Соціально-правові студії. 2021. Випуск 3 (13). С. 156-162
Social & Legal Studios. 2021. Issue 3 (13). P. 156-162

UDC (УДК) 658.3:005.95/.96
JEL Classification: M12

Блага Наталія Василівна,
кандидат економічних наук, доцент,
доцент кафедри менеджменту
Львівського державного університету внутрішніх справ
(Львів, Україна)
e-mail: nblaga77@gmail.com
ORCID ID: 0000-0001-9433-9459

Гобела Володимир Володимирович,
кандидат економічних наук, доцент кафедри менеджменту
Львівського державного університету внутрішніх справ
(Львів, Україна)
e-mail: vvgobela@gmail.com
ORCID ID: 0000-0001-7438-2329

УДОСКОНАЛЕННЯ КОМУНІКАЦІЙНИХ ПРОЦЕСІВ НА ПІДПРИЄМСТВІ У КОНТЕКСТІ ЗМІЦНЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. Розглянуто елементи комунікаційного процесу на підприємстві з погляду інформаційної безпеки. Вказано на аспекти запровадження елементів сучасних інформаційних технологій у процес комунікації, котрі можуть і поліпшити рівень безпеки, і спричиняти певні ризики. Розроблено й запропоновано загальні принципи, дотримання яких сприяє інформаційній безпеці процесу комунікації на підприємстві. Водночас безпеку розуміємо як захист, якість та актуальність важливої інформації.

Ключові поняття: інформація, комунікаційний процес, інформаційна безпека, інформаційні технології, підприємство.

Blaga Nataliya,
PhD (Economics), Associate Professor,
Associate Professor of the Department of Management,
Lviv State University of Internal Affairs
(Lviv, Ukraine)
e-mail: nblaga77@gmail.com
ORCID ID: 0000-0001-9433-9459

Hobela Volodymyr,
PhD (Economics),
Associate Professor of the Department of Management,
Lviv State University of Internal Affairs
(Lviv, Ukraine)
e-mail: vvgobela@gmail.com
ORCID ID: 0000-0001-7438-2329

IMPROVEMENT OF INFORMATION SECURITY OF THE COMMUNICATION PROCESS AT THE ENTERPRISE

Abstract. The mechanism of communication process and information security at an enterprise is considered. The theoretical aspects of the communications at the enterprise are based on the variety of its form and the relation of organizational and information structures: most activities have underlying links via information processes. Thus information security of communication process has a significant impact on the information security of the enterprise as a whole. In modern conditions and circumstances, the information security of the enterprise is largely reduced to cybersecurity and suffers from most threats of the latter. However, the human factor is responsible for most of the real facts of inflicting harm due to information security breaches.

Thus, traditional mechanisms of privacy and confidentiality ensuring need to be adapted to new realities. New opportunities also set new requirements for understanding the very concept of information security: information must not only be protected but also timely and accurate as far as it is possible to be provided with modern telecommunication systems and information technologies: information security is a system of information protection of the enterprise – protection against theft, delayed and inaccurate providing of essential information to the recipient inside the enterprise or outside it. There are proposed and justified four principles necessary but not sufficient to ensure efficient mechanism of information security regarding communication process at small to medium enterprises. These include information awareness of staff even if they are not advanced with information technologies, traditional methods of protection against cyber threats such as passwords and encryption, control over information flows and the infrastructure that provides them, reliable cooperation and protection of remote access. These principles should be followed by managers at all levels.

Key concepts: information, communication process, information security, information technologies, enterprise.

DOI 10.32518/2617-4162-2021-3-156-162

Вступ

Розвиток ринкових відносин в Україні визначає діяльність організацій та умови їх функціонування. Щоб вижити організації мають правильно визначити свою стратегію і тактику поведінки на ринку, а також систематично управляти робочою силою, аби отримати прибуток. Управління передбачає комунікацію, що відбувається в інформаційному просторі підприємства.

