ICST

Information Control Systems and Technologies

Монография

Информационные системы и технологии. Состояние и перспективы

Информацйионные системы управления

Интеллектуальные системы и анализ данных

Моделирование и разработка программ

ICST-2021

ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
«ОДЕССКАЯ ПОЛИТЕХНИКА»

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ. СОСТОЯНИЕ И ПЕРСПЕКТИВЫ

МОНОГРАФИЯ

Под науч. ред. проф. В. Вычужанина

ОДЕССА 2021

УДК 681.518.54

И74

Рекомендовано в печать ученым советом
Государственного университета «Одесская политехника»
(протокол № 2 от 21.09.2021 г.)

Рецензенты:

ГОВОРУЩЕНКО Татьяна, доктор технических наук, профессор, Хмельницкий национальный университет (Украина);

ПАКСТАС Альгирдас, доктор технических наук, профессор, институт математики и информатики (Великобритания);

ЦАРЕВ Александр, доктор технических наук, профессор, Западно-Поморский технологический университет (Польша).

Авторский коллектив:

Бармак О., Божаткин С., Бородкина І., Бородкин Г., Волошин В., Вороной С., Вычужанин В., Вычужанин А., Гохман Р., Гусєва-Божаткина В., Джорджевич О., Дрозд А., Дрозд М., Жуковская Н., Журавська И., Защелкин К., Егошина А., Ивановская О., Илькив И., Ковалев И., Косенко С., Крак Ю., Кудря В., Лисецкий Ю., Лисицкая И., Лисицкий К., Литвиненко В., Мазурець О., Манзюк Е., Мартынюк А., Мироненко Д.,, Отрадская Т., Пасюк Б., Петров И., Петросян А., Петросян Р., Пилькевич И., Пихнастий О., Присяжнюк Е., Рудниченко Н., Сафоник А., Ситников В., Стрельцов О., Ступень П., Ухина А., Фарионова Т., Федосова И., Чупринка В., Чупринка Н., Шибаева Н., Шибаев Д.,

И74 Информационные системы и технологии. Состояние и перспективы: монография / Бармак О., Божаткин С..и др.; под науч. ред. проф. В. Вычужанина. – Одеса: НУ «ОМА», 2021. – 206 с.

На укр., рус. и англ. языках.

ISBN 978-617-7857-11-1

В монографии отражены результаты научных исследований в области информацйионных, интеллектуальных систем и анализа данных, моделирования и разработки программ. Материалы монографии будут полезными для аспирантов, магистрантов, преподавателей высших учебных заведений, специализирующихся в области IT-технологий.

УДК 681.518.54

ISBN 978-617-7857-11-1

ОГЛАВЛЕНИЕ

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ. СОСТОЯНИЕ И ПЕРСПЕКТИВЫ

УДК: 004.7

МОДЕЛЬ ЗАГРОЗ КІБЕРБЕЗПЕКИ БЕЗДРОТОВОЇ СИСТЕМИ ОПОВІЩЕННЯ СПІВРОБІТНИКІВ ПІДПРИЄМСТВА

Гусєва-Божаткіна В.А., Божаткін С.М., к.т.н. Фаріонова Т.А., д.т.н. Журавська І.М., Пасюк Б.Б.

Анотація. Сучасні системи оповіщення розроблені з використанням інноваційних технологій для підвищення якості життя та безпеки людей. В даний час практично у всіх установах є щонайменше одна бездротова мережа. Типові моделі загроз кібербезпеки для бездротових систем оповіщення занадто малоінформативні та потребують доопрацювання на кожному рівні. Було проведено аналіз існуючих моделей загроз кібербезпеки для безпровідної системи оповіщення. В ході роботи було також виконано аналіз існуючих моделей загроз кібербезпеки бездротових систем оповіщення та досліджено ключові компоненти моделей загроз кібербезпеки. Запропоновану модель загроз кібербезпеки для бездротової системи оповіщення побудовано на основі моделі «Ланцюжок кібер-вбивства», що дозволило підвищити рівень точності при визначенні превентивних дій на кожному рівні моделі загроз кібербезпеки.

