УДК 004. 056
DOI: 10.31673/2409-7292.2021.033641

Коваль Т.Р., Смирнов Д.С.

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КІНЦЕВИХ ТОЧОК КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ MICROSOFT DEFENDER ADVANCED THREAT PROTECTION

В роботі зроблено аналіз проблеми забезпечення кібербезпеки корпоративної інформаційної системи та визначено мета та завдання забезпечення кібербезпеки її кінцевих точок. Проведено аналіз існуючих технологій забезпечення кібербезпеки кінцевих точок корпоративної інформаційної системи. Досліджено методи та засоби забезпечення кібербезпеки кінцевих точок на базі Microsoft Defender Advanced Threat Protection. Визначено призначення, основні функції та склад платформи Microsoft Defender Advanced Threat Protection. На основі досліджень проведених в роботі запропоновано варіант технології забезпечення кібербезпеки кінцевих точок корпоративної інформаційної системи та рекомендації щодо її застосування на підприємстві.

Ключові слова: корпоративна інформаційна система, кібербезпека, кінцева точка.

Вступ

Один з векторів для проведення кібератак і розповсюдження шкідливого програмного забезпечення є кінцеві точки корпоративної інформаційної системи. Тому, захист кінцевих точок є найважливішою складовою забезпечення кібербезпеки корпоративної інформаційної системи. Сьогодні класичні підходи до захисту кінцевих точок корпоративної інформаційної системи вже не забезпечують належний рівень захищеності від сучасних кіберзагроз.

За результатами дослідження Gartner [1] ринку платформ захисту кінцевих точок компанія Microsoft визначена як компанія-лідер. Microsoft унікальна в області EPP, оскільки це єдиний постачальник, який може надати вбудовані можливості захисту кінцевих точок, тісно інтегровані з ОС. Її рішення Microsoft Defender ATP є корпоративною платформою для захисту кінцевих точок, яка призначена для запобігання, виявлення, дослідження та реагування на додаткові загрози в корпоративних мережах [2]. Вищенаведені аргументи актуалізують дослідження щодо забезпечення кібербезпеки кінцевих точок корпоративної інформаційної системи на базі рішення Microsoft Defender ATP.

Мета роботи – запропонувати варіант технології забезпечення кібербезпеки кінцевих точок корпоративної інформаційної системи та рекомендації щодо її застосування на підприємстві.

Аналіз проблеми забезпечення кібербезпеки корпоративної інформаційної системи.

Ключем до використання інформаційних систем та ІКТ для підтримки діяльності підприємств є налагодження зв'язків і бізнес-процесів як усередині організацій, так і між ними. Це вимагає створення внутрішніх організаційних бізнес-процесів і зв'язків, які полегшували б доставку необхідної інформації як між підрозділами підприємства, що відповідають за маркетинг, збут, закупівлі, фінанси, виробництво, розподіл і транспортування, так і між підприємствами - споживачами та постачальниками на всьому ланцюжку створення доданої вартості [3].

Корпоративні інформаційні системи – це технологія управління, що об'єднує бізнес-стратегію підприємства і новітні інформаційні технології. КІС є розвитком інформаційних систем для робочих груп, зазвичай орієнтовані на великі компанії. Вони можуть підтримувати вузли, що територіально розподілені або функціонують на базі корпоративної мережі [3].

В основному вони мають ієрархічну структуру з кількох рівнів. Для таких систем характерна архітектура клієнт-сервер зі спеціалізацією серверів або багаторівнева архітектура. При їх розробці можуть використовуватися ті самі сервери баз даних, що і при розробці групових інформаційних систем, проте в корпоративних інформаційних системах найбільшого поширення набули сервери Oracle, DB2, Microsoft SQL Server тощо.

З метою підвищення ефективності функціонування бізнес-процесів сучасного

підприємства застосовуються інформаційні системи BI, ERP, CRM, АСУ ТП, СЕДО тощо. Основою існування бізнес-процесів сучасного підприємства є інформаційна інфраструктура (рис. 1), яка створюється і підтримується власними силами підприємства (силами департаменту (відділу) IT) або силами компанії-аутсорсера.

