Proceedings of the 1st International Scientific and Practical Conference «Modern Knowledge: Research and Discoveries»

(May 19-20, 2023). Vancouver, Canada

No 155

# ACCOUNTING AND AUDITING

DOI 10.51582/interconf.19-20.05.2023.011

# Інформаційна безпека в умовах диджиталізації документообігу

**Людвенко Дмитро Віталійович[1],**

**Томілова-Яремчук Надія Олександрівна[2],**

**Хомовий Сергій Михайлович[3],**

**Крупа Наталія Миколаївна[4]**

[1] Доктор економічних наук, доцент, старший науковий співробітник відділу економіки регіонального розвитку та прогнозування; *ННЦ «Інститут аграрної економіки»;* Україна

[2] Кандидат економічних наук, доцент кафедри обліку і оподаткування; *Білоцерківський національний аграрний університет;* Україна

[3] Кандидат економічних наук, доцент, завідувач кафедри обліку і оподаткування *Білоцерківський національний аграрний університет;* Україна

[4] Кандидат біологічних наук, доцент кафедри садово-паркового господарства; *Білоцерківський національний аграрний університет;* Україна

**Анотація.**
У статті проаналізовано рівні захисту інформаційної безпеки. Визначено, що інформаційна безпека в системах цифрового документообігу є комплексним завданням, вирішення якого потребує поєднання заходів на законодавчому, адміністративному та програмно-технічному рівнях. Запропоновано заходи із захисту інформаційної безпеки в контексті цифровізації документообігу з метою підвищення оперативності прийняття управлінських рішень, прозорості в діяльності підприємств, збереження інформації.

**Ключові слова:**
*інформаційна безпека*
*цифровізація документообігу*
*електронний цифровий підпис*
*прийняття управлінських рішень*
*аналіз рівнів безпеки*
*програмні продукти*



*This work is distributed under the terms of the Creative Commons Attribution-ShareAlike 4.0 International License (https://creativecommons.org/licenses/by-sa/4.0/).*

Proceedings of the 1st International Scientific and Practical Conference «Modern Knowledge: Research and Discoveries»

(May 19-20, 2023). Vancouver, Canada

No 155

# ACCOUNTING AND AUDITING

Нині інформаційні технології розвиваються все стрімкішими темпами, і постає питання їх ефективного впровадження в роботу підприємств. Довгий час розроблялися паперові схеми документообігу, але сьогодні, в епоху розвитку інформаційних технологій, вони витісняються електронними. Вже досить давно підприємства різних форм власності спілкуються за допомогою обміну електронними документами. Все більше підприємств переходять на внутрішній електронний документообіг, оскільки це не тільки економить час, але й полегшує роботу співробітників і скорочує транзакційні витрати.

Характерною рисою сучасного етапу економічного і науково-технічного прогресу є бурхливий розвиток інформаційних технологій, їх максимально широке використання як у виробничо-господарській діяльності, так і в державному управлінні. Інформація та інформаційні технології все більше визначають розвиток суспільства і виступають новими джерелами національної сили. Становлення інформаційного суспільства докорінно змінює політичну, екологічну та соціальну сфери життя людини. За цих умов становлення інформаційного суспільства змінює предмет праці на інформацію та знання. У свою чергу, основою глобалізації є інтеграція інформаційних систем різних держав в єдину глобальну інформаційну систему, формування єдиного інформаційного простору, створення глобальних інформаційно-телекомунікаційних тенет, інтенсивне впровадження нових інформаційних технологій в усі галузі суспільного життя, включаючи і державне управління.

Інформатизація – це організаційний соціально-економічний і науково-технічний процес створення оптимальних умов для всебічного задоволення інформаційних потреб і реалізації прав громадян суспільства, органів державної влади і управління на основі формування і використання інформаційних ресурсів і використання інформаційних систем, мереж, ресурсів та інформаційних технологій з використанням обчислювальної та комунікаційної техніки [1].

Постає питання аналізу безпеки інформації та рівнів її захисту. Розуміння сутності поняття «інформаційна безпека» є важливим завданням наукового аналізу. Будь-яке вчення досягає зрілості і досконалості лише тоді, коли воно розкриває сутність досліджуваних явищ, має здатність передбачати майбутні зміни не тільки в області явищ, а й у сфері

*This work is distributed under the terms of the Creative Commons Attribution-ShareAlike 4.0 International License (https://creativecommons.org/licenses/by-sa/4.0/).*

# ACCOUNTING AND AUDITING

сутностей. Пізнання сутності інформаційної безпеки можливе лише на основі абстрактного мислення, створення теорії досліджуваного предмета, усвідомлення внутрішнього змісту, виявлення характерних ознак, розкриття сутнісних характеристик поняття, що вивчається.

