УДК 004.021
DOI: 10.31673/2409-7292.2021.032935

Коваленко С.В., Смолєв Є.С., Баргилевич О.А.

ТЕХНОЛОГІЯ АУДИТУ КІБЕРБЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ЗА МЕТОДИКОЮ ISO/IES: 27001

В роботі проаналізовано проблему забезпечення кібербезпеки корпоративних інформаційних систем та визначено мету та завдання їх захисту. Проведено аналіз існуючих технологій аудиту кібербезпеки корпоративних інформаційних систем та міжнародних стандартів, які їх описують. Досліджено методи проведення аудиту кібербезпеки за методиками міжнародних стандартів ISO/IEC 27001, ISO/IEC 19011 та COBIT. Визначено види, принципи та основні етапи проведення аудиту кібербезпеки. На основі досліджень проведених в роботі розроблено варіант технології проведення аудиту кібербезпеки корпоративних інформаційних систем за методикою міжнародних стандартів. Розроблено рекомендації щодо застосування технології варіант технології проведення аудиту кібербезпеки корпоративних інформаційних систем.

Ключові слова: Корпоративна інформаційна система, аудит кібербезпеки, аудит інформаційної безпеки, загрози корпоративним інформаційним системам, технологія аудиту кібербезпеки.

Вступ

Сьогодні аудит інформаційної безпеки корпоративних систем є одним з найбільш актуальних напрямків стратегічного і оперативного менеджменту в області безпеки корпоративних систем. Його основне завдання – об'єктивно оцінити поточний стан інформаційної безпеки компанії, а також її адекватність поставленим цілям і задачам бізнесу з метою збільшення ефективності і рентабельності економічної діяльності компанії. Тому під терміном аудит інформаційної безпеки корпоративної системи зазвичай розуміється системний процес отримання об'єктивних якісних і кількісних оцінок поточного стану інформаційної безпеки компанії відповідно до визначених критеріїв та показниками безпеки. Вважається, що результати якісно виконаного аудиту інформаційної безпеки компанії дозволяють побудувати оптимальну по ефективності і витратам корпоративну систему захисту, адекватну її поточним завданням і цілям бізнесу.

Мета роботи – розробити варіант аудиту кібербезпеки корпоративних інформаційних систем та рекомендації щодо застосування технології аудиту кібербезпеки корпоративних інформаційних систем на підприємстві.

Аналіз проблеми забезпечення кібербезпеки корпоративних інформаційних систем.

Корпоративна інформаційна система [1] – це сукупність технічних і програмних засобів підприємства, що реалізують ідеї і методи автоматизації. Головне завдання КІС – ефективне управління всіма ресурсами підприємства (матеріально-технічними, фінансовими, технологічними і інтелектуальними) для отримання максимального прибутку і задоволення матеріальних і професійних потреб усіх співробітників підприємства.

Корпоративні інформаційні системи залишаються вразливими для атак зловмисників. З кожним роком збільшується частка компаній, де вдається отримати доступ до ресурсів мережі від імені зловмисника [11]. Використання методів соціальної інженерії і експлуатація недоліків захисту мереж додатково підвищують шанси на успішне подолання мережевого периметра. Подальший розвиток атаки з сегмента внутрішньої мережі призводить до отримання повного контролю над інфраструктурою в усіх системах.

Оскільки компанії далеко не завжди своєчасно модернізують ПЗ, а методи кібератак розвиваються активно і поступально, застарілі моделі інформаційного захисту не мають можливості з ними впоратися. Не варто розраховувати на те, що цілісність і конфіденційність інформації в корпоративних системах страждає тільки від витоків, викликаних діями хакерів або інсайдерів [3]. Порушення цілісності захисту інформаційного периметра може привести і до більш серйозних ризиків. Так, все частіше зустрічаються атаки, пов'язані з втручанням в роботу систем управління і безпеки промислових об'єктів або об'єктів критично важливої інфраструктури.

Основною причиною вразливості інформаційних систем є їх складність, пов'язана з тим, що інформаційні системи складаються з безлічі взаємопов'язаних компонентів, які розробляються і виробляються окремо різними групами людей Сучасні корпоративні інформаційні системи мають велику кількість вразливостей з боку зовнішніх і внутрішніх зловмисників, а реалізація їх атак не вимагає серйозної кваліфікації. Основною проблемою є досить низький рівень захищеності мереж і рівень обізнаності користувачів в питаннях інформаційної безпеки.

