпекою реально стає частиною системи управління безперервністю діяльності, організація отримує можливості:

– ідентифікувати потенційні загрози і своєчасно захистити свою діяльність, репутацію та інтереси споживачів й інших зацікавлених сторін від можливих інцидентів та надзвичайних ситуацій;

– адекватно реагувати, управляти ситуацією і швидко відновлювати діяльність та необхідний рівень безперервності щодо інформаційної безпеки під час та після руйнівних інцидентів;

– підвищити довіру споживачів і, як наслідок, конкурентоспроможність організації, розширити ринок збуту продукції і послуг;

– демонструвати законодавчим і наглядовим органам, а також всім, зацікавленим в діяльності організації, сторонам свою прихильність до загальноприйнятої практики управління безперервністю діяльності та забезпечення інформаційної безпеки.

Все це дає підстави організації позиціонувати себе як надійний і безпечний партнер.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] N.N. Taleb, *The Black Swan: The Impact of the Highly Improbable.* New York, USA: Random House Publishing Group, 2007.

[2] The One Essential Guide to Disaster Recovery: How to Insure IT and Business Continuity. [Online]. Available: https://www.pax8.com/resource/display/1499. Accessed on: May 02, 2019.
[3] DRP & BCP. Disaster Recovery and Business Continuity Plan. Exclusive research 2018 from IDC. [Online]. https://www.business-solutions.telefonica.com/media/2207/drp_bcp-white-paper-may18-web.pdf. Accessed on: May 02, 2019.
[4] International Organization for Standardization. (2012, May 15). *ISO 22301. Societal security. Business continuity management systems. Requirements.* [Online]. Available: https://www.iso.org/obp/ui/#iso:std:50038:en. Accessed on: May 02, 2019.
[5] A. Hiles, *The Definitive Handbook of Business Continuity Management.* Chichester, England: John Wiley & Sons, 2011.
[6] S. Snedaker, *Business Continuity and Disaster Recovery for IT Professionals.* Burlington, USA: Syngress Publishing, 2013.
[7] J. Rittinghouse, and J. Ransome, *Business Continuity and Disaster Recovery for InfoSec Managers.* Oxford, USA: Elsevier, 2005.
[8] M. Wieczorek, U. Naujoks, and B. Bartlett, *Business Continuity: IT Risk Management for International.* Berlin, Germany: Springer, 2002.
[9] S. Akhtar, and S. Afsar, *Business Continuity Planning Methodology.* Mississauga, Canada: Sentryx, 2004.
[10] *Business Continuity Preparedness Handbook.* AT&T Believes. 2016. [Online]. Available: https://www.attbelieves.com/ecms/dam/pages/disaster_relief/AT&T%20BCH.pdf. Accessed on: May 02, 2019.
[11] С.А. Петренко, и А.В. Беляев, *Управление непрерывностью бизнеса. Ваш бизнес будет продолжаться. Информационные технологии для инженеров*. Москва, Российская Федерация: ДМК Пресс, 2018.
[12] Kurt J. Engemann, *The Routledge Companion to Risk, Crisis and Security in Business*. New York, USA: Routledge, 2018.
[13] *Enhancing business continuity management to address changing business realities*. New York, USA: IBM Corporation, 2017. [Online]. Available: https://www.ibm.com/downloads/cas/ZGLEMLRR. Accessed on: May 02, 2019.
[14] В.В. Якубовський, "Сучасні підходи та моделі в менеджменті безперервності бізнесу", *Актуальні проблеми міжнародних відносин,* вип. 126, ч. II, с. 91-100, 2015.
[15] International Organization for Standardization. (2011, Dec. 15). *ISO 22313. Societal security. Business continuity management systems. Guidance*. [Online]. https://www.iso.org/standard/50050.html. Accessed on: May 02, 2019.
[16] International Organization for Standardization. (2011, March 01). *ISO/IEC 27031. Information Technology. Security Techniques. Guidelines for Information and Communication Technology Readiness for Business Continuity*. [Online]. https://www.iso.org/obp/ui/#iso:std:iso-iec:27031:ed-1:v1:en. Accessed on: May 02, 2019.
[17] Н.П. Кухарська, "IRBC – взаємозв'язок процесів управління інформаційною безпекою і безперервністю діяльності організацій", на *І Міжнар. наук.-техн. конф. Інформаційна безпека в сучасному суспільстві*, Львів, 2014, с. 35-37.
[18] International Organization for Standardization. (2013, Okt. 01). *ISO/IEC 27001. Information technology. Security techniques. Information security management systems. Requirements*. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en. Accessed on: May 02, 2019.
[19] International Organization for Standardization. (2018, June 06). *ISO/IEC 27005. Information technology. Security techniques. Information security risk management*. [Online]. https://www.iso.org/ru/standard/75281.html. Accessed on: May 02, 2019.