Розуміння сутності цієї категорії визначається категоріально-понятійною системою інформаційної безпеки (табл. 1).

*Таблиця 1*

**Категоріально-понятійна система управління інформаційною безпекою**

| Назва категорії | Суть |
|---|---|
| **Інформаційні відносини** | виникають у всіх сферах життя і діяльності людини, суспільства і держави при отриманні, використанні, поширенні та зберіганні інформації. |
| **Інформаційний простір** | інформаційне середовище, в якому здійснюються інформаційні процеси та інформаційні відносини щодо створення, збирання, відображення, реєстрації, накопичення, збереження, захисту та розповсюдження інформації, інформаційної продукції та інформаційних ресурсів, на яке поширюється юрисдикція держави. |
| **Інформаційна інфраструктура** | набір взаємодіючих систем виробництва, накопичення, збереження та розвитку інформаційних продуктів та їх доставки, виробництва інформаційних технологій, інфраструктурних сервісних і систем навчання. |
| **Інформаційний ринок** | система економічних, організаційних і правових відносин щодо купівлі-продажу інформаційних ресурсів, технологій, продукції та послуг. |
| **Інформаційне забезпечення** | підтримка за допомогою систем баз даних і баз знань процесів виробництва, торгівлі, менеджменту, навчання, наукових досліджень та будь-якої іншої діяльності в усіх сферах життя суспільства, яка спрямована на створення умов для задоволення інформаційних потреб людей, суспільства та суспільства. |
| **Інформаційне поле** | сукупність енергетичних речовин окремих об'єктів. |
| **Сугестія** | прихований інформаційний вплив на інформаційну систему. |

*Джерело: складено на основі [2]*



*This work is distributed under the terms of the Creative Commons Attribution-ShareAlike 4.0 International License (https://creativecommons.org/licenses/by-sa/4.0/).*

# ACCOUNTING AND AUDITING

На нашу думку, інформаційну безпеку слід визначати як процес управління загрозами та небезпеками в інформаційній сфері. Враховуючи те, що структура внутрішньої системи інформаційної безпеки неможлива поза контекстом загроз і небезпек, наступним елементом для розгляду будуть рівні захисту інформаційної безпеки, які в сукупності дозволять окреслити напрями функціонування інформаційної безпеки.

Інформація може бути загальнодоступною або доступною лише для обмеженого кола людей. Питання захисту інформаційних систем актуальне лише тоді, коли наявні файли не призначені для загального огляду. Існує таке поняття, як захист інформаційних систем, яке поділяється на різні рівні безпеки. Захист даних є дуже актуальним з точки зору роботи бізнесу та державних підприємств, які дотримуються таємниці. Кожна компанія має певний обсяг інформації, який повинен бути доступний лише обмеженому колу людей. Тому підприємства розробляють захисні рівні інформаційних систем.

Розрізняють такі рівні захисту інформації [3]:

1. на робочому місці користувача;
2. на рівні підрозділу компанії;
3. на загальному рівні підприємства.

Перший рівень захисту досить простий, оскільки інформація вводиться користувачем, а потім зберігається на тому ж комп'ютері. У цьому випадку, щоб дані не надавалися іншим користувачам, досить просто поставити на комп’ютері код безпеки – і все. Але на великих підприємствах комп’ютери об’єднані в загальну локальну мережу.

Ця опція виключає можливість захисту інформації простим введенням пароля, оскільки всі користувачі локальної мережі мають доступ до файлової системи комп'ютера. У цьому випадку компанія розробляє захист на рівні підрозділу компанії. Створюються спеціальні засоби захисту, за допомогою яких лише певна кількість людей отримує доступ до локальної мережі.