Ключові слова: Системи оповіщення, бездротові системи оповіщення, загальнодоступні бездротові точки доступу, несанкціонований доступ до даних, надзвичайні ситуації, кібербезпека, модель загроз кібербезпеки, «Ланцюжок кібер-вбивства».

Вступ

Одним з основних способів захисту населення від надзвичайних ситуацій є своєчасне повідомлення про небезпеку, а також інформування про порядок та правила поведінки в контексті надзвичайної ситуації. Сьогодні відбувається перегляд вимог щодо сучасних систем оповіщення, які були створені з метою виконання завдань цивільного захисту за допомогою автоматизованих систем централізованого оповіщення, мереж зв'язку, радіомовлення. Відбувається перехід до нових структур організації таких систем з урахуванням сучасного стану технічних засобів зв'язку, захисту від несанкціонованого доступу та розповсюдження шкідливого програмного забезпечення [1]. Гучномовець, звичайно, привертає увагу і може надавати необхідну інформацію для подальших дій, але водночас наявність на екрані смартфона, планшета, ноутбука чіткої схеми, плану евакуації та інструкцій щодо дій співробітників підприємства (особливо з вадами слуху) – скоротить час для прийняття рішень щодо реагування на надзвичайні ситуації або визначення заходів щодо їх пом'якшення. Наразі, фактично кожен громадянин має мобільний пристрій (смартфон). Майже у всіх закладах (організаціях) є доступ до бездротової мережі. Отже система, яка, підключившись до відповідного сервера підмережі, інформує про небезпеку, що виникла, та дії, які співробітники повинні вжити, щоб уникнути ушкоджень, є надважливою на сьогодні.

При побудові бездротової систем сповіщень необхідно враховувати безпеку точок доступу та системних серверів від можливості зламу зловмисниками, запобігання DDoS-атак тощо [1]. Слід зазначити, що одним із актуальних напрямів, який активно розвивається у сфері інформаційної безпеки є виявлення кібератак і запобігання вторгнень до інформаційних систем з боку неавторизованої сторони. Також слід наголосити, що мережеві атаки з кожним роком стають все досконалішими, глобальнішими та частішими.

Ідея створення бездротової системи оповіщення досить приваблива для впровадження, але існує загроза різного роду мережевих атак. Для визначення рівня кібербезпеки такої системи пропонується розробити удосконалену модель загроз на основі моделі «Ланцюжок кібер-вбивства» та вивчити різницю (ключові критичні відмінності) за допомогою типової моделі загроз [2]. Швидке прискорення розвитку комп'ютерних технологій тягне за собою більш складні та різноманітні атаки, які важко описати наявними типовими моделями загроз. Тому існує потреба в розробці більш точної та детальної моделі з експертними оцінками для кожного етапу розробленої моделі загроз для мережі, що перевіряється на можливість зламу. При складанні моделі загроз визначається рівень початкової безпеки та джерела загроз. Потім висвітлюються фактичні загрози і виключаються непотрібні (теоретичні або непідтверджені) - ті, які не завдають шкоди системі. Не виключені загрози включаються до моделі з описом.

Найефективнішим інструментом опису є моделі зловмисника та загроз системі, які одночасно забезпечують уявлення щодо двох ключових питань: визначення системного суб'єкта, який може завдати шкоди інформаційній системі та векторів мережевої атаки. Отже, для початку, визначимо об'єкт, предмет та актуальність роботи. Система безпеки систем оповіщення базується на моделі загроз та моделі зловмисника. Наявність загрози не означає неминучого можливого витоку інформації. Це говорить лише про те, що зловмисники мають теоретичну можливість несанкціонованого доступу до персональних даних підприємства. Об'єкт дослідження: методи удосконалення типової моделі загроз за допомогою моделі «Ланцюжок кібер-вбивства». Предметом дослідження є властивості моделі порушника кібербезпеки інформаційної системи після реалізації ключових пунктів моделі «Ланцюжок кібер-вбивства».

Актуальність дослідження полягає у розробці більш детальних та ефективних моделей загроз бездротових систем оповіщення.