[20] Н.П. Кухарська, та А.Е. Лагун, "Інформаційна безпека процесу управління безперервністю бізнесу", на *наук.-практ. конф. Актуальні проблеми управління інформаційною безпекою держави,* Київ, 2015, с. 440-443.

[21] А.В. Дорофеев, и А.С. Марков, "Планирование обеспечения непрерывности бизнеса и восстановления", *Вопросы кибербезопасности,* № 3 (11), с. 68-73, 2015. [Электронный ресурс]. Доступно: https://cyberrus.com/wp-content/uploads/2015/09/vkb_11_9.pdf. Дата обращения: Май 02, 2019.

Стаття надійшла до редакції 05.06.2019.

REFERENCE

[1] N.N. Taleb, *The Black Swan: The Impact of the Highly Improbable.* New York, USA: Random House Publishing Group, 2007.

[2] The One Essential Guide to Disaster Recovery: How to Insure IT and Business Continuity. [Online]. Available: https://www.pax8.com/resource/display/1499. Accessed on: May 02, 2019.

[3] DRP & BCP. Disaster Recovery and Business Continuity Plan. Exclusive research 2018 from IDC. [Online]. https://www.business-solutions.telefonica.com/media/2207/drp_bcp-white-paper-may18-web.pdf. Accessed on: May 02, 2019.

[4] International Organization for Standardization. (2012, May 15). *ISO 22301. Societal security. Business continuity management systems. Requirements.* [Online]. Available: https://www.iso.org/obp/ui/#iso:std:50038:en. Accessed on: May 02, 2019.

[5] A. Hiles, *The Definitive Handbook of Business Continuity Management.* Chichester, England: John Wiley & Sons, 2011.

[6] S. Snedaker, *Business Continuity and Disaster Recovery for IT Professionals.* Burlington, USA: Syngress Publishing, 2013.

[7] J. Rittinghouse, and J. Ransome, *Business Continuity and Disaster Recovery for InfoSec Managers.* Oxford, USA: Elsevier, 2005.

[8] M. Wieczorek, U. Naujoks, and B. Bartlett, *Business Continuity: IT Risk Management for International.* Berlin, Germany: Springer, 2002.

[9] S. Akhtar, and S. Afsar, *Business Continuity Planning Methodology.* Mississauga, Canada: Sentryx, 2004.

[10] *Business Continuity Preparedness Handbook.* AT&T Believes. 2016. [Online]. Available: https://www.attbelieves.com/ecms/dam/pages/disaster_relief/AT&T%20BCH.pdf. Accessed on: May 02, 2019.

[11] S.A. Petrenko, and A.V. Beliaev, *Business Continuity Management. Your business will continue. Information technology for engineers*. Moscow, Russian Federation: DMK Press, 2018.

[12] Kurt J. Engemann, *The Routledge Companion to Risk, Crisis and Security in Business*. New York, USA: Routledge, 2018.

[13] *Enhancing business continuity management to address changing business realities*. New York, USA: IBM Corporation, 2017. [Online]. Available: https://www.ibm.com/downloads/cas/ZGLEMLRR. Accessed on: May 02, 2019.

[14] V. Yakubovskyi, "Modern approaches and models in the management of business continuity", *Actual problems of international relations,* vol. 126, iss. II, pp. 91-100, 2015.

[15] International Organization for Standardization. (2011, Dec. 15). *ISO 22313. Societal security. Business continuity management systems. Guidance*. [Online]. https://www.iso.org/standard/50050.html. Accessed on: May 02, 2019.

[16] International Organization for Standardization. (2011, March 01). *ISO/IEC 27031. Information Technology. Security Techniques. Guidelines for Information and*

Communication Technology Readiness for Business Continuity. [Online]. https://www.iso.org/obp/ui/#iso:std:iso-iec:27031:ed-1:v1:en. Accessed on: May 02, 2019.

[17] N. Kukharska, "IRBC – the interconnection of the processes of information security management and the continuity of the activities of organizations", at *I International Sci.-Tech. conf. Information security in modern society*, Lviv, 2014, pp. 35-37.

[18] International Organization for Standardization. (2013, Okt. 01). *ISO/IEC 27001. Information technology. Security techniques. Information security management systems. Requirements*. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en. Accessed on: May 02, 2019.

[19] International Organization for Standardization. (2018, June 06). *ISO/IEC 27005. Information technology. Security techniques. Information security risk management*. [Online]. https://www.iso.org/ru/standard/75281.html. Accessed on: May 02, 2019.

[20] N. Kukharska, and A. Lagun, "Information security of business continuity management process", on *conf. Actual problems of information security management of the state*, Kyiv, 2015, pp. 440-443.

