УДК 004.94[351.746:007]334 **JEL Classification C6; H61; H72**
DOI: https://doi.org/10.32515/2663-1636.2018.3(36).9-20

О.І.Волот, доц., канд. екон. наук
Чернігівський національний технологічний університет, м. Чернігів, Україна

Інформаційна та кібернетична безпека сучасного підприємства: забезпечення та моделювання

Висвітлені питання щодо забезпечення безпеки економічної інформації та створення надійної моделі кібернетичної безпеки підприємства. Визначено основні завдання та джерела загроз інформаційній безпеці, а також методологічні засади побудови інформаційної та кібернетичної безпеки сучасного підприємства. Представлено модель побудови системи інформаційної безпеки підприємства та проаналізовані основні моделі організації кібербезпеки.
інформаційне забезпечення, кібернетична безпека, інформаційно-комунікаційні технології (ІКТ), інформаційні технології (ІТ), модель

Е.И.Волот, доц., канд. экон. наук
Черниговский национальный технологический университет, г. Чернигов, Украина
Информационная и кибернетическая безопасность современного предприятия: обеспечение и моделирование

Освещены вопросы обеспечения безопасности экономической информации и создания надежной модели кибернетической безопасности предприятия. Определены основные задачи и источники угроз информационной безопасности, а также методологические основы построения информационной и кибернетической безопасности современного предприятия. Представлена модель построения системы информационной безопасности предприятия и проанализированы основные модели организации кибербезопасности.
информационное обеспечение, кибернетическая безопасность, информационно-коммуникационные технологии (ИКТ), информационные технологии (ИТ), модель

Постановка проблеми. В сучасних умовах розвитку і широкого використання інформаційно-комунікаційних технологій (ІКТ) сформувалися принципово нові глобальні субстанції — інформаційне суспільство, а також інформаційний та кібернетичний простори, які мають нині практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожного сучасного підприємства. Проте через небачене досі поширення ІКТ підприємства отримали не лише численні переваги, а й цілу низку проблем, зумовлених дедалі більшою вразливістю інфосфери щодо стороннього кібернетичного впливу, зокрема зростанням кількості кібератак. Кібератака - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій

для здійснення кібератак на інші об’єкти кіберзахисту [2]. Тому основними завданнями для сучасних підприємств є забезпечення безпеки економічної інформації та створення надійної моделі кібернетичної безпеки (своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз корпоративним та/або інформаційним системам), що є актуальністю сьогодення.

Аналіз останніх досліджень і публікацій. Вагомий внесок у дослідження теоретичних засад автоматизованого ведення обліку та запобіганню кібератакам зробили вітчизняні вчені, зокрема: Дубов Д.В. [4]; Зубок М. І. [9], Толубко В.Б. [14]., Низенко Е. І. [12], Ортинський В.Л. [13] та інші. Проте, ці напрацювання носять, в основному, технічний характер, чи розглядають суть і наслідки кібератак. Недостатньо висвітленими у науковій літературі залишаються питання, пов’язані з дослідженням кібератак в контексті їх впливу на функціонування системи обліку українського підприємства, питання щодо моделювання організації кібербезпеки підприємства та процесу створення надійної системи кібернетичної безпеки.

Постановка завдання. Метою статті є розглянути методичні підходи щодо побудови, забезпечення та моделювання інформаційної та кібернетичної безпеки сучасного підприємства з врахуванням проблем та ризиків при впровадженні та експлуатації інформаційних систем та технологій, які в повній мірі відповідають усім вимогам управління вітчизняними підприємствами. Розробити концепцію інформаційної та кібернетичної безпеки підприємства для формулювання шляхів зниження негативних наслідків, зокрема, мінімізації пов’язаних з ними витрат.

Виклад основного матеріалу. На сьогоднішній день своєчасна та об’єктивна інформація є важливим фактором виробництва, який розглядають, як один з основних ресурсів розвитку суспільства. Широкі можливості інформаційних систем та технологій дозволяють автоматизувати процеси моніторингу та управління державними, економічними, соціальними, оборонними та іншими об'єктами і системами, отримувати, накопичувати, обробляти і передавати інформацію про ці процеси практично з будь-якої необхідною швидкістю, в будь-якій кількості.