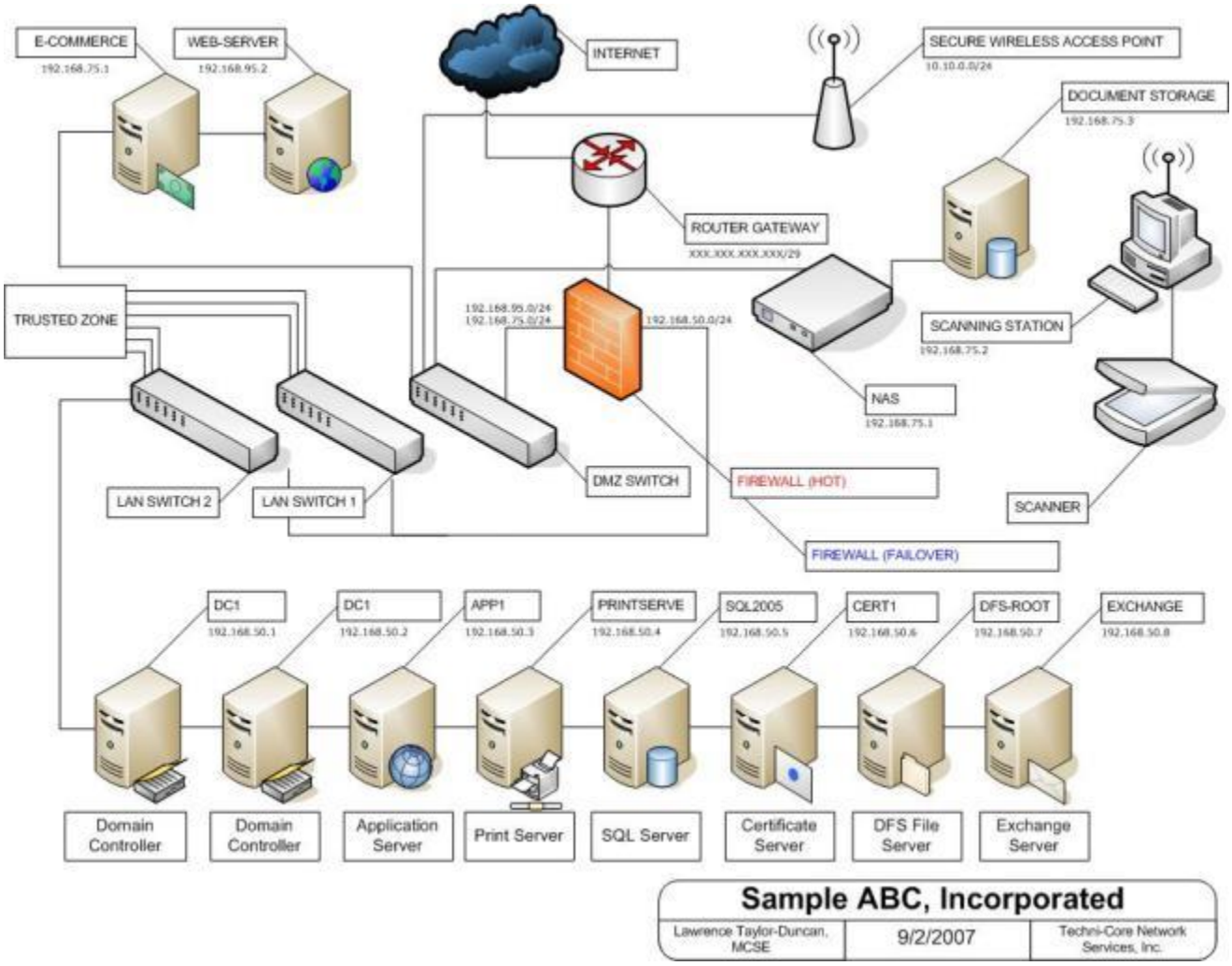

Рис. 1. Приклад основних компонентів IT-інфраструктури підприємства

Кінцеві точки корпоративних інформаційних систем часто стають метою різного роду кібератак. Дослідження показують, що третина атак було скоєно за допомогою установки шкідливого ПЗ на кінцевих точках. Необхідно підкреслити, що зловмисники постійно вдосконалюють свої методи досягнення цілей, багато з яких звичайний антивірус просто не сприймає як загрозу кібербезпеки. Прикладів сучасних векторів атак [4, 5]:

безфайлові атаки – це скріпти, які виконуються в оперативній пам’яті системи і практично не залишають слідів. Вони не заражають файли, які не зберігають свої дані на жорсткому диску і не виявляються звичайними антивірусами, так як використовують *PowerShell.exe* або *wmic.exe* для свого виконання і зберігають інформацію про набір команд в реєстрі системи;

експлойти – далеко не всі компанії своєчасно оновлюють ПЗ та операційні системи. Це може призвести до того, що хакери використовують відомі (і вже виправлені в нових версіях) уразливості, щоб увійти в систему. За цим сценарієм розвивалася ситуація з програмою-шифрувальником WannaCry, яка поширювалася через уразливість в протоколі SMB. Причому вразливість ця була відома Microsoft і усунена в свіжих патчах, які просто не були встановлені на заражених комп'ютерах;

атаки з застосуванням мобільних додатків – багато користувачі скачують програми з сторонніх джерел, щоб отримати їх безкоштовно або позбутися від набридливої реклами. Але разом із такими додатками вони можуть бути зараженими шкідливим ПЗ, троянськими модулями і додатками, які стежать за активністю процесів користувача. Причому, шанс завантажити небажане ПЗ є і при використанні офіційних магазинів Play Market і App Store, які не завжди здатні виявити його до публікації. Найчастіше хакери використовують для поширення своїх шкідливих програм популярні категорії програм, наприклад, VPN;

атаки із застосуванням соціальної інженерії – за фактом, це навіть не кіберзагроза в прямому сенсі, так як ніяких вірусів і шкідливого ПЗ в даному випадку не використовується. Зловмисники під виглядом партнерів або керівництва компанії надсилають листи по електронній пошті співробітникам з фінансових служб і вимагають перевести кошти на свої рахунки. Такі атаки спрацьовують через постійну завантаженість співробітників і керівництва цих відділів і мімікрії троянських листів під звичайне ділове листування [4].

За визначенням компанії Avast [6] управління захистом кінцевих точок є набором правил, що визначають рівень безпеки, якому має відповідати кожен пристрій, підключений до мережі підприємства. Ці правила можуть передбачати використання схваленої операційної системи (ОС), установку віртуальної приватної мережі (VPN) або використання сучасного антивірусного програмного забезпечення. Якщо підключається до мережі пристрій не має необхідного рівня захисту, може використовуватися гостьова мережа з обмеженим доступом.

Кінцевими точками є [6]:

комп'ютери та ноутбуки. Будь-який комп'ютер або ноутбук, підключений до мережі підприємства, може використовуватися для розповсюдження шкідливих програм. Обов'язково аналізуйте як корпоративні комп'ютери, так і особисті пристрої співробітників в рамках політики використання особистих пристроїв (BYOD), а також зовнішні ПК, які підключаються до офісної мережі через VPN;

мобільні телефони. Мобільні телефони вимагають особливої уваги. Небезпечно підключати особисті пристрої до офісної мережі до установки на них мобільного антивіруса з останніми оновленнями програмного забезпечення. Персонал, який використовує особисті пристрої, також повинен пройти навчання в рамках політики використання особистих пристроїв (BYOD);

офісна техніка. Під загрозою перебувають не тільки мобільні пристрої і комп'ютери. Принтери, факси, розумні і інші пристрої, які підключаються до корпоративної мережі, є потенційно вразливостями і повинні бути захищені;

сервери. Сервери – один з найбільш традиційних типів кінцевих точок. Їх особливо важливо захистити, оскільки на них зберігаються або обробляються бізнес-дані, електронна пошта і ділова документація. Ця конфіденційна інформація потребує особливого захисту.