Для створення такої моделі необхідно проаналізувати дані, отримані під час інформаційного аудиту підприємства. Це допоможе виявити слабкі сторони бездротової системи оповіщення; зрозуміти, що може їй загрожувати; джерела загроз і якими засобами їх можна буде нейтралізувати або запобігти виявленню заздалегідь [3]. Тому метою роботи є проектування та розробка удосконаленої моделі загроз кібербезпеки бездротової системи оповіщення співробітників підприємства.

Постановка проблеми

Автори [4,5] у своїх працях представляють моделі загроз у вигляді переліку можливих вразливостей IP-мереж та мережевих компонентів (типові атаки: DoS, DDoS, заміна заголовків пакетів, тощо), але такі об'єкти як система оповіщення,

підлягають набагато ретельнішому огляду і розроблена модель має бути певною мірою більш детальною. Високий рівень безпеки бездротової мережі є перевою її використання та дозволяє отримати доступ до глобальної мережі Інтернет не лише зі свого комп'ютера чи ноутбука, а й з портативних пристроїв, які оптимізують робочий процес співробітників підприємства за рахунок сучасної *мережевої інфраструктури: відеоконференції, IP-телефонії, електронної пошти,* управління серверами та мережевими пристроями. При розробці моделі загроз визначається рівень початкової безпеки бездротової системи оповіщення, що тестується. Це глобальний параметр, який визначається один раз і не змінюється *залежно від типу загрози. Потім висвітлюються фактичні загрози і виключаються* несуттєві, тобто ті, які не можуть завдати шкоди системі. Не включені загрози додаються до моделі з їх описом. Для захисту від несанкціонованого доступу до вузла оповіщення та збереження бази даних підключених абонентів рекомендується використовувати протокол *RADIUS, який є найпоширенішим* протоколом AAA (автентифікація, авторизація та облік), *який розроблено для* передачі інформації між прикладними програмами [1]. Модель AAA призначена для керування доступом до комп'ютерних ресурсів, проведення певних політик, аналізу використання ресурсів і надання інформації. Всі ці процедури вважаються життєво важливими для ефективного і раціонального керування мережею і забезпечення її безпеки. Незважаючи на те, що протокол RADIUS було розроблено ще до створення моделі AAA, він все одно може слугувати прикладом її реалізації. Слід зазначити, що цю модель можна застосувати до роботи *працівників з внутрішньою (локальною) мережею підприємства,* яким надається доступ до бездротової мережі через сервер RADIUS (сервер авторизації) та сервер сповіщень (основний сервер). Це означає, що з'єднання між AP (точкою доступу) та Користувачем (співробітником) повинно мати зашифроване з'єднання.

Протокол RADIUS досить часто використовують в публічних бездротових мережах. Його можна вважати за протокол безпеки, в якому для автентифікації користувачів використовується клієнт-серверна модель. Він реалізується у вигляді серії запитів та відповідей, які клієнт передає від сервера доступу до мережі кінцевому користувачу. Даний протокол існує як джерело програмної автентифікації, авторизації та обліку дій користувачів в такій мережі, яким необхідно надати контрольований доступ до різних частин мережі.

Варто зазначити, що обраний тип з'єднання для підключення клієнтів обрано недарма. Під час автентифікації користувача, обмін даними між клієнтом та сервером шифрується за допомогою розподільного ключа, який ніколи не передається мережею у відкритому вигляді. Паролі користувачів клієнт передає RADIUS-серверу також в зашифрованому вигляді, щоб виключити можливість визначення ключа за допомогою «прослуховування» трафіку (сніфінгу).

Проаналізуємо, які типові загрози кібербезпеки існують для таких систем. Існує багато специфічних видів атак на бездротові мережі: злам паролів *WPA/WPA2 (handshake catching); атака* WEP; злам WPS Pin; заміна справжньої точки доступу на *підроблену; атака на точку доступу* бездротової мережі з глобальної та локальної мереж; атаки відмови в обслуговуванн; атаки на певні послуги та функції маршрутизаторів; кейлогери на мобільних пристроях; викрадення; соціальна інженерія.