Інформаційне суспільство – це соціологічна концепція, що визначає головним фактором розвитку суспільства виробництво та використання науково-технічної та іншої інформації, а також сміливо можна говорити, що – це нова цивілізація, як інший рівень суспільного розвитку і культури, досягнутий суспільно-економічною формацією [15]. За умов швидкого розвитку глобального інформаційного суспільства, широкого використання ІКТ у всіх сферах життя особливого значення набувають проблеми інформаційної безпеки.

Інформаційна безпека підприємства – стан захищеності інформаційного середовища підприємства, який забезпечує його формування, використання та розвиток. Такі складові інформаційного середовища України, як інформаційні ресурси (у тому числі й інформаційні технології) та інформаційна інфраструктура (як матеріально-технічна основа створення, розповсюдження і використання інформаційних ресурсів), які входять до складу національного інформаційного потенціалу, сьогодні значною мірою визначають рівень і темпи соціально-економічного, науково-технічного і культурного розвитку країни [1].

Можна виділити цілу низку джерел загроз інформаційній безпеці сучасного підприємства:

- протизаконна діяльність деяких економічних структур у сфері формування, поширення і використання інформації;
- порушення встановлених регламентів збору, обробки та передачі інформації;
- навмисні дії та ненавмисні помилки персоналу інформаційних систем;
- помилки в проектуванні інформаційних систем;

− відмова технічних засобів і збоїв програмного забезпечення в інформаційних і телекомунікаційних системах, тощо [11].

Головною метою будь-якої системи інформаційної безпеки підприємства є забезпечення стійкого функціонування підприємства, запобігання погрозам його безпеці, захист законних інтересів від протиправних посягань, недопущення розкрадання фінансових коштів, розголошування, втрати, спотворення і знищення службової інформації, забезпечення нормальної виробничої діяльності всіх підрозділів об'єкту. Досягнення заданих цілей можливе в ході вирішення таких основних завдань [6]:

– виділення і віднесення інформації з найбільш важливих інформаційних потоків до категорії обмеженого доступу, тобто комерційної таємниці;

– прогнозування і своєчасне виявлення загроз безпеці інформаційним ресурсам, причин і умов, які ведуть до фінансового, матеріального і морального збитку, порушення нормального функціонування і розвитку підприємства;

– створення умов функціонування з найменшою вірогідністю реалізації загроз безпеці інформаційним ресурсам і нанесення різних видів збитку;

– створення механізму й умов оперативного реагування на загрози інформаційній безпеці і прояви негативних тенденцій у функціонуванні, ефективне припинення посягань на ресурси на основі правових, організаційних і технічних засобів забезпечення безпеки;

– створення умов для максимально можливого відшкодування і локалізації збитків, які спричиняються неправомірними діями фізичних і юридичних осіб, послаблення негативного впливу наслідків порушення інформаційної та економічної безпеки на досягнення стратегічних цілей.

Для побудови збалансованої моделі інформаційної безпеки підприємства спочатку передбачається провести аналіз ризику в області безпеки інформаційних потоків підприємства. Потім визначити оптимальний рівень ризику для підприємства на основі заданого критерію. Модель інформаційної безпеки підприємства повинна бути побудова таким чином, щоб досягти заданого рівня ризику.

На рис. 1 представлена модель побудови системи інформаційної безпеки підприємства, що відповідає спеціальним нормативним документам з забезпечення інформаційної безпеки, прийнятим міжнародним стандартам ISO/IEC 15408 "Інформаційна технологія – методи захисту – критерії оцінки інформаційної безпеки", стандарту ISO/IEC 27002 "Управління інформаційною безпекою" і враховує тенденції розвитку вітчизняної нормативної бази щодо питань інформаційної безпеки [16].