Основні складові аудиту кібербезпеки корпоративних інформаційних систем

До основних складових аудиту інформаційної безпеки відносяться [4, 5]:

критерії аудиту – міжнародні, національні та галузеві стандарти, законодавча та нормативна база, внутрішні організаційно-розпорядчі документи організації, вимоги, сформульовані за результатами оцінки ризиків;

методика проведення аудиту ІБ, яка включає в себе методи аналізу захисту, що містять в своєму складі тестування щодо вторгнення (penetration testing), засоби захисту інформації аналізу конфігурації, аналіз сценаріїв проведення атак і застосування списків перевірки (checklists);

інтерв'ю зі співробітниками організації з використанням завчасно знайдених та підготованих осіб, що проходили опитування; використання спеціалізованого програмного забезпечення і шаблонів звітів аналізів ризику, документованих системою; аналіз організаційно-розпорядчих документів установи захисту інформації;

оцінку процесів забезпечення інформаційної безпеки в організації, та знань співробітників своїх посадових обов'язків та ступеня їх обізнаності в питаннях інформаційної безпеки, кваліфікації;

оцінку матеріальності фізичних механізмів безпеки.

Документи аудиту:

програма зовнішнього аудиту ІБ – план діяльності з проведення одного або декількох аудитів ІБ, запланованих на конкретний період часу і спрямованих на досягнення конкретної мети, що включає опис діяльності, необхідної для планування, проведення, контролю, аналізу та вдосконалення зовнішніх аудитів ІБ (Рис. 1);

план зовнішнього аудиту ІБ – опис діяльності та заходів якого-небудь конкретного аудиту ІБ;

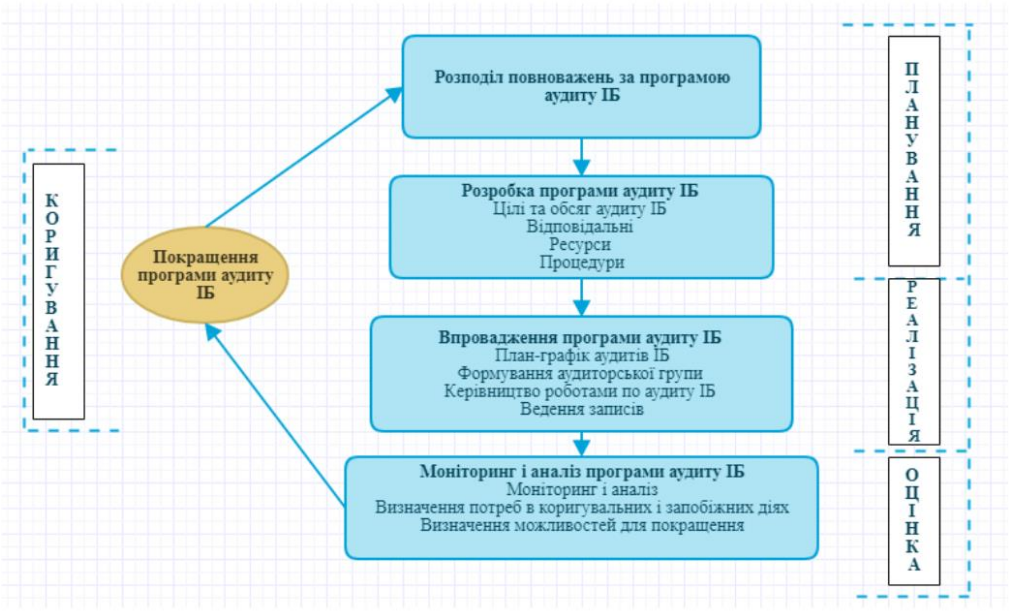

Рис. 1. Послідовність процесів керування програмою аудиту ІБ

аудиторський висновок (висновок за результатами аудиту ІБ) – якісна і/або кількісна оцінки відповідності встановленим критеріям аудиту ІБ, представлені аудиторською групою після перегляду всіх висновків аудиту ІБ відповідно до цілей аудиту ІБ.

Проведення аудиту безпеки корпоративної інформаційної системи замовника включає чотири основні етапи [6]:

проведення експрес-обстеження;

постановка завдань і уточнення складу робіт;

збір даних відповідно до детального переліку робіт, визначених в ТЗ на аудит;

аналіз зібраних даних, оцінка ризиків і підготовка звіту.