[21] A. Dorofeev, and A. Markov, "Business continuity planning and disaster recovery planning", *Issues of Cybersecurity*, no. 3 (11), pp. 68-73, 2015. [Online]. Available: https://cyberrus.com/wp-content/uploads/2015/09/vkb_11_9.pdf. Accessed on: May 02, 2019.

NATALIIA KUKHARSKA,
OREST POLOTAI

INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

Most of modern enterprises use information infrastructure and corporate information systems to organize their businesses. Continuity of business processes, availability and integrity of data and the activity of the organization as a whole depend directly on the reliability and security of their functioning. The article deals with the issues of ensuring the sustainability of basic business processes and information security of organizations to the negative impacts of natural, man-made, economic, social nature emergencies, as well as the issue of recovery of business and the necessary level of continuity in information security during and after situations that hindered the regular functioning of the organization, taking into account the nature and extent of their impact. In the first case, the task of managing business continuity is preventing a risky event, developing and implementing preventative measures. In the second case, the task of managing business continuity is reducing the impact of negative consequences, that caused interruption of activity of organization, reducing the time it takes to replace assets, and reducing the costs related to the replacement. The evolution of approaches to ensure the continuity of the business is described. An overview of standards and other regulations, where best practices in building business continuity management systems are reflected, are done. In the context of the process model of management, the main stages of business continuity management, which consist in the sequential implementation of the closed cycle "Plan – Do – Check – Act", namely: the processes of planning, implementation, maintenance, monitoring, analyzing and improving the performance of business continuity management system, are considered. Attention is drawn to the fact that organizations within this system must develop, document, implement and maintain security procedures and security measures to ensure the necessary level of information security continuity in the face of threats and destabilizing factors of various nature. Conclusions have been made regarding the benefits that organizations gained due to developed and implemented a business continuity management system that has measures for information security.

Key words: information security; business continuity management; process approach; risk assessment; maximum tolerable period of disruption; recovery time objective; recovery point objective.

Кухарська Наталія Павлівна, кандидат фізико-математичних наук, доцент, доцент кафедри управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності, Львів, Україна.
ORCID: 0000-0002-0896-8361.
E-mail: kukharska.n@gmail.com.
Полотай Орест Іванович, кандидат технічних наук, доцент кафедри управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності, Львів, Україна.
ORCID: 0000-0003-4593-8601.
E-mail: orest.polotaj@gmail.com.

Kukharska Nataliia, candidate of physical and mathematical sciences, associate professor, associate professor of information security academic department, Lviv state university of life safety, Lviv, Ukraine.
Polotai Orest, candidate of technical sciences, associate professor of information security academic department, Lviv state university of life safety, Lviv, Ukraine.

DOI: 10.20535/2411-1031.2019.7.2.190559
УДК 004.056.53

ВІКТОР ГОРЛИНСЬКИЙ,
БОРИС ГОРЛИНСЬКИЙ

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Показано, що глобалізаційний вплив на кіберпростір, що проявляється у розповсюдженні кіберзлочинності, кібертероризму та інформаційній експансії, потребує його надійного захисту, а забезпечення кібербезпеки України в умовах проведення Операції об'єднаних сил, постає невід'ємною складовою і чинником забезпечення національної безпеки. Доведено, що побудова усталеної системи інформаційної безпеки держави в умовах глобалізації та розвитку інформаційних технологій і телекомунікаційних систем потребує з'ясування системоутворювальних основ і базових принципів системи забезпечення кібербезпеки як найважливішої складової інформаційної безпеки України. На підставі аналізу наукових публікацій стверджується, що дослідження проблеми забезпечення інформаційної безпеки відбувається, як правило, за двома основними напрямами – інформаційно-психологічному, спрямованому на захист свідомості від негативного інформаційного впливу та інформаційно-технічному, в якому основним об'єктом захисту є інформаційні ресурси в інформаційно-телекомунікаційних системах. Обґрунтовано, що методологічною основою розв'язання цього питання є системний підхід, який дозволяє враховувати у розумінні інформаційної безпеки як системного явища, не тільки певні види інформаційних загроз, але і багатофункціональність і багатовимірність предметного поля інформаційної безпеки. Доведено, що на підставі визначення об'єктів, що потребують захисту, розгалуження функцій і секторів відповідальності державних і приватних структур, доцільно розрізняти предметні області інформаційної та кібербезпеки. Сформульовано визначення інформаційної безпеки в широкому сенсі поняття, як сфери національної безпеки, що характеризується всебічною (правовою, економічною, техніко-технологічною і організаційною) захищеністю усталеного функціонування інформаційного простору, захищеністю інформаційних, інформаційно-технологічних і безпекових інтересів держави і