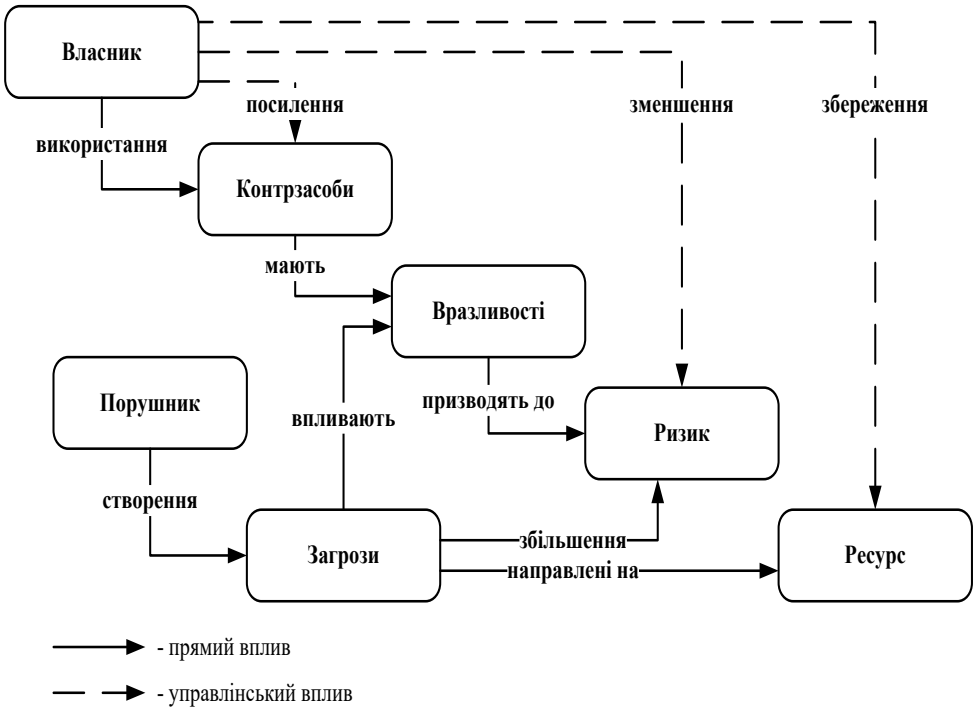

Рисунок 1 – Модель побудови системи інформаційної безпеки підприємства
Джерело: складено автором на основі [13]

Представлена модель інформаційної безпеки – це сукупність об'єктивних зовнішніх і внутрішніх чинників та їх вплив на інформаційну безпеку на підприємстві і на збереження матеріальних та інформаційних ресурсів. До цих об’єктивних чинників належать наступні:

– загрози інформаційній безпеці, які характеризуються вірогідністю виникнення, і реалізації загроз;

– вразливості інформаційної системи або системи контрзаходів, які впливають на вірогідність реалізації загроз для підприємства;

– економічний ризик – чинник, що відображає можливі збитки підприємства в результаті реалізації загрози інформаційній безпеці: витік інформації і неправомірне її використання, і як наслідок, вірогідні прямі та непрямі фінансові збитки.

Принципами побудови збалансованої моделі інформаційної безпеки підприємства є:

– аналіз ризиків у сфері інформаційної безпеки;

– визначення оптимального рівня ризику для підприємства на основі заданого критерію;

– вибір таких контрзаходів, які можуть забезпечити досягнення заданого рівня ризику.

Така методика дає змогу проаналізувати вимоги щодо гарантування інформаційної безпеки підприємства. Для досягнення поставленої мети необхідне вирішення певних завдань:

– розподілення інформації за рівнями доступу;

– прогнозування і своєчасне виявлення загроз безпеці інформаційних ресурсів,

– створення умов, при яких найменш вірогідна загроза безпеці інформаційних ресурсів;

– створення механізму і умов оперативного реагування на загрози інформаційній безпеці, забезпечення проведення робіт в короткі терміни;

– створення механізму і умов для максимально можливого відшкодування і локалізації збитку, завданого неправомірними діями фізичних і юридичних осіб;

– забезпечення оптимального вибору заходів протидії;

– оцінка ефективності контрзаходів, порівняння різних варіантів [13].

Кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [7].