Концепція загроз інформаційній безпеці виникла майже одночасно з інформаційним середовищем. Інформаційна безпека, що як поняття існувала у давні часи, в еру інтернету та телекомунікацій набула нових рис і потерпає від специфічних загроз, імманентних електронним телекомунікаційним системам. Спершу це виявлялося у несанкціонованому доступі до критичної комп'ютерної інформації, в неправдивому та незаконному її використанні, а також пошкодженні даних на персональних комп'ютерах. Згодом через розвиток інформаційних систем, провідну інформаційну загрозу несли такі засоби, як мережні віруси. Не можна сказати, що ці загрози відійшли у минуле, проте зараз на перше місце виходить безпека персональних даних, через яку відбувається вплив майже на кожного учасника світового інформаційного середовища. В Україні, що впродовж останніх декад долучилася до здобутків розвиненого інформаційного суспільства, проблеми інформаційної безпеки актуалізуються і на загальнодержавному рівні, і в межах кожної окремої компанії або підприємства.

Нині в Україні є близько трьох тисяч законів, які регулюють захист інформації та інформаційні відносини різних державних органів із громадськістю та підприємництвом. Українське законодавство в галузі інформації та інформаційної безпеки базується на Конституції України, Законі про інформацію, Законі про захист інформації в автоматизованих системах, низці кодексів та ряді спеціальних законів.

У процесі діяльності кожного підприємства як самостійної одиниці формується особливе інформаційне середовище із певними комунікаційними засобами. Керівництво вимагає від менеджерів спілкування з працівниками, щоб мотивувати їх ефективно виконувати завдання. Організаційна діяльність менеджера вимагає збору інформації про ситуацію на підприємстві, яка пояснює працівникам принципи, методи та цілі роботи.

Сьогодні комунікації набувають все більшої важливості та цінності. Особливої уваги потребує інформаційна безпека підприємств. Адже, нехтуючи інформаційними носіями, підприємець може отримати чималі збитки або й втратити компанію загалом, якщо відповідальний працівник не є обізнаний із сучасними можливостями і загрозами у цій сфері. Саме тому тема інформаційної безпеки комунікацій в сучасних умовах є актуальною і потребує детального дослідження. Менеджери можуть мати необхідні професійні якості, а для успішного виконання завдань повинні володіти техніками та навичками спілкування із урахуванням особливостей електронної комунікації.

Чимало відомих учених досліджували питання інформаційної безпеки підприємства, зокрема В. Цимбалюк, О. Сороківська, Г. Аніловська, О. Крюков, Ю. Коваленко та інші [1–3]. Проте донині низка питань є вкрай актуальною й потребує детального дослідження.

Метою статті є дослідження комунікаційного процесу на підприємстві у контексті інформаційної безпеки, з'ясування й обґрунтування основних принципів захисту комунікацій.

1. Аналіз теоретичних основ комунікаційного процесу та інформаційної безпеки підприємства

На початку 60-х років минулого століття лише в зарубіжній філософській та соціологічній літературі існувало близько сотні визначень поняття комунікації; можна стверджувати, що таких визна-

чень сьогодні набагато більше. Є низка підходів до дослідження спілкування й комунікації як теоретичного феномена та практичного інструменту.

Одним із важливих факторів інтеграції керівної структури організації є комунікація, тобто спілкування людей у процесі їхньої спільної діяльності: обміну ідеями, думками, відчуттями й інформацією. Жодна організована група людей не може існувати без комунікації.

Ефективне міжособистісне спілкування в сучасних умовах гуманістичного суспільства є важливе для успіху майже всіх типів організацій, зокрема підприємств. Це визначається двома чинниками: по-перше, вирішення багатьох завдань керівництва ґрунтується на безпосередній взаємодії людей (начальник з підлеглим, підлеглий з іншим підлеглим) між різними подіями; по-друге, міжособистісне спілкування може бути найкращим способом обговорення та вирішення проблем, що характеризуються невизначеністю і браком інформації у головних керівних ланках. Отож менеджер повинен пам'ятати, що процес комунікації потребує особливої уваги.