Управління активами корпоративної інформаційної системи стає все більш складним з постійно зростаючим числом кінцевих точок, таких як ноутбуки, настільні комп'ютери, планшети і смартфони. Управління кінцевими точками стає ще складніше з різнорідними пристроями або з пристроями, які виходять за межі мережі організації. Кращий спосіб забезпечити правильне управління пристроями – використання програмного забезпечення для управління кінцевими точками.

Розроблення варіанта технології забезпечення кібербезпеки кінцевих точок корпоративної інформаційної системи на базі Microsoft Defender ATP

Зміст технології забезпечення кібербезпеки кінцевих точок корпоративної інформаційної системи на базі Microsoft Defender ATP будуть становити операції безпеки та застосовувані методи та засоби під час їх реалізації (рис. 2).

Розглянемо основні операції безпеки та застосовувані методи та засоби їх здійснення:

1. Виявлення загроз кінцевої точки і відповідь (endpoint detection and response)

Можливості виявлення кінцевих точок в Microsoft Defender ATP і реагування на них забезпечують розширене виявлення атак, яке здійснюється практично в реальному часі і

вимагає дій. Аналітики безпеки можуть ефективно розставляти пріоритети для попереджень, бачити повну картину порушення і вживати відповідних заходів для усунення загроз. При виявленні загрози в системі створюються попередження, які аналітик може досліджувати. Сповіщення з однаковими методами атаки або приписувані одному і тому ж зловмиснику об'єднуються в об'єкт, званий інцидентом. Таке агрегування попереджень спрощує для аналітиків колективне розслідування загроз і реагування на них.

Рис. 2. Технологія забезпечення кібербезпеки
кінцевих точок корпоративної інформаційної системи на базі Microsoft Defender ATP

Microsoft Defender ATP постійно збирає поведінкову «кібер-телеметрію». Сюди входить інформація про процеси, взаємодію, глибока оптика ядра і диспетчера пам'яті, дії користувача при вході в систему, зміни реєстру і файлової системи та інші. Інформація зберігається протягом шести місяців, що дозволяє аналітику повернутися в часі до початку атаки. Потім аналітик може вибирати різні точки зору і підходити до розслідування з використанням декількох векторів. Можливості реагування дозволяють швидко усувати загрози, впливаючи на порушені об'єкти.

Панель управління безпекою Microsoft Defender Security Center

На панелі управління безпекою знаходяться можливості виявлення кінцевих точок і реагування (рис. 3.). Забезпечується загальний огляд того, де були виявлені такі події, і вказує, де необхідні відповідні дії.