На відміну від ІТ безпеки, що фокусується на захисті даних від крадіжки (таких як номери кредитних карток, корпоративна інформація та ін.), головна мета заходів із кібербезпеки системи керування – це підтримувати виробництво у робочому та безпечному стані. Основна загроза для обох цілей – це проникнення зловмисної програми до системи [5].

На сьогоднішній день, зростає кількість крадіжок та шахрайств в інтернеті, які зачіпають приватний сектор. Майже кожне підприємство в свой діяльності використовує комп'ютеризовану форму обліку, при цьому в них зберігається і оброблюється великий обсяг інформації і будь-який збій може призвести до великих витрат для підприємства [4].

За останні чотири роки в Україні відбулося кілька великих кібератак різного рівня складності і поширення. Одним з найвідоміших кіберінцидентів, що вразило інформаціно-телекомунікаційні системи як на державному рівні, так і на рівні окремих підприємств є вірус-шифрувальник Diskcoder.C (ExPetr, PetrWrap, Petya, NotPetya), що відбувся 27 червня 2017 року. Згідно з даними Департаменту кіберполіції Національної поліції України, під час масованої хакерської атаки в Україні були інфіковані понад 12,5 тисяч комп'ютерів. Основним каналом розповсюдження вірусу стало програмне забезпечення M.E.Doc, сервери якої було зламана задовго до самої атаки. Незважаючи на те, що вірус маскувався під дію віруса-здирника його цілями були шпигунство та подальше знищення атакованих систем [8].

27 жовтня 2017 року відбулася кібератака за допомогою вірусу Bad Rabbit, що вразила інформаційні системи Міністерства інфраструктури України, київський метрополітен, що призвело до збоїв в оплаті проїзду та аеропорт Одеси. Зараження комп'ютерних технологій здійснювалося за схожою схемою PetyA, відбувалося шифрування файлів. Самі хакери вимагали викуп у розмірі 0,05 біткоїн за кожний комп'ютер і встановлювався термін на його сплату. Аналітики стверджують, що сам вірус розповсюджувався за допомогою фейкового оновлення Adobe Flash.

Тому актуальним на сьогодні стає розроблення нових моделей кіберзахисту, в яких враховується весь період атаки, максимальний спектр підходів до оцінки загроз та арсенал можливостей інших споріднених видів діяльності (кіберрозвідки, кіберконтррозвідки, кібероборони та інші). Серед формалізованих моделей аналізу кібератак найбільшої уваги заслуговують Діамантова модель (Diamond Model) та Q Модель (Q Model) (табл.1). Вони застосовуються тільки для аналізу кібератак, для їх формалізації з метою надання відповіді на питання хто, навіщо і яким чином реалізував кібератаку, надають індикатори компрометації кібератак для подальшої кримінальнотехнічної експертизи, але вони не відображають етапів проведення кібератак . Діамантова модель встановлює основний атомний елемент будь-якої діяльності вторгнення, події, що складається з чотирьох основних функцій: зловмисника, інфраструктури, спроможності та жертви, які утворюють умовний "діамант". Проходячи по ребрах та вершинах, аналітики виявляють більше інформації про операції зловмисника та нові спроможності, інфраструктуру та жертв [8].