Процес комунікації – це процес передачі інформації від однієї людини до іншої або між групами людей за різними каналами та розмаїтими засобами спілкування (вербальними, невербальними тощо).

Для ефективного виконання своїх завдань керівник повинен планувати роботу об'єкта управління, організовувати її, розподіляти завдання серед безпосередніх виконавців і забезпечувати їх необхідними ресурсами, зацікавлювати працівників у якості дорученої роботи, контролювати результати та коригувати їхню діяльність, якщо це необхідно. Цю роботу неможливо виконати без чіткого уявлення про стан об'єкта, яким він керує, та його оточення, що можливо лише за наявності відповідної інформації. Серед щоденних робіт менеджера 50–70% видів робіт – це робота з інформацією. Сюди відносять обробку документів, заплановані та позапланові зустрічі, телефонні дзвінки, відвідування круглих столів тощо.

Способи фактичної організації комунікацій розмаїті – письмові, усні, за допомогою невербальних знаків та забезпечуються різними каналами – віч-на-віч, телефоном, конференційно, електронним спілкуванням із застосуванням зокрема сучасних мереж. Кожен із методів і каналів має свої переваги та недоліки залежно від їх використання, зазвичай оптимальним є поєднання різних способів.

Методи спілкування можна суміщати між собою, це даватиме більшу ефективність. На додаток до одночасного використання у спілкуванні елементів вербальної та невербальної комунікації, ми можемо вказати на ширше поєднання усного спілкування з паралельною інструкцією, у якій збалансовано поєднано чіткі вербальні інструкції із допоміжними засобами, такими як графіки, таблиці, діаграми, інші інструменти, які є конфігураціями письмової інформації. Такий підхід спрощує сприйняття, особливо, якщо воно складне і потребує часу для його розуміння, формує в адресата більш повне розуміння завдань, що перед ним стоять, підвищує надійність комунікаційного процесу щодо випадкових помилок та полегшує аналіз їх причин у разі виникнення.

При виборі способу спілкування необхідно враховувати певні обставини, пов'язані з процесом обміну інформацією. Так, усне спілкування має перевагу, коли інформацію потрібно надати негайно, тоді ж зворотний зв'язок зразу підтверджує правильне розуміння наданої інформації. Невербальні сигнали, які найчастіше супроводжують вербальне спілкування, допомагають правильно зрозуміти інформацію, і тому їх слід враховувати. Письмове спілкування є більш прийнятним, аніж усне, коли йдеться про важливі деталі та коли сторони оперують чисельними показниками. У деяких випадках необхідно поєднувати усне та письмове спілкування (ви можете повідомити про зустріч телефоном, а потім надіслати її дату письмово, щоб одержувач пам'ятав про зустріч і міг у будь-який момент уточнити її дату).

Отож комунікації – важливий елемент діяльності підприємства, а тому безпека підприємства загалом суттєво залежить від безпеки механізмів, що формують обмін інформацією у підприємстві та із його партнерами. Йдеться передусім про інформаційну безпеку.

Чимало відомих учених досліджували питання інформаційної безпеки загалом і підприємств зокрема. Так, В. Цимбалюк наголошує, що інформаційна безпека підтримує належний (бажаний, можливий) рівень життя інформаційної системи, включаючи підприємництво [1]. О. Сороківська зауважує, що поняття інформаційної безпеки підприємства слід також розглядати у контексті забезпечення безпечних умов існування інформаційних технологій, включаючи питання захисту інформації, побудови ефективної інформаційної інфраструктури, інформаційного ринку та створення безпечних умов існування і розвитку інформаційних процесів [2]. На жаль, суттєвий вплив на інформаційний ринок нерідко є поза можливостями конкретного підприємства, а тому питання розвитку інформаційних процесів у тому, що стосується інформаційної безпеки підприємства, не може бути вирішено загалом, а лише для конкретного підприємства у відповідних умовах. О. Коваленко вказує на багатоаспектність поняття інформацій-