Варіант технології проведення аудиту кібербезпеки корпоративної інформаційної системи (на прикладі ДП «Укртелебачення»)

При розробці технології проведення аудиту кібербезпеки корпоративної інформаційної системи використовувалися міжнародні стандарти ISO/IEC 27001, ISO/IES 19011 та вітчизняні нормативні документи та закони: нормативні документи технічного захисту інформації НД ТЗІ 2.7-009-09 «Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу», НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу» та Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Технологію було реалізовано на прикладі аудиту корпоративних інформаційних систем державного підприємства.

Початком робіт з проведення аудиту став договір між Замовником – Державне підприємство «Укртелебачення» (далі – ДП, Підприємство) та Виконавцем – товариство з обмеженою відповідальністю (ТОВ) «Захисний захист» щодо надання послуг з проведення аудиту кібербезпеки корпоративних інформаційних систем державного підприємства «Укртелебачення». Договір між обома сторонами складено у формі поєднання типового договору на надання аудиторських послуг та програми проведення аудиту. Договір підписано керівництвом Замовника та Виконавця. Договір включає в себе аудит та обстеження наступних інформаційних систем:

офіційний веб-сайт ДП «Укртелебачення»;

телекомунікаційна система підприємства;

інформаційна система для здійснення офіційного моніторингу супутникових і цифрових кабельних телеканалів.

Аудиторською командою спільно з керіництвом ДП «Укртелебачення» було проведено вступну нараду, під час якої аудиторам було видано службові перепустки на час проведення аудиту, а також документацію попереднього аудиту та техніну документацію, яка стосується інформаційних систем Підприємства. Аудиторська команда представила план аудиту (Рис. 2), згідно якого аудит буде проводитися.

Джерелами інформації та доказами аудиту були:

офіційна веб-сторінка ДП «Укртелебачення»;

технічна документація та інструкції;

опитувач, підготовлений заздалегідь аудиторською командою, до якого увійшли інтерв'ю з працівниками та власні спостереження.

До опитувача увійшли запитання, які стосуються:

інформації, що зберігається і обробляється на підприємстві (в організації);

ресурсів, на яких зберігається інформація;

каналів, по яких переміщається інформація;

програмного забезпечення, яке використовується для обробки інформації;

основних функціональних модулів інформаційних систем, що підлягають аудиту, що входять до складу КЗЗ;

засобів фізичного захисту інформації;

користувачів та їх атрибутів доступу;

засобів забезпечення мережевої безпеки;

засобів антивірусного захисту робочих станцій, серверів, електронної пошти, доступу в Інтернет;

засобів шифрування даних;

засобів безперебійного живлення;

заходів щодо забезпечення доступу до ресурсів інформаційних систем;

юридичної та технічної документації.

ПЛАН АУДИТУ

Організація-Замовник – ДП «Укртелебаченння» Організація-Виконавець – ТОВ «Захисний Захист»			
№	Заплановані види робіт	Період виконання	Виконавець
1	Проведення вступної наради з керівництвом Замовника,	01.09.2020	Петренко, Іваненко
2	Оформлення перепусток для команди аудиторів	01.09.2020	Петренко
3	Подання запиту щодо необхідної документації	01.09.2020	Петренко
4	Вивчення запитуваної документації, обстеження організації, розподіл аудиторської команди по ключовим напрямам (структурним підрозділам)	01.09.2020	Петренко, Іваненко, Вітренко, Сидоренко
5	Аудит ІС для здійснення офіційного моніторингу супутникових і цифрових кабельних телерадіоканалів: обстеження інформаційного середовища, фізичного середовища, складу користувачів, програмного та апаратного середовища.	02.09.2020	Петренко, Іваненко
6	Аудит ІС офіційного веб-сайту ДП «Укртелебачення»: обстеження інформаційного середовища, фізичного середовища, складу користувачів, програмного та апаратного середовища.	02.09.2020	Вітренко
7	Аудит телекомунікаційної системи: обстеження інформаційного середовища, фізичного середовища, складу користувачів, програмного та апаратного середовища.	02.09.2020	Сидоренко
8	Формування загального результату аудитів всіх відділів, вироблення рекомендацій, складання звіту про аудит.	04.09.2020	Петренко, Іваненко, Вітренко, Сидоренко
9	Проведення заключної наради, представлення результату аудиту у вигляді звіту.	05.09.2020	Петренко, Іваненко, Вітренко, Сидоренко

Рис. 2. Приклад плану аудиту

Звіт за результатами проведення аудиту інформаційних систем ДП «Укртелебачення»

Метою аудиту було оцінити відповідність кібербезпеки інформаційних систем ДП «Укртелебачення» до вимог міжнародних стандартів та вітчизняних нормативних документів у сфері ТЗІ, приділяючи особливу увагу аспектам і вимогам безпеки інформаційних технологій. Проведення аудиту мало на меті довести, що внутрішній контроль над управлінням ІТ-безпекою був адекватним і ефективним.