Таблиця 1 - Найбільш ефективні моделі організації кібербезпеки

Моделі кібербезпеки	**Можливості та особливості застосування**
Модель Лоткі-Вольтерра	Описує динаміку взаємодії сутностей двох видів - «хижаків» і «жертв». Модель представлена у вигляді системи двох звичайних диференціальних рівнянь першого порядку, де вводяться позначення: *X* – кількість атак на комп'ютерну мережу, що виконуються зловмисниками, це аналог «жертв»; *У* - кількість операцій, що виконуються захисниками комп'ютерної мережі, це аналог «хижаків»
Діамантова модель	Представляє нову концепцію аналізу вторгнень, побудовану аналітиками кібербезпеки. Перевагами моделі є: використання взаємозалежних індикаторів, що покращують обмін інформацією про кіберзагрози, підвищення контрольованості аналітичного процесу, підтримка характеристики подій у режимі реального часу, встановлення основи онтологій, таксономій, методик кіберзахисту та протоколів обміну розвідувальною інформацією про загрози, а також управління знаннями.
Q Модель	Дозволяє визначити атрибути кібератаки для з'ясування питання того, чи є кіберінцидент кіберзлочином. На рівні тактики модель допомагає аналітикам вирішувати весь спектр відповідних питань, інтегрувати як технічну, так і нетехнічну інформацію в конкуруючі гіпотези, допомагає критично мислити та провести результативне розслідування. Представлена модель є описовою й складається з трьох частин. Перша частина концептуальна: вона вводить розуміння атрибуції як процесу, описуючи модель в загальних рисах та вводячи кілька критичних відмінностей. Друга частина є емпіричною: вона ілюструє різні етапи процесу атрибуції в динаміці. У третій частині описується комунікація потенціалів та обмежень атрибуції й перетворення висновків у дію
Cyber Kill-Chain	Ця модель визначає типовий порядок дій зловмисника для досягнення поставлених цілей. Модель виражає, що для досягнення успіху зловмисник повинен пройти усі вісім етапів: розвідка, озброєння, доставка, зараження, інсталяція, отримання управління, виконання дій, знищення слідів
Adaptive Security Architecture	Є практично універсальною програмою. Вона передбачає імплементацію чотирьох типів реакції на кіберінцидент: запобігання, детектування, реагування і передбачення. Унікальність моделі проявляється в оперативному реагуванні на небезпеку і захист виробничого процесу від різних злочинних дій таких як: цільові атаки, спалахи кіберінфекції та навіть помилок людини. На скільки підприємство готово ретельно реалізовувати кожну стадію, характеризує ступінь зрілості її економічної безпеки. Ефективне практичне застосування цієї моделі на підприємстві повинно бути адаптованим до його специфіки та технологічних особливостей

Джерело: складено автором на основі [8,10,3]

При моделюванні системи кібербезпеки підприємства повинні бути враховані усі проблеми та ризики впровадженні та експлуатації інформаційних систем та технологій, що дозволить керівництву впроваджувати тільки ті технології, які в повній мірі

відповідають усім вимогам управління підприємствами та дозволяють підвищити ефективність діяльності і досягти конкурентних переваг на ринку галузі, а також дотримання певних принципів системи заходів кібербезпеки облікової інформації:

- підтримка програмного забезпечення (контроль за відсутністю неавторизованої зміни програм і прав доступу до них);
- охорона конфіденційної інформації (неухильне виконання персоналом бухгалтерської служби правил дотримання конфіденційності);
- персональна відповідальність (персональна відповідальність кожного користувача за всі види операцій, які він вчиняє з комп'ютерною обліковою інформацією);
- секретність (інформаційні ресурси доступні тільки авторизованим користувачам);
- комплексність (при побудові системи захисту передбачати прояв усіх видів можливих загроз для підприємства та всі можливі засоби захисту в межах єдиного комплексу захисту);
- ефективний контроль доступу до облікових даних (запровадження обмежень користувачів при роботі з цінною обліковою інформацією)

При побудові моделі необхідно враховувати взаємозв'язки між ресурсами: для виділених ресурсів визначається їх цінність як з точки зору можливих фінансових збитків, так і з точки зору можливого збитку репутації підприємства, дезорганізації його діяльності, нематеріального збитку від розголошування конфіденційної інформації тощо. Далі необхідно описати взаємозв'язки між інформаційними потоками, визначити загрози інформаційній безпеці підприємства і оцінити вірогідність реалізації даних загроз. На основі побудованої моделі можна обґрунтовано вибрати систему контрзаходів, які знижують ризики до допустимих рівнів і мають найбільшу економічну ефективність. Частиною системи контрзаходів є рекомендації щодо проведення перевірок ефективності системи захисту.

Висновки і перспективи подальших досліджень. На жаль, кіберзлочинність постійно вдосконалюється і йде в ногу з технологіями. Тому варто усвідомити, що протидія кіберзлочинності та рівень кібербезпеки на сьогодні – це проблема не лише загальнодержавного рівня, а кожного окремо взятого підприємства.

Отже, на кожному підприємстві повинна бути створена програма визначених дій, спрямованих на створення кіберзахисту облікової інформації.