ної безпеки й бачить її суть у певних діях щодо вияву, усунення та нейтралізації негативних джерел, причин і умов впливу на інформацію [3]. Саме ж поняття характеризує стан інформаційного захисту господарюючого суб'єкта. Погляди щодо суттєвості захисту інформації збігаються у більшості дослідників. Захист передбачає протидію ризикам, тому варто деталізувати загрози та ризики інформаційній безпеці.

2. Загрози інформаційній безпеці комунікаційного процесу на підприємстві

Ведучи свою справу, сучасний підприємець неодмінно стикається з потребами збору, обробки, зберігання, перетворення, передачі необхідної інформації. Якщо будь-яка інформація є цінною для підприємця, вона повинна бути захищеною від зловмисників.

Стверджують [3], що на сучасних підприємствах у сфері ІТ щороку відбувається до 20–30 інцидентів на рік, пов'язаних із втратою даних, більшість із яких має ненавмисний характер, за іншими даними близько 25% усіх працівників розкривають інформацію конкуруючим компаніям з певною метою.

Захист інформації в компанії є дуже важливим фактором для ефективного її розвитку і цей фактор повинен бути присутнім обов'язково. Коли фірма укладає контракт зі своїм працівником, особливо, якщо цей працівник займає керівну посаду в компанії, має укладатися договір про зберігання інформації. Хоча в нашій країні комунікаційна система на різному управлінському рівні не достатньо захищена юридично.

Загалом небезпеку становить можливість втрати чи розкриття інформації, що зберігається в інформаційних системах підприємства. Ці системи пересічно включають автоматизоване системне програмне забезпечення, програми для виконання певних завдань компанії, програмні оболонки, текстові процесори, програмні пакети, бази даних та інструменти обміну даними з інтернет. Традиційно саме останній блок програмного забезпечення становить особливий інтерес зловмисників. Нерідко це популярні соціальні мережі, поштові та пошукові сервіси тощо. Так, організація зі захисту споживачів у кіберпросторі вказує, що з 15/05/2020 в українському сегменті інтернету може відновити роботу потенційно шкідливе ПО (Яндекс, Mail.ru, «В контакте», «Одноклассники») [4]. Міжнародну компанію з управління готелями, Marriott, нещодавно зламали хакери: особисті дані 5,2 мільйона клієнтів зазнали ризику несанкціонованого доступу, включаючи імена, адреси електронної пошти тощо [5].

Щороку складність і масштаби інформаційних загроз зростають. Ми виокремили основні типи сучасних інтернет-загроз, які повинен знати кожен підприємець і пересічний громадянин [6].

Ціль фішингу *(phishing)* – видавання себе за іншу особу задля отримання цінної інформації, яка може бути продана або використана для зловмисних цілей, наприклад, вимагання чи крадіжка грошей або особистих даних. Найчастіше зловмисники фішингу видають себе за банки чи інші фінансові установи, щоб змусити жертву заповнити фальшиву форму та отримати інформацію про рахунок. Структурний підхід до комунікаційної безпеки у сфері банківської діяльності серед інших стисло розкрито у [7].

Загроза бекдор *(backdoor)* дозволяє зловмисникам контролювати заражений пристрій жертви без дозволу та віддалено; з цією метою здійснюють обхід автентифікації доступу.

Незаконний майнінг *(mining)* використовує нелегальний програмний код, що призначений для споживання обчислювальної потужності певного пристрою.