Моделлю, яку зазвичай використовують для виокремлення етапів проведення кібератак є модель «Ланцюжок кібер-вбивства» [2]. Ця модель визначає типовий порядок дій зловмисника для досягнення поставлених цілей. Так, для досягнення успіху зловмисник повинен пройти усі вісім етапів (рис. 1). Технічний характер ключових етапів атаки включає розвідку, визначення інструментів для атаки, доставку, експлуатацію, встановлення, командування та управління та дії у разі успішного проникнення до системи.

Рис. 1. Етапи проведення кібератак

Кожен етап пов'язаний з певним видом діяльності при здійсненні кібератаки зловмисником, незалежно від того, чи це внутрішня чи зовнішня атака:

• Розвідка

Етап спостереження: зловмисник зазвичай оцінює ситуацію ззовні, щоб визначити цілі (прогалини в безпеці) та методи атаки;

• Вторгнення до системи

Виходячи з того, що зловмисники виявили на етапі розвідки, вони можуть використати шкідливе програмне забезпечення або вразливості безпеки (наприклад, відкриті назовні мережеві порти);

• Експлуатація вразливостей

Акт використання вразливих місць та доставки шкідливого коду в систему для закріплення в ній;

• Ескалація привілеїв

Зловмисникам часто потрібні додаткові привілеї в системі, щоб отримати доступ до більшої кількості даних та дозволів до надважливих і системних файлів: для цього їм потрібно використати або самостійно написати експлоїт для підняття привілеїв до рівня адміністратора або суперадміністратора;

• Інсталяція

Після того, як зловминсик успішно отримує доступ до системи, він може отримати зв'язок з іншими системами в локальній мережі та скомпрометувати облікові записи, щоб отримати більше важелів впливу: будь то більші системні дозволи, більше даних або привілейований доступ до інших систем;

• Анти-форензика

Щоб успішно здійснити кібератаку, зловмисники повинні прикрити свої сліди, і на цьому етапі вони часто залишають хибні сліди, компрометують дані та очищають системні журнали і файли логів, щоб заплутати та/або уповільнити роботу будь -якої групи експертів з форензики;

• Відмова в обслуговуванні

Порушення звичного доступу для користувачів та систем, щоб припинити

моніторинг, відстеження або блокування атаки;

• Ексфільтрація

Етап вилучення: вилучення даних із скомпрометованої системи.

Як правило, методи виявлення атак розділяють на методи виявлення зловживань і аномалій. Зловживання засновані на використанні існуючих недоліків бездротової системи оповіщення. Основною відмінністю між аномалією і зловживанням є те, що аномалія – це процес, який виникає перед можливим вторгненням в систему або вказує на наявність вже існуючої атаки (відхилення від нормального стану системи, незвичайна активність в ній, що може свідчити про певні атакуючі дії). Враховуючи вищесказане, визначимо модель порушника інформаційної безпеки. Типова модель порушника [6] кібербезпеки та модель загроз для бездротової системи сповіщення на підприємстві за критеріями: конфіденційність, цілісність та доступність [7] відображають лише загальну інформацію та практично не несуть жодного смислового навантаження для спеціаліста з кібербезпеки або системного адміністратора (рис. 2). Варто додати, що широке використання сучасних засобів захисту від кібератак не гарантує безпеки на належному рівні, оскільки останнім часом: зростають атаки, спрямовані на корпоративні системи, публічні, конфіденційні та державні інформаційні ресурси; кібератаки, постійно модифікуються, удосконалюються і стають більш регулярними; виявлення кібератак класичними засобами захисту не завжди є ефективним; частішають випадки здійснення складних атак на системи.

Це також пов'язане з інтенсивним розвитком програмно-апаратних засобів і глобалізації інформаційних мереж та їх повсякденного використання у всіх сферах діяльності суспільства.