Автоматизовані інформаційні системи Замовника призначені для автоматизації обробки інформації під час виконання функцій, передбачених законодавством.

Загальні принципи і напрямки захисту інформації в автоматизованих іфнормаційних системах, згідно з якими має бути проведено обстеження середовищ функціонування та аудит інформаційної безпеки, є досягнення належного рівня забезпечення [7,8]:

конфіденційності інформації;

цілісності інформації та автоматизованої інформаційної системи;

доступності інформації та автоматизованої інформаційної системи;

спостережності автоматизованої інформаційної системи.

Аудит інформаційної системи офіційного веб-сайту

Підприємство підтримує функціонування веб-сайту, який відображений за адресою: http://www.ukrtelecom.ua Сайт розроблений ТОВ «IT Universe». Надано договір з ТОВ «IT

Universe» з підтримки інформаційного ресурсу http://www.ukrtelecom.ua, його оновлення та внесення змін (супроводження).

Веб-сайт побудований на платформі WordPress (система управління вмістом сайту з відкритим вихідним кодом). Наповненням та оновленням інформації веб-сайту займається відділ зв'язків зі ЗМІ, громадськими організаціями та діяльності суспільного мовлення.

Функціонування веб-сайту забезпечується автоматизованою системою, за допомогою якої здійснюється:

актуалізація розміщених на веб-сайті інформаційних ресурсів;

керування доступом до інформаційних ресурсів веб-сайту.

Інформація веб-сайту за функціональним призначенням поділяється на категорії:

загальнодоступна інформація;

технологічна інформація;

службова інформація (персональні дані).

До загальнодоступної інформації відноситься публічно оголошувана інформація, користуватися якою можуть будь-які фізичні або юридичні особи (користувачі інформаційних ресурсів), що мають доступ до мережі Інтернет.

До технологічної інформації веб-сайту відноситься інформація щодо адміністрування та управління обчислювальною системою АС і засобами обробки інформації – дані про мережеві адреси, імена, персональні ідентифікатори та паролі користувачів, їхні повноваження та права тощо.

За рівнем повноважень щодо доступу до інформації, характером та складом робіт, які виконуються в процесі функціонування веб-сайту, користувачі поділяються на такі категорії:

користувачі, яким надано право доступу до загальнодоступної інформації веб-сайту;

користувачі, що є представниками телерадіоорганізацій (суб'єктами інформаційної діяльності), яким надано повноваження введення персональних даних ліцензіатів (виконується через персональний кабінет сайту шляхом введення логіну та паролю), занесення інформації про структуру власності;

користувачі, яким надано повноваження інформаційного наповнення веб-сторінок сайту (працівники відділу зв'язків зі ЗМІ, громадськими організаціями та діяльності суспільного мовлення);

розробники програмного забезпечення веб-сайту, які здійснюють розробку та впровадження нових функціональних процесів, а також супроводження вже діючого функціонального ПЗ.

технічний обслуговуючий персонал, що забезпечує повсякденну підтримку життєдіяльності фізичного середовища (електрики, технічний персонал з обслуговування приміщень будівель, ліній зв'язку тощо).

Розпорядчих документів, які б регламентували порядок ведення веб-сайту, журналу обліку занесення інформації, а також відповідальність посадових осіб за зміст, цілісність і доступність інформації та за управління системою захисту інформації у дію, на час проведення аудиту, не надано.

Аудит інформаційної системи для здійснення офіційного моніторингу супутникових і цифрових кабельних телеканалів

ДП «Укртелебачення» має змогу здійснювати нагляд за дотриманням телерадіоорганізаціями законодавства України. Для цього використовується інформаційна система для виконання офіційного моніторингу супутникових і кабельних телерадіоканалів.

Підприємство має змогу здійснювати моніторинг супутникового мовлення (українські і міжнародні канали), цифрового телебачення (DVB-T2, DVB-T), IPTV, аналогового радіомовлення.

Інформаційна система для виконання офіційного моніторингу супутникових і кабельних телерадіоканалів призначена для багатоканального прийому, запису і зберігання ефірних, кабельних та супутникових програм телебачення і радіо. За результатами моніторингу отримується систематизована інформація, необхідна для проведення

подальшого більш глибокого аналізу. Аналіз отриманих таким чином даних дозволяє комунікаційному підрозділу оцінити, наскільки контрольованим є інформаційний простір, а також оцінити ефективність інформаційної роботи.