Загрози інтернет-безпеці є численні і пересічному користувачеві складно визначити, котрі саме файли є шкідливими програмами в мережі інтернет. У таких випадках застосовують рішення, що опирається на виявлення загроз за допомогою баз даних відомих програм, які несуть небезпеку та використання технологій для захисту від нових, а також для видалення шкідливих програм. Ці технології реалізовано у більшості сучасних антивірусних програм, проте має два суттєвих мінуси: передусім ці програми спроможні захистити лише від відомих вірусів, допоки вірус не вивчено й внесено у бази даних, антивірус його «не помічає». Тому, якщо зловмисник використовує новий код, розроблений безпосередньо для конкретної програми, він має всі шанси на успіх. З іншого боку, сучасне антивірусне забезпечення доволі вартісне і щодо фінансів, і щодо використання обчислювальних ресурсів комп'ютера, на який здійснюється його встановлення.

Кіберзлочинці постійно шукають нові шляхи зараження. Зокрема, сучасні загрози поширюються через вразливості системи, обходячи безпеку, приховуючи в пам'яті або наслідуючи законним програмам залишатися непоміченими. Однак більшість пристроїв заражаються вірусами через нехтування людиною, неуважність, некваліфікованість менеджера. Спеціально розроблені електронні листи з небезпечними доповненнями виявились ефективним та недорогим способом входу в систему жертви. Для цього зловмисникам потрібен лише один клік користувача, а розсилки таких листів здійснюються автоматизовано й широкому колу інтернет-користувачів. Саме від таких загроз

працівників підприємства може захистити елементарна кібергігієна [4].

Заразом значної шкоди іміджу підприємства завдають не лише витоки інформації (як от згаданий вище випадок із *Marriott*), а елементарна неуважність чи некомпетентність працівників, застарілі, некоректні чи неточні дані на сайті підприємства тощо. В епоху, коли інтернет-грамотність виховується із дошкільного віку, коли пошук товару користувач проводить на основі перших знайдених посилань на власному смартфоні, інформаційна обізнаність персоналу та вміння об'єднати у єдину систему знань професійну діяльність на підприємстві із можливостями інтернет-комунікації у і за межами підприємства є важливим чинником конкурентоспроможності останнього.

Так, на наш погляд, інформаційна безпека підприємства – це система захисту інформації підприємства; захисту від злодійства, невчасного і неточного подання її одержувачу. Нехтуючи інформаційними носіями, підприємець може отримати чималі збитки або й втратити компанію загалом.

3. Основні принципи інформаційної безпеки на підприємстві

Сьогодні традиційні методи інформування втрачають свою цінність внаслідок актуалізації медіа, кібер, діджитал та контентних потоків інформації. Кіберзлочинці можуть націлюватись не лише на відомі корпорації, а й на малий та середній бізнес, який обробляє інформацію про кредитні картки або зберігає певну конфіденційну інформацію; понад половину підприємств, опитаних згідно з [4], стикались із різними потенційними загрозами (рис. 1).

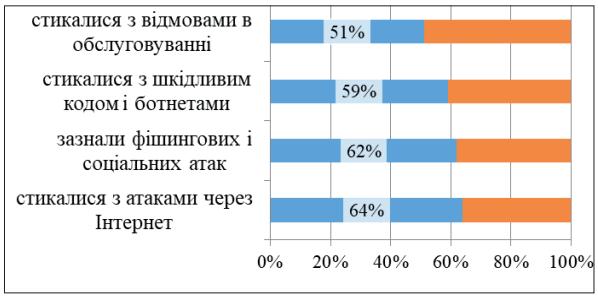

Рис. 1. Випадки порушення кібербезпеки підприємствами

(Складено на основі даних Організації з захисту споживачів у кіберпросторі)

Багато власників бізнесу з метою економії коштів на інформаційному захисті роблять велику помилку, оскільки не звертають уваги на захист даних, позаяк вважають, що це їх не стосується. Однак інструменти кіберзлочинців удосконалюються, а кількість жертв зростає. Проте найбільш поширеними причинами порушень кібербезпеки є людська недбалість