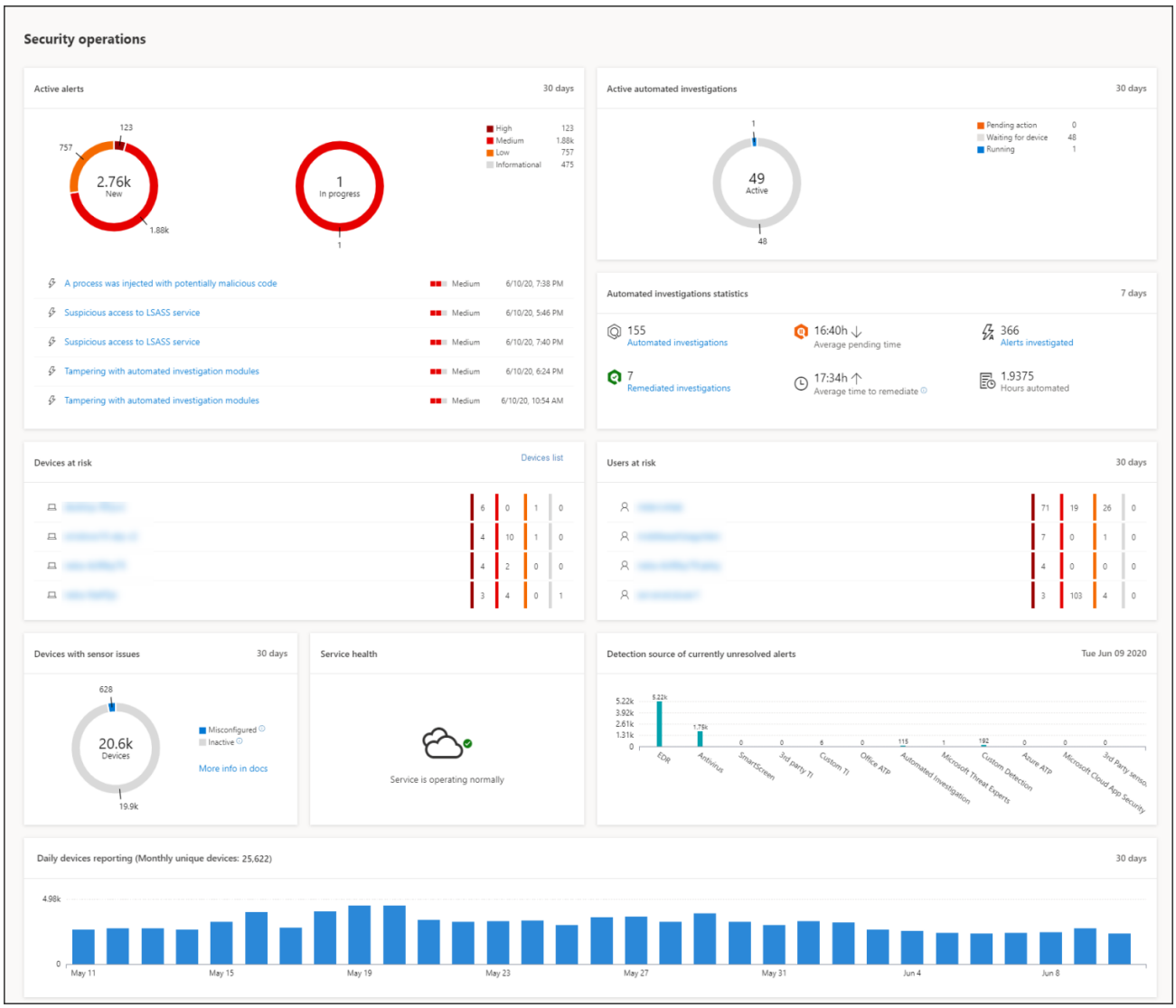

Рис. 3. Панель управління безпекою Microsoft Defender Security Center

Управління інцидентами – важлива частина кожної операції з кібербезпеки. В Microsoft Defender ATP можна управляти інцидентами, вибираючи інцидент з черги інцидентів або на панелі управління інцидентами. При виборі інциденту з черги інцидентів відкривається панель управління інцидентами, де можна відкрити сторінку інциденту для отримання докладної інформації. Можна призначати інциденти членам команди, змінювати статус і класифікацію, перейменовувати або коментувати їх, щоб відстежувати їх прогрес. Під час розслідування інцидентів, які впливають на мережу, можна зрозуміти, що вони означають, і зібрати докази для їх вирішення: деталі інцидентів, коментарі та дії щодо інцидентів, різні дані щодо попередження, пристроїв, розслідування, доказів, графіків.

Виконання дій відповіді на пристрої. Microsoft Defender ATP надає можливості швидкого реагування на виявлені атаки, ізолюючи пристрою або збираючи пакет розслідування. Після виконання дій на пристроях можна перевірити інформацію про дії в Центрі повідомлень. Дії відповіді виконуються у верхній частині сторінки певного пристрою і включають команди та функції: управління тегами; почати автоматичне розслідування; почати сеанс живої відповіді, зібрати пакет розслідування, запустити антивірусне сканування; обмежити виконання програми; ізолювати пристрій; консультація з фахівцем з питань загроз, центр подій.

Виконання дій відповіді над файлом. Microsoft Defender ATP надає можливості швидкого реагування на виявлені атаки, зупиняючи і поміщаючи файли в карантин або блокуючи файл. Після виконання дій з файлами можна перевірити відомості про дії в Центрі

дій. Дії відповіді доступні на сторінці докладного профілю файлу. Відповідні дії виконуються у верхній частині сторінки файлу і включають можливості: зупинити і помістити файл в карантин; додати індикатор; завантажити файл; проконсультуйтеся з фахівцем з питань загроз; центр подій. Також є можливість відправити файли на глибокий аналіз, щоб запустити файл в безпечній хмарній пісочниці.