Структурна схема інформаційної системи для виконання офіційного моніторингу супутникових і кабельних телеканалів показана на Рис. 3, радіоканалів – на Рис. 4.

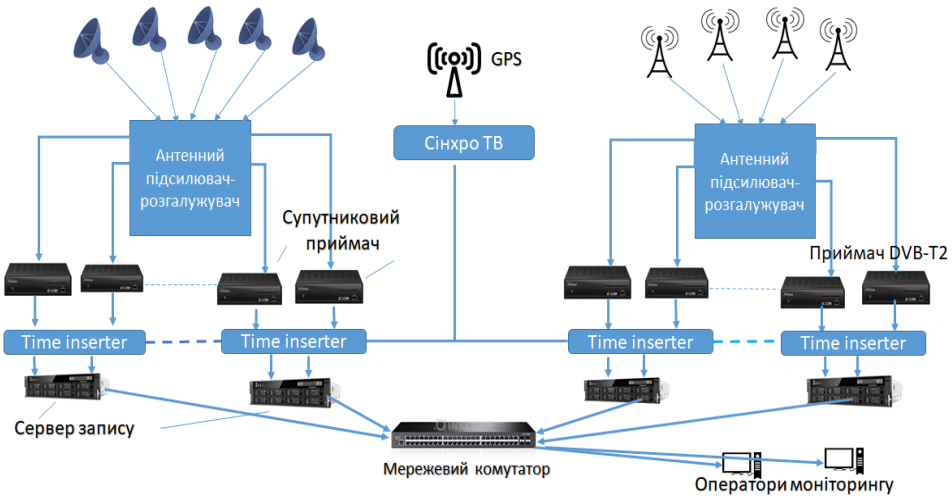

Рис. 3. Структурна схема інформаційної системи для виконання офіційного моніторингу супутникових і кабельних телеканалів

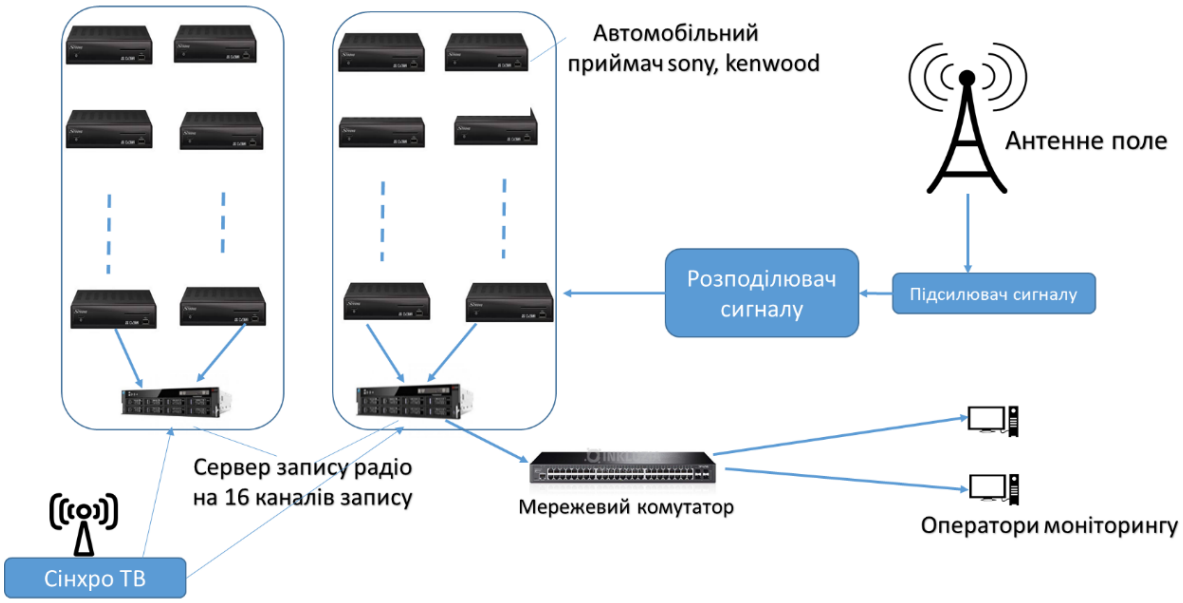

Рис. 4. Структурна схема інформаційної системи для виконання офіційного моніторингу радіоканалів

Система моніторингу складається з:

блок приймання сигналу (супутникового мовлення, цифрового телебачення (DVB-T2, DVB-T), IPTV, аналогового радіомовлення);

блок захоплення та обробки інформації;

блок зберігання інформації.