У цілому, в статті розглянутий методичний підхід щодо моделювання інформаційної та кібернетичної безпеки дозволяє оцінити або переоцінити рівень поточного стану інформаційної безпеки інформаційних потоків підприємства, виробити рекомендації по забезпеченню інформаційної безпеки підприємства, знизити потенційні витрати підприємства шляхом підвищення стійкості системи інформаційних потоків, розробити концепцію і політику інформаційної та кібернетичної безпеки підприємства.

На основі методичного підходи та побудованої моделі можна обґрунтовано запропонувати плани захисту внутрішніх і зовнішніх інформаційних потоків, які створюються на підприємстві та передаються по різного роду каналах зв'язку і захистити інформацію підприємства від умисного спотворення, несанкціонованого доступу, копіювання або використання.

Перспективою подальших досліджень може бути аналіз загроз та сучасних засобів підтримки кібербезпеки інформаційних потоків підприємства.

Список літератури

1. Бабінська М.: Проблеми інформаційної безпеки України. – Вісник Науково-інформаційного центру НАТО Прикарпатського національного університету імені

Василя Стефаника. – 2009. № 2. - С. 11-15. URL: http://nato.pu.if.ua/journal/2009/2009-2.pdf (дата звернення:03.09.2019).
2. Вітер С.А., Світлишин І.І. Захист облікової інформації та кібербезпека підприємства. *Економіка і суспільство: електронне фахове видання*. 2017. № 11. С. 497–502. URL: http://www.economyandsociety.in.ua/journal/11_ukr/80.pdf (дата звернення:03.09.2019).
3. Войтов М. Модель адаптивної кібербезпеки для захисту промислових об'єктів URL: https://www.kaspersky.ru/blog/ics-asa/4455 (дата звернення:03.09.2019).
4. Дубов Д.В. Стратегічні аспекти кібербезпеки . *Стратегічні пріоритети* : наук.-аналіт. щокварт. зб. / Нац. ін-т стратег. дослідж. Київ : НІСД, 2013. 2013. № 4(29). – С. 119-126.
5. Гринцевич С. Базові рекомендації з кібербезпеки промислових систем керування для відділів АСУ ТП [Електронний ресурс] / Світлана Гринцевич // Асоціація Підприємств Промислової Автоматизації України. – 2017. URL: https://appau.org.ua/tk-185/bazovi-rekomendatsiyi-z-kiberbespeky-promyslovyh-system-keruvannya-dlya-viddiliv-asu-tp/ (дата звернення:03.09.2019).
6. Єрмоленко О. А. Економічна безпека системи інформаційних потоків підприємства [Текст] / О.А. Єрмоленко // Економіка: проблеми теорії та практики : зб. наук. праць / ДНУ. – 2009. – Т. 1. Вип. 253. – С. 82-89.
7. Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості Верховної Ради України. –2017. – № 2469-VIII – URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення:03.09.2019).
8. Жилін А. Функціональна модель ситуаційного центру кіберзахисту / А. Жилін, М. Худинцев, М. Літвінов. // Information Technology and Security. – 2018. URL: http://its.iszzi.kpi.ua/article/viewFile/153490/153471 (дата звернення:03.09.2019).
9. Зубок М. І. Безпека підприємницької діяльності: Нормативно-правові документи комерційного підприємства, банку. Київ: Істина, 2004. 144 с.
10. Кононович І. В. Моделі системи забезпечення кібербезпеки із запізнюванням реагування на інциденти / І. В. Кононович, Д. А. Маєвський, Р. С. Подобний // Інформатика та математичні методи в моделюванні. - 2015. - Т. 5, № 4. - С. 339-346. - URL: http://nbuv.gov.ua/UJRN/Itmm_2015_5_4_8 (дата звернення:03.09.2019).
11. Литвинюк, А. А. Основи інформаційної безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування / А.А.Литвинюк // Вісник ЦВК. – 2008. - №4. – С.18-21.
12. Низенко Е.І., Каленяк В.П. Забезпечення інформаційної безпеки підприємництва: навч. посіб. Київ: МАУП. 2006. 134 с.
13. Ортинський В.Л. Економічна безпека підприємств, організацій та установ : навч. пос. [для студ. вищ. навч. закл.] / [Ортинський В. Л., Керницький І. С., Живко З. Б. та ін.]. – К. : Правова єдність, 2009. – 544 с.
14. Толубко В.Б., Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: монографія. Київ: НАУ. 2013. 432 с.
15. Тоффлер Э. Третья волна: Пер. с англ. / Э. Тоффлер. – М., 2004. - 784 с.
16. ISO/IEC 15408:2008 – Information technology – Security techniques – Evaluation criteria for IT security. URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46414 (дата звернення:03.09.2019).