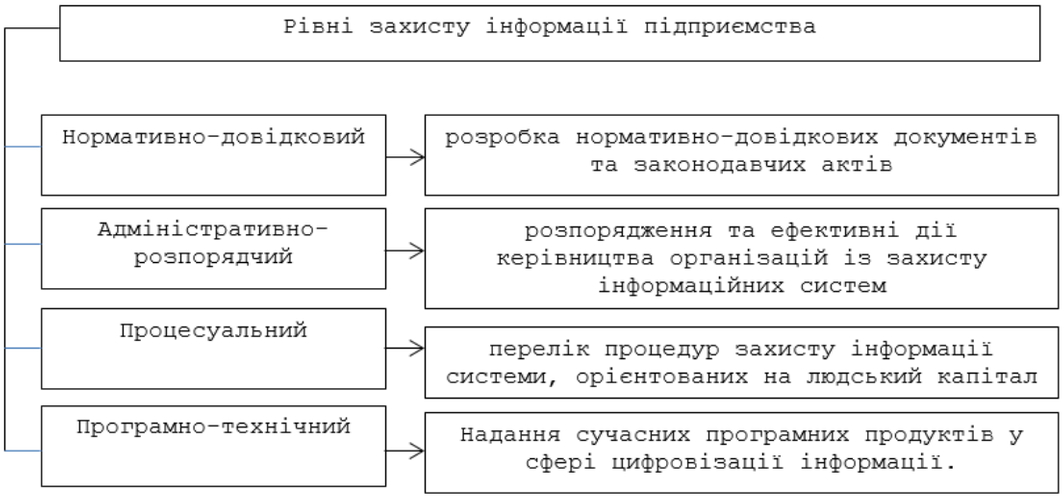
Сучасні підприємства не можуть не скористатися перевагами, які надає всесвітня мережа Інтернет. Підключення локальних мереж до Інтернету створює ризик несанкціонованого доступу до закритої інформації компанії, тому постає питання про захист інформаційних систем на рівні підприємства. Організувати захист інформації на підприємстві можна такими способами [4]:

*This work is distributed under the terms of the Creative Commons Attribution-ShareAlike 4.0 International License (https://creativecommons.org/licenses/by-sa/4.0/).*

# ACCOUNTING AND AUDITING

– захистити доступ до баз даних на фізичному рівні;
– контролювати доступ і персоналізувати кожного користувача;
– використовувати складні паролі та ключі для захисту інформаційних систем;
– захистити випромінювання від кабелю та захистити доступ до вузлів комутації;
– підключити систему захисту «зворотний дзвінок».

Будь-які засоби захисту інформаційних систем хороші, але, на жаль, вони не надійні на 100 відсотків. Тому для повноцінного захисту інформації рекомендуємо використовувати комбінації різних засобів захисту, а саме використання наступних рівнів захисту інформації (рис. 1).




*Джерело: розроблено авторами*

Визначення рівнів захисту інформаційної безпеки підприємства набуває особливого значення в умовах цифровізації, особливо документообігу, оскільки це дозволить без проблем обробляти будь-яку інформацію, що сприятиме прийняттю оперативних управлінських рішень щодо діяльність підприємства зокрема. Нові цифрові технології дозволяють створювати та поширювати величезні обсяги інформації майже необмеженому колу людей – швидко, якісно, дешево.

Документ — базовий елемент системи управління документами, який може бути файлом або записом у базі даних.


*This work is distributed under the terms of the Creative Commons Attribution-ShareAlike 4.0 International License (https://creativecommons.org/licenses/by-sa/4.0/).*

# ACCOUNTING AND AUDITING

Говорячи про безпечний документообіг, часто мають на увазі захист документів, тобто збереження інформації, яку ці документи містять. В даному випадку все зводиться до захисту даних від несанкціонованого доступу. Але мова йде не тільки про захист даних всередині системи, а про захист всієї системи, її працездатності, швидкого оновлення після пошкоджень, збоїв і навіть після руйнування.

Диджиталізація торкнулася всіх сфер нашого життя. На сучасному підприємстві його елементом є системи електронного документообігу. Адже робота з документами – як внутрішніми, так і зовнішніми – вважається найбільш трудомісткою. Сучасне програмне забезпечення допомагає оптимізувати та значно спростити процес. Ринок пропонує різні програмні продукти для диджиталізації документообігу. Проведемо порівняльний аналіз представлених програм (табл. 2).

*Таблиця 2*

**Порівняльний аналіз програмних продуктів для диджиталізації документообігу**

| Назва програми | Особливості | Переваги | Недоліки |
|---|---|---|---|
| M.E.Doc | Надійний та функціональний сервіс для підготовки та подання податкової та бухгалтерської звітності зі зручним інтерфейсом та широким функціоналом. Він дозволяє працювати не тільки зі звітністю, а й вести облік заробітної плати, обмінювати податкові/акцизні накладні, акти, накладні. | Програма універсальна, її можуть використовувати компанії та підприємці, які працюють у будь-якій галузі. Підходить для всіх форм оподаткування. Легко інтегрується з 1С:Підприємство (BAS) Обмін документами (без ліцензії та в демо-доступі можна відправити 50 документів безкоштовно) Автоматична обробка | Працює тільки під Windows 7 SP1, Windows 8, 10<br><br>Надсилати звіти на підпис директору не можна<br><br>Інтеграція потрібна для перенесення зведеного звіту з 1С:Підприємства |
| COTA | Зручний онлайн сервіс податкової звітності. Працює з податковими накладними та | Усі форми звітності до контролюючих органів можна подавати без встановлення | Якщо ви використовуєте SOTA з телефону або планшета, підключити |