Обладнання ІС для виконання офіційного моніторингу супутникових і кабельних телерадіоканалів розміщене в приміщенні моніторингового центру (кімн. № 210). ІС

моніторингу має доступ до мережі Інтернет, необхідний для приймання IPTV та телерадіоконтенту від регіональних підрозділів. На даний час відсутнє обладнання захисту інтернет доступу (фаєрвол, маршрутизуючий комутатор) до ІС моніторингу.

ІС моніторингу (відеосервери, архівні сервери, комутатори) має систему безперебійного електроживлення, що складається з стійкових блоків безперебійного електроживлення Black-UPC.

Інформація, яка обробляється в ІС для виконання офіційного моніторингу супутникових і кабельних телерадіоканалів є відкритою, підлягає захисту в частині збереження цілісності та забезпечення її доступності.

За результатами аудиту встановлено, що ДП «Укртелебачення» з метою автоматизації виконання передбачених законодавством функцій створила певні автоматизовані інформаційні системи та здійснює обробку в цих системах інформацію, яка має підлягати захисту відповідно до законодавства.

Таким чином, забезпечення захисту інформації може бути здійснено шляхом впровадження систем захисту інформації з підтвердженою відповідністю для кожної із автоматизованих інформаційних систем Підприємства, якими буде визначено та впроваджено комплекс засобів та заходів, спроможних забезпечити захист цілісності та доступності відкритої інформації, а також конфіденційність, цілісність та доступність інформації з обмеженим доступом.

Висновок. Безпека – це не тільки стан захищеності системи, а й постійний процес його забезпечення. При побудові систем інформаційної безпеки важливе значення мають процеси контролю адекватності заходів і засобів захисту, а також виявлення вразливостей в існуючій інформаційній системі. Аудит кібербезпеки корпоративних інформаційних систем дозволяє провести такий контроль і виявити нові уразливості. Таким чином, кібербезпека вимагає більшого, ніж використання обладнання і програмного забезпечення: організації повинні бути обізнанами в цьому питанні і ставитися до безпеки як до однієї з найголовніших складових забезпечення бізнес-процесів. Без такого правильного ставлення майбутні зусилля щодо забезпечення безпеки можуть зазнати невдачі, і організації завжди будуть на крок відставати в своїй діяльності щодо забезпечення кібербезпеки.

Перелік посилань

1. Корпоративні інформаційні системи [Електронний ресурс] – Режим доступу: World Wide Web – URL: http://iablov.narod.ru/igupit/kislec.htm (Дата звернення: 20.11.2020).
2. Вразливості корпоративних інформаційних систем, 2019 – [Електронний ресурс] Режим доступу: World Wide Web – URL: https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2019/ (Дата звернення: 30.11.2020).
3. The 7 Security Vulnerabilities My Business Could Face Right Now – [Електронний ресурс] Режим доступу: World Wide Web – URL: https://www.dobson.net/7-business-it-security-vulnerabilities/ (Дата звернення: 30.11.2020).
4. ISO/IEC 27001:2013 / Information technology – Security techniques –Information security management systems – Requirements. // – 2013 – 38 p.
5. Скабцов М. Аудит безпеки інформаційних систем. / Микита Скабцов - СПб.: Издательский дом «Вильямс», 2018. - 272 с.
6. ДСТУ ISO 19011:2012 «Настанова щодо здійснення аудитів систем управління» (Guidelines for auditing management systems) – [Електронний ресурс] Режим доступу: World Wide Web – URL: https://uk.wikipedia.org/wiki/ISO_19011 (Дата звернення: 07.12.2020).
7. Коваленко С. В. Системна архітектура IoT-Fog-Cloud для систем аналізу великих даних і кібербезпеки: огляд туманних обчислень, впровадження аудиту інтернету речей // Коваленко С.В., Колісник Д.Р., Місевич К.С. – Науковий журнал «Сучасний захист інформації».– 2020 – № 3 – с. 34-38.
8. Аудит інформаційної безпеки – основа ефективного захисту підприємства // Коваленко С. В. – XII науково-практична конференція «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв'язку, автоматизації та кібербезпеки в операції Об'єднаних сил» (збірник тез і доповідей) – с.151-152.

Надійшла: 08.07.2021 Рецензент: д.т.н., професор Савченко В.А.