Дії щодо виправлень та автоматичних розслідувань. Коли запускається автоматичне розслідування, вирок виноситься по кожному дослідженому доказу. Вердикти можуть бути: «шкідливий», «підозрілий» або «загрози не виявлено». Залежно від типу загрози, підсумкового вердикту й як налаштовані групи пристроїв організації, дії по виправленню можуть виконуватися автоматично або тільки після схвалення фахівцями групи безпеки організації.

Звіти про захист від загроз в Microsoft Defender ATP. Звіт про захист від загроз надає високорівневу інформацію про оповіщення, створених у організації. Звіт включає інформацію про тенденції, яка показує джерела виявлення, категорії, серйозність, статуси, класифікації та визначення попереджень в часі. Панель інструментів складається з двох розділів: тенденції попереджень та відомості щодо попереджень.

Висновки

В статті проведено дослідження та аналіз проблеми забезпечення кібербезпеки кінцевих точок як складової частини корпоративної інформаційної системи, встановлена сутність завдань їх захисту. Встановлено основні функції та принципи роботи програмного комплексу Microsoft Defender ATP. Microsoft Defender ATP. Microsoft Defender ATP – це уніфікована платформа для превентивного захисту, виявлення порушень, автоматичного розслідування і реагування. Microsoft Defender ATP захищає кінцеві точки від кіберзагроз, виявляє складні атаки і витоки даних, автоматизує інциденти безпеки і покращує стан безпеки. Microsoft Defender ATP реалізує технологію, вбудовану в ОС Windows 10 і хмарну службу Microsoft. Правильна реалізація технології забезпечення кібербезпеки кінцевих точок корпоративної інформаційної системи на базі рішення Microsoft Defender ATP має забезпечити ефективний захист корпоративних даних та кібербезпеку корпоративної інформаційної системи підприємства в умовах кібернетичних впливів.

Перелік посилань

1. Kim Zetter. Countdown to Zero Day. Stuxnet and the Launch of the World`s First Digital Weapon - Published in the United States by Crown Publishers, an imprint of the Crown Publishing Group, a division of Random House LLC, a Penguin Random House Company, New York. – 2016. – 319p.
2. Gabrielle Desarnaud. Cyber Attacks and Energy Infrastractures. Anticipating Risks - Etudes de l'Ifri – 2017.-60p.
3. Eric D. Knapp Industrial Network Security - 225 Wyman Street, Waltham, MA 02451, USA – 2015.- 360p.
4. APT-атаки на топливно-энергетический комплекс: обзор тактик и техник [Электронный ресурс] – URL: https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-energy-2019/
5. Почему защита АСУ ТП сегодня стала критически важной? [Электронный ресурс] – Режим доступа: World Wide Web. – URL: https://www.securitylab.ru/analytics/484730.php
6. Безопасность от кибератак и аварий в АСУ ТП [Электронный ресурс] – Режим доступа: World Wide Web. – URL: https://automation-system.ru/main/11-asutp/asu-tp/468-security-asutp.html
7. NERC Critical Infrastructure Protection (CIP), NERC CIP [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://www.nerc.com/pa/Stand/Pages/CIPStandards. aspx
8. NIST SP 800-82 [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://csrc.nist.gov/publications/detail/sp/800-82/archive/2011-06-09#:~:text=NIST%20Special%20Publication%20(SP)%20800,control%20system%20configurations%20such%20as
9. Nuclear Regulatory Commission Regulation 5.71 [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://www.nrc.gov/docs/ML0903/ML090340159.pdf
10. Довгуша І.М., Кітура О.В. Безпека автоматизованих систем управління технологічними процесами / Довгуша І.М., Кітура О.В. // Актуальні проблеми кібербезпки: всеукраїнська наукова конференція, тези доп. – К., 2020. – С.91-92.

Надійшла: 13.07.2021 Рецензент: д.т.н., професор Вишнівський В.В.