*This work is distributed under the terms of the Creative Commons Attribution-ShareAlike 4.0 International License (https://creativecommons.org/licenses/by-sa/4.0/).*

# ACCOUNTING AND AUDITING

*Продовження табл. 2*

| | | | |
|---|---|---|---|
| | розрахунками коригування; формує декларації з використанням книги доходів. | програмного забезпечення, просто з веб-браузера, доступного з планшета чи телефону. (Функція ідентична MEDoc, тільки веб-версія) | токен неможливо Реєстр отриманих та виданих рахунків відсутній |
| FREDO: Звіт | Дозволяє реєструвати податкові накладні, формувати та надсилати звіти до контролюючих органів, а також надсилати та отримувати документи контрагентам. | Можливість автоматичного заповнення звіту даними з 1С:Підприємства або BAS будь-якої конфігурації в один клік. Ціна! У вартість ліцензії входить як облік ПДВ, так і облік акцизного податку | Реєстр отриманих та виданих рахунків відсутній |
| FREDO: Докмен | Дозволяє створювати документи безпосередньо в сервісі на основі готових шаблонів. Також надається можливість підписувати та надсилати їх користувачам аналогічного сервісу, а також MEDoc і SOTA, Flydoc | Дозволяє відправляти електронні первинні документи контрагентам без створення їх друкованих копій | Безкоштовних 50 документів немає |
| FlyDoc | Це модуль, який безпосередньо інтегрується в вашу базу даних «1С:Підприємство» або BAS і дозволяє обмінюватися документами безпосередньо з неї. | Він сумісний з багатьма конфігураціями цих програм, а обмін документами можливий з іншими сервісами за допомогою сервера «РТАН» або відправивши посилання на пошту, в месенджері. Користувачі | Якщо ви розробили новий шаблон у своїй програмі і хочете надіслати такий документ контрагенту, або ситуація навпаки, ви повинні мати такий самий |



*This work is distributed under the terms of the Creative Commons Attribution-ShareAlike 4.0 International License (https://creativecommons.org/licenses/by-sa/4.0/).*

# ACCOUNTING AND AUDITING

*Продовження табл. 2*

| | | | |
|---|---|---|---|
| | | вищезазначених рішень за чинним контрактом на підтримку ITS можуть БЕЗКОШТОВНО оновити свою програму до спільного BAS + FlyDoc. Після оновлення на робочому столі BAS з'явиться пункт меню «FlyDoc», який переведе вас на робочий стіл модуля FlyDoc з усіма можливостями сервісу. | шаблон у системі одержувача/ відправника. Вартість розробки такого зразка, в середньому, коштує 20 тис. грн. |

*Джерело: складено на основі [5, 6]*

Отже, використання диджиталізованого документообігу сприятиме отриманню оперативних даних про виробничо-господарську діяльність підприємства, а також сприятиме аналізу інформаційної безпеки з метою запобігання сторонньому доступу до відповідної інформації. Для цього необхідно розробити заходи захисту інформаційної безпеки в умовах диджиталізованого документообігу. Одним із способів такого захисту є використання програмних приманок як засобу забезпечення інформаційної безпеки.

Залежно від цілей, які переслідує програмна приманка, вона може мати різні параметри конфігурації, починаючи від програмних рівнів, які не вимагають великих налаштувань, і закінчуючи складними апаратними комплексами. Залежно від рівня складності приманки і її можливостей їх можна класифікувати на три групи: слабкий, середній і сильний рівні взаємодії.

Сьогодні найбільшої популярності набувають програмні приманки Honeypot – це приманка, на яку в разі удачі і високого коефіцієнта надійності потрапляє зловмисник. Завдання Honeypot – пройти атаку або несанкціоноване розслідування, що дозволить вивчити стратегію зловмисника та визначити спектр засобів, за допомогою яких можуть бути здійснені атаки на реальні об'єкти безпеки [7]. Реалізація Honeypot не є принциповою, і це може бути як спеціальний виділений сервер, так і один мережевий сервіс, завдання якого — привернути увагу хакерів.