References

1. Babinska, M. (2009). Problemy informatsiinoi bezpeky Ukrainy [Problems of information security of Ukraine]. *Visnyk Naukovoho informatsiino-analitychnoho tsentru NATO Prykarpatskoho natsionalnoho universytetu imeni Vasylia Stefanyka - Bulletin of the NATO Scientific Information and Analysis Center Vasyl Stefanyk Precarpathian National University, 2,* 11-15. Retrieved from http://nato.pu.if.ua/journal/2009/2009-2.pdf [in Ukrainian].
2. Viter, S.A., & Svitlyshyn, I.I. (2017). Zakhyst oblikovoi informatsii ta kiberbezpeka pidpryiemstva [Protection of accounting information and cybersecurity of the enterprise]. *Ekonomika i suspilstvo: elektronne fakhove vydannia - Economy and Society: An Electronic Professional Edition, 11,* 497-502. Retrieved from http://www.economyandsociety.in.ua/journal/11_ukr/80.pdf [in Ukrainian].
3. Voytov, M. (2016). Model adaptyvnoi kiberbezpeky dlia zakhystu promyslovykh obiektiv [An Adaptive Cybersecurity Model for Industrial Security]. *kaspersky.ru.* Retrieved from https://www.kaspersky.ru/blog/ics-asa/4455 [in Russian].
4. Dubov, D.V. (2013). Stratehichni aspekty kiberbezpeky Ukrainy [Strategic aspects of cybersecurity in Ukraine]. *Stratehichni priorytety: naukovo-analitichnii shchokvartalnyi zbirnik Natsionalnoho institutu stratehichnykh doslidzhen - Strategic Priorities: National Science Institute Strategic Research Quarterly, 4(29),* 119-126 [in Ukrainian].
5. Hryntsevych, S. (2017). Bazovi rekomendatsii z kiberbezpeky promyslovykh system keruvannia dlia viddiliv ASU TP [Basic cybersecurity recommendations for industrial control systems for ACS departments]. *appau.org.ua*. Retrieved from https://appau.org.ua/tk-185/bazovi-rekomendatsiyi-z-kiberbespeky-promyslovyh-system-keruvannya-dlya-viddiliv-asu-tp/ [in Ukrainian].
6. Yermolenko, O.A. (2009). Ekonomichna bezpeka systemy informatsiinykh potokiv pidpryiemstva [Economic security of the enterprise information flow system]. *Ekonomika: problemy teorii ta praktyky : zbirnik naukovykh prats DNU - Economics: Problems of Theory and Practice: Collection of Scientific Papers DNU, Vol. 1, 253,* 82-89. [in Ukraine].
7. Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» [Law of Ukraine «On the Fundamental Principles of Cyber Security in Ukraine»]. (2017). *Vidomosti Verkhovnoi Rady Ukrainy - Information of the Verkhovna Rada of Ukraine, 45,* 403. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19. [in Ukraine].
8. Zhylin, A., Khudyntsev, M., & Litvinov, M. (2018). Funktsionalna model sytuatsiinoho tsentru kiberzakhystu [Functional model of cyber defense situation center]. *Zbirnyk "Information Technology and Security" KPI im. Ihoria Sikorskoho - Collection of "Information Technology and Security" KPI them. Igor Sikorsky, Vol. 6, 2(11),* 51-67. Retrieved from http://its.iszzi.kpi.ua/article/viewFile/153490/153471 [in Ukrainian].
9. Zubok, M.I. (2004). *Bezpeka pidpryiemnytskoi diialnosti: Normatyvno-pravovi dokumenty komertsiinoho pidpryiemstva, banku [Business security: Regulatory documents of a commercial enterprise, bank]*. Kyiv: Istyna [in Ukrainian].
10. Kononovych, I.V., Maievskyi, D.A., & Podobnyi, R.S. (2015). Modeli systemy zabezpechennia kiberbezpeky iz zapizniuvanniam reahuvannia na intsydenty [Models of cyber security systems with delayed response to incidents]. *Informatyka ta matematychni metody v modeliuvanni - Informatics and mathematical methods in modeling, Vol. 5, 4,* 339-346. Retrieved from http://nbuv.gov.ua/UJRN/Itmm_2015_5_4_8 [in Ukrainian].
11. Lytvyniuk, A.A. (2008). Osnovy informatsiinoi bezpeky. Kompleksna systema zakhystu informatsii: struktura, vstanovlennia ta pidtrymka funktsionuvannia [Fundamentals of Information Security. Comprehensive information security system: structure, installation and maintenance of operation]. *Visnyk TsVK - CEC Bulletin, 4,* 18-21 [in Ukrainian].
12. Nyzenko, E.I., & Kaleniak, V.P. (2006). *Zabezpechennia informatsiinoi bezpeky pidpryiemnytstva: Navchalnyi posibnik [Ensuring information security for entrepreneurship: A textbook]*. Kyiv: IEMA [in Ukrainian].
13. Ortynskyi, V.L., Kernytskyi, I.S., & Zhyvko, Z.B. (2009). *Ekonomichna bezpeka pidpryiemstv, orhanizatsii ta ustanov: Navchalnyi posibnik [Economic security of enterprises, organizations and institutions: A textbook]*. Kyiv: Pravova yednist [in Ukraine].
14. Tolubko, V.B., & Buriachok, V.L. (2013). *Osnovy formuvannia derzhavnoi systemy kibernetychnoi bezpeky: Monohrafiia [Fundamentals of formation of the state system of cyber security: Monograph]*. Kyiv: NAU [in Ukrainian].
15. Toffler, A. (2004). The Third Wave. (A. Toffler, Trans). Moskow: AST.
16. Mizhnarodnyj standart «Informatsijni tekhnolohii» ISO/IEC 15408:2008 [International Standard «Information Technology» ISO/IEC 15408:2008]. (2008). *iso.org.* Retrieved from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46414 [in Switzerland].