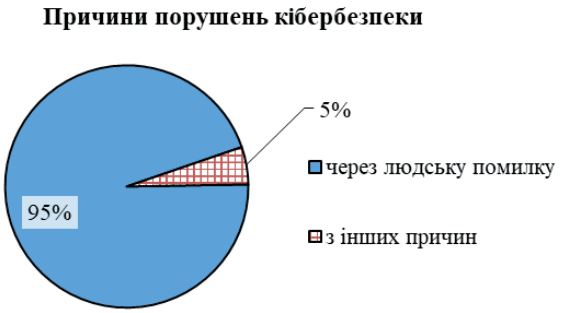

Рис. 2. Причини порушень кібербезпеки

(Складено на основі даних Організації з захисту споживачів у кіберпросторі)

(рис. 2).

Саме тому для того, щоб захистити своє підприємство від інформаційних загроз потрібно дотримуватися таких принципів:

1. *Вчасно і достовірно інформувати своїх працівників* про поточні зміни в організації, загрози занепаду чи перспективи розвитку. Зазвичай кіберзлочинці намагаються отримати доступ до даних організації через її «найслабше місце», а саме недосвідчений персонал. Спочатку зловмисники надсилають фальшиве повідомлення, настільки реальне, що працівник не підозрює про зловмисну роботу і відкриває його, якщо недостатньо обізнаний щодо справ фірми. Тоді сценарії різні: на пристрій завантажують віруси, трояни, шпигунське або інше шкідливе ПЗ. Саме тому першим кроком до посилення інформаційної безпеки в організації має стати інформування працівників про поточні загрози та засоби захисту від них. Кожен працівник має усвідомлювати необхідність захисту даних компанії та клієнтів, особливості кібергігієни, якщо у єдиному інформаційному просторі зберігаються власні та корпоративні дані. Керівникам підприємств треба регулярно проводити навчання з інформаційної безпеки у всіх підрозділах (маркетингу, продажів, кол-центру тощо), які працюють з даними щодо інформаційної безпеки та правил захисту даних, можливі способи атаки зловмисників та способи їх уникнення.

2. *Захист комп'ютера і носіїв інформації.* Незахищені дані зазнають кібератак та дії шкідливим програмам. Тому, якщо флешки, ноутбуки чи смартфони працівника компанії втрачені або вкрадені, працівник нерідко ставить під загрозу всі дані компанії. Щоб уникнути подібних ситуацій, рекомендуємо: завжди виходити з системи та ресурсів, що містять кон-

фіденційні дані, не залишати комп'ютер включеним; шифрувати всі ділові дані за допомогою інструментів шифрування, доцільно використовувати віддалене управління ключами шифрування та встановлювати правила для роботи з файлами, змінними дисками, картами пам'яті, іншими електронними носіями та електронною поштою. У разі втрати пристрою зловмисники не зможуть прочитати дані компанії, навіть якщо їх буде втрачено. Задля уникнення втрати даних можна використовувати хмарні сховища, як от *iCloud*, проте у цьому разі ви частково довіряєте організацію інформаційної безпеки третій стороні; альтернативою може бути регулярне створення резервних копій файлів.

3. *Контроль*. Із міркувань інформаційної безпеки на підприємстві конфіденційні дані слід зберігати на окремих серверах, одночасно забезпечуючи додатковий захист за допомогою служб безпеки. За належного рівня налаштувань та компетентності здебільшого можна майже до нуля знизити ризик розкриття даних шляхом використання надійних інструментів шифрування, інша річ, що це, зазвичай, значно ускладнює роботу з даними, передусім спільний доступ. Так, зменшується ризик крадіжки даних. Крім того, потрібно стежити за користувачами, які купують або намагаються отримати доступ до вашої мережі. Це дозволяє адміністраторам швидко виявляти підозрілу поведінку та реагувати на неї.