*This work is distributed under the terms of the Creative Commons Attribution-ShareAlike 4.0 International License (https://creativecommons.org/licenses/by-sa/4.0/).*

# ACCOUNTING AND AUDITING

При бажанні адміністратор мережі може стежити за подіями в хронологічному порядку і дізнаватися, що сталося в певній частині інфраструктури за X годин Y хвилин Z секунд. Однак не можна заперечувати, що отримати необхідну інформацію часто досить складно, оскільки потрібно переглядати величезні файли журналів, щоб дізнатися, коли, де та як була виявлена ймовірна несанкціонована діяльність. З цієї точки зору інструменти Honeypot майже ідеальні: зібраної інформації небагато, але вся вона має велику цінність, оскільки така інформація розкриває суть спроби злому, сканування чи дослідження. Оскільки Honeypot спочатку був «скинутий» для атаки та дослідження, можна припустити, що майже вся інформація, взята з пастки, відображає дії зловмисників. На його основі ми можемо аналізувати, будувати статистичні дані щодо методів, які використовують хакери, а також визначати наявність будь-яких нових рішень.

Honeypot потенційно не може охопити всі питання безпеки, тому доведеться або досліджувати рівень безпеки окремої частини інфраструктури, або використовувати кілька приманок. Неможливо виключити ризик того, що зловмисник зрозуміє, що перед ним не справжній «фронт роботів», а лише фальшива пастка. Найчастіше це відбувається через неправильну або недостатньо ретельної постановки пастки, тобто в переважній більшості випадків винен людський фактор.

Так, крім суто практичного застосування Honeypot, не менш важлива інша сторона питання – дослідження. На жаль, одна з найактуальніших проблем, з якою стикаються професіонали в сфері безпеки, – це брак інформації. Хто погрожує, чому нападає, як і які засоби використовує – на ці запитання дуже часто немає однозначної відповіді. Інформовані засоби озброєні, але у світі безпеки бракує такої інформації – немає джерел даних. Як правило, фахівці з безпеки дізнавалися про зловмисників, вивчаючи інструменти, які вони використовували, і аналізуючи ознаки атаки. Коли систему було зламано, адміністратори часто знаходили інструменти, які зловмисники залишили у зламаній системі. Таким чином, багато припущень було зроблено на основі фіксованих інструментів і методів.

Пастки створені людиною, тому вони також вразливі. Крім того, вони є лише частиною «системи захисту». Покладати всі надії на приманки безглуздо. Необхідно використовувати



*This work is distributed under the terms of the Creative Commons Attribution-ShareAlike 4.0 International License (https://creativecommons.org/licenses/by-sa/4.0/).*

# ACCOUNTING AND AUDITING

комплексний підхід, в якому програмна приманка займає свою нішу. Вони повинні працювати з добре налаштованим брандмауером і бути ізольованими від мережі. Користувачі повинні обговорити, які паролі вибрати та якими вони мають бути. Системний адміністратор повинен підвищувати кваліфікацію, регулярно оновлювати систему та контролювати її стан. І керівництво не повинно економити на безпеці даних.

**References:**

[1] Milov, O., Voitko, A., Husarova, I., Opirskyy, I., Fraze-Frazenko, O., et.al., «Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems» Eastern-European Journal of Enterprise Technologies, 2019. DOI: 10.15587/1729-4061.2019.164730.

[2] ДудикевичВ.Б. Забезпечення інформаційної безпеки держави: навчальний посібник. Львів: Видавництво Національного університету «Львівська політехніка», 2017. 204с. (IBSN 978-966-941-091-7).

[3] Andrea Dominguez, «The State of Honeypots: Understanding the Use of Honey Technologies Today», SANS Reading Room, 2020.

[4] Khan, Z.A.; Abbasi, U. «Reputation Management Using Honeypots for Intrusion Detection in the Internet of Things». Electronics 2020, 9, 415.

[5] Z. Brzhevska, N. Dovzhenko, R. Kyrychok, G. Gaidur, і A. Anosov, «Інформаційні війни: проблеми, загрози та протидія»,Кібербезпека: освіта, наука, техніка, вип. 3, вип. 3, с. 88-96, бер 2019.

[6] Akiyama, M., Yagi, T., Hariu, T., & Kadobayashi, Y. (2017). Honeycirculator: distributing credential honeytoken for introspection of web-based attack cycle. International Journal of Information Security. DOI:10.1007/s10207-017-0361-5.

[7] Gandotra, V., Singhal, A., & Bedi, P. (2012). Threat-Oriented Security Framework: A Proactive Approach in Threat Management. Procedia Technology, 4, 487-494. DOI:10.1016/j.protcy.2012.05.078.

*This work is distributed under the terms of the Creative Commons Attribution-ShareAlike 4.0 International License (https://creativecommons.org/licenses/by-sa/4.0/).*