Olena Volot, Associate Professor, PhD in Economics (Candidate of Economic Sciences)
Chernihiv National University of Technology, Chernihiv, Ukraine

Information and Cybernetic Security of Modern Enterprise: Provision and Modeling

The article covers the issues of economic information security and creation of a reliable model of enterprise cyber security.

The overriding goal of any enterprise information security system is to ensure that the enterprise operates smoothly, prevention of threats to its security, protection of legitimate interests against unlawful attacks, preventing theft of funds, disclosure, loss, distortion and destruction of official information, ensuring the normal production activity of all units of the facility. Therefore, the article identifies the main tasks and sources of information security threats, as well as the methodological principles for building information and cyber security of a modern enterprise.

The model of building of information security system of the enterprise is presented and the basic models of the organization of cybersecurity are analyzed. Methodical approaches are offered, which allow to fully analyze and formulate requirements related to ensuring information security of the enterprise; avoid the expense of unnecessary security measures that are possible in subjective risk assessment; to assist in the planning and implementation of protection at all stages of the life cycle of the enterprise information system; provide justification for the choice of counteraction means; evaluate performance and compare different countermeasures.

In general, a methodical approach to modeling information security and cyber security was considered allows to evaluate or overestimate the level of the current state of information security of information flows of the enterprise, to make recommendations for ensuring information security of the enterprise, reduce the potential costs of the enterprise by increasing the stability of the information flow system, to develop the concept and policy of information and cyber security of the enterprise.

information provision, cyber security, information and communication technologies (ICT), information technologies (IT), model

ПЕРЕВІРЕНО. ВИПРАВЛЕНО