4. Надійне співробітництво та захист віддаленого доступу. Будь-яка угода про надання послуг, постачання або інше співробітництво має містити конкретні вимоги щодо безпеки. Багато постачальників хмарних послуг регулярно відслідковують ризики різних типів, щоб відповідати стандартам інформаційної безпеки в певній галузі. Постачальник послуг повинен мати рівень безпеки, який відповідає партнерським відносинам, і цінності захищеної інформації.

Швидкісний доступ до інтернету та сучасна робоча етика дозволяють багатьом офісним працівникам працювати вдома. Цей спосіб операції щороку стає все більш популярним. Особливо сьогодні можливість безпечної роботи на дистанції є великим активом для компаній. Водночас кожен працівник або клієнтський пристрій, що забезпечує віддалений доступ до робочої мережі, повинен відповідати стандартам захисту інформації.

Хоча, теоретично, сховище даних будь-якої компанії, що зберігає та обробляє дані користувачів, може бути зламано, дотримання усіх правил інформаційної безпеки дає змогу усунути від 80 до 95% найпоширеніших загроз, а тому таке підприємство матиме значно менші втрати в бізнес-процесах.

Висновки

Комунікація є невід'ємною рисою процесу управління, а інформаційна безпека комунікаційного процесу – суттєвим елементом безпеки підприємства загалом. Особливістю комунікації є те, що вона відбувається і у внутрішньому середовищі компанії, і за його межами. В сучасних умовах інформаційні технології виводять на новий рівень комунікаційні можливості, проте формують нові ризики для інформаційної безпеки.

Користувачі глобальної мережі та сучасних інформаційних систем зазнають ризиків втрат від численних зловмисних дій у вигляді фішингу, вірусів тощо. Водночас форми втрат й збитків можуть відрізнятися: розголошення персональних та конфіденційних даних й супутні іміджові втрати, розкриття негласної інформації та супутні втрати конкурентних переваг, втрата даних на електронних носіях, необхідних для нормального функціонування підприємства тощо. Інтеграція сучасних інформаційних систем у комунікаційний процес робить ці ризики актуальними для більшості підприємств.

Відмова від інформаційних технологій майже неможлива й може мати наслідком втрату позицій підприємства на ринку, проте оптимальним є поєднання розмаїтих методів та каналів комунікації із дотриманням правил інформаційної безпеки та кібергігієни. Одночасне використання елементів комунікації різного типу ускладнює діяльність зловмисників та сприяє підвищенню якості процесу спілкування у широкому сенсі. Підходи до організації обміну інформацією працівників підприємства між собою та із клієнтами відіграють визначальну роль в інформаційній безпеці підприємства.

Інформаційна безпека підприємства, на нашу думку, це система захисту інформації підприємства: захисту від злодійства, невчасного і неточного подання її одержувачу. Подання авторизованому споживачу неактуальної чи неточної (а по факту достовірної) інформації може нести загрозу, співвимірну із недостатнім захистом інформації на підприємстві.

Більшість загроз інформаційній безпеці пов'язані із людським чинником, а тому належна підготовка, навчання й інформування персоналу є першочерговим завданням щодо оптимізації механізму інформаційної безпеки. Ми вважаємо, що потрібно дотримуватися таких принципів: інформування персоналу, захист інформації, контроль інформаційної структури, надійна співпраця у сфері інформаційних технологій та послуг.

Список використаних джерел

1. Цимбалюк В. Інформаційна безпека підприємницької діяльності, визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації). *Підприємництво, господарство і право.* 2004. № 3. С. 88–91.
2. Сороківська О. А., Гевко В. Л. Інформаційна безпека підприємства: нові загрози та перспективи. *Вісн. Хмельниц. нац. ун-ту.* 2010. № 2. Т. 2. С. 32–35.
3. Коваленко Ю. О. Забезпечення інформаційної безпеки на підприємстві. *Економіка пром-сті*. 2010. № 3. С. 123–129.
4. Громадська організація «З захисту споживачів у кіберпросторі». *Офіційний сайт.* URL: https://bezbid.com/news/poperedzhennya-pro-zagrozu-kiberbgigiyeni/
5. Центр інформаційної та технічної підтримки в Україні. Компанія ESET. *Офіційний сайт.* URL: https://www.eset.com/ua/
6. Блага Н. Дослідження інформаційної безпеки комунікаційного процесу на підприємстві. Актуальні проблеми зміцнення економічної безпеки держави та суб'єктів господарської діяльності : матер. всеукр. наук.-практ. конф. (м. Львів, 16 квітня 2021р.) / за заг. ред. В. С. Бліхара. Львів : Львівський державний університет внутрішніх справ, 2021. С. 19–22. *Офіційний сайт*. URL: https://www.lvduvs.edu.ua/documents_pdf/biblio teka/nauk_konf/16_04_2021.pdf
7. Аніловська Г. Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій *Науковий вісник НЛТУ України*. 2008, 18.9. С. 270–273.

References

1. Tsymbaliuk, V. (2004). Informatsiina bezpeka pidpryiemnytskoi diialnosti vyznachennia sutnosti ta zmistu poniattia za umov vkhodzhennia Ukrainy do informatsiinoho suspilstva (Hlobalnoi kibertsyvilizatsii) [Information security of business activity, definition of essence and content of the concept under the conditions of Ukraine's entry into the information society (global cybercivilization)]. *Pidpryiemnytstvo hospodarstvo i pravo (Entrepreneuship, economy and law), 3,* 88–91 [in Ukr.].
2. Sorokivska, O. A. & Hevko, V. L. (2010). Informatsiina bezpeka pidpryiemstva: novi zahrozy ta perspektyvy. [Information security of the enterprise: new threats and prospects]. *Visn. Khmelnyts. nats. un-tu (Khmelnytskyi national university bulletin),* 2, *2,* 32–35 [in Ukr.].
3. Kovalenko, Yu. O. (2010). Zabezpechennia informacijnoji bezpeky na pidpryjemstvi [Ensuring information security at the enterprise]. *Ekonomika promyslovosti (Economics of industry),* 3, 123–129 [in Ukr.].
4. Gromads`ka organizaciya «Z zaxystu spozhyvachiv u kiberprostori» [Public Organization «Consumer Protection in Cyberspace»]. Retrieved from https://bezbid.com/news/poperedzhennya-pro-zagrozu-kiberbgigiyeni/ [in Ukr.].
5. Centr informacijnoyi ta texnichnoyi pidtrymky v Ukrayini. Kompaniya ESET [Information and technical support center in Ukraine. ESET]. Retrieved from https://www.eset.com/ua/ [in Ukr.]
6. Blaga, N. (2021). Doslidzhenia informacijnoji bezpeky komunikacijnogo procesu na pidpryjemstvi [Research of information security of the communication process at the enterprise]. *Aktualni problemy zmitsnennia ekonomichnoi bezpeky derzhavy ta subiektiv hospodarskoi diialnosti: materialy vseukrainskoi naukovo-praktychnoi konferentsii (Actual problems of strengthening the economic security of the state and economic entities: materials of the All-Ukrainian scientific-practical conference)* (Lviv, April 16, 2021), ed. V. S. Blikhar. Lviv : Lviv State University of Internal Affairs, 19–22 [in Ukr.].
7. Anilovska, H. Y. (2008). Informacijna bezpeka pidpryjemstva v umovah vykorystania suchasnyh informacijnyh tekhnologij [Information security of the enterprise in the conditions of use of modern information technologies]. *Naukovyi visnyk NLTU Ukrainy (UNFU Scientific Bulletin),* 18.9, 270–273 [in Ukr.].

Стаття: надійшла до редакції 19.04.2021
прийнята до друку 01.06.2021
The article: is received 19.04.2021
is accepted 01.06.2021