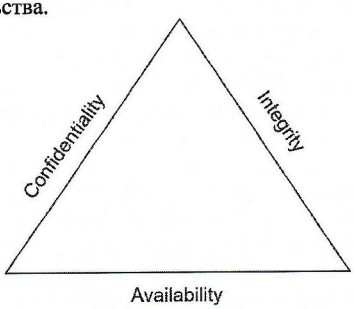

Рис. 2. Модель загроз для бездротової системи сповіщення на підприємстві

«Тріада інформаційної безпеки» була створена для забезпечення базового стандарту для оцінки та реалізації інформаційної безпеки незалежно від основної системи та/або організації. Три основні цілі мають чіткі вимоги та процеси всередині однієї. Конфіденційність: Забезпечує доступ до даних або інформаційної системи лише уповноваженою особою. Ідентифікатори користувача та паролі, списки контролю доступу та безпека, заснована на політиці, - це деякі методи, завдяки яким досягається конфіденційність.

Цілісність: Цілісність гарантує, що даним або інформаційній системі можна довіряти. Забезпечує редагування лише уповноваженими особами та залишається

в початковому стані, коли знаходиться в «спокої». Алгоритми шифрування даних та хешування є ключовими процесами забезпечення цілісності.

Доступність: Дані та інформаційні системи доступні за потреби. Обслуговування обладнання, виправлення/оновлення програмного забезпечення та оптимізація мережі забезпечують доступність [9]. Ці моделі керуються відображенням загальних рекомендацій, які слід враховувати, але вони жодним чином не вказують на реальні можливі вектори атак можливих порушників і на якому етапі вони можуть почати використовувати вразливості системи. Тому виникла потреба у побудові удосконаленої моделі загроз, яка з підвищеною достовірністю надаватиме дані про можливі вразливості інформаційних систем на прикладі бездротової системи оповіщення.

Основні результати

Дослідження проведено під час розробки бездротової системи оповіщення для співробітників підприємства при виникненні надзвичайних ситуацій. Першим кроком було проведення моделювання загроз для визначеняя потенційних загроз та вразливостей безпеки. Далі визначається серйозність кожної з них та оцінюється пріоритетність методів превентивності можливості атак для захисту IT-ресурсів [1]. В результаті проведеного дослідження було визначено критерії, за якими буде побудовано модель загроз кібербезпеки бездротової системи оповіщення:

- етап моделі «Ланцюжок кібер-вбивства»;
- опис загрози на поточному етапі;
- типові інструменти зловмисника на даному етапі;
- точки входу зловмисника на даному етапі (можливі прогалини в безпеці);
- актор небезпеки (особа чи відділ, за допомого яких можна увійти в інформаційну систему) на даному етапі;
- механізм реалізації шкідливих дій на даному етапі;
- рівень небезпеки зловмисника на даному етапі;
- сучасний рівень реалізації превентивних дій в системі або організації на етапі моделі «Ланцюжок кібер-вбивства» (екпертна оцінка).

Враховуючи визначені критерії для побудови удосконаленої моделі загроз кібербезпеки для бездротової системи оповіщення співробітників було отримано модель загроз, яка використовує етапи перевірки з моделі «Ланцюжок кібер-вбивства» та критерії загроз кібербезпеки бездротової системи оповіщення, що визначені вище під час екпериментy.Враховуючи складність існуючої проблеми, її новизну та необхідність, недостатньої кількості інформації, неможливості математичної формалізації процесу вирішення, доводиться звертатися до рекомендацій компетентних фахівців, які знають проблему - до експертів. Їх вирішення проблеми, аргументація, формування кількісних оцінок, обробка даних формальними методами називаються методом експертних оцінок.

Експертна оцінка передбачає створення колективної думки, яка має більші можливості порівняно з можливостями однієї особи (навіть експерта в даній галузі) [10]. Джерелом колективної думки є пошук слабких асоціацій та припущень на основі досвіду окремого фахівця. Експертний підхід має набагато більший потенціал для вирішення проблем, які неможливо вирішити звичайним

аналітичним способом [11].

Висновки

В результаті дослідження були отримані дані, які дозволяють зробити висновок про використання моделі «Ланцюжок кібер-вбивств», як базової для удосконаленої моделі загроз. Рекомендовано запровадити експертні оцінки для визначення ступеня безпеки бездротової системи оповіщення на кожному етапі розроблення моделі, що потребує подальшого дослідження вдосконалення розширеної моделі загроз кібербезпеки. Апробацію було проведено на невеликому сегменті мережі для збору даних про безпеку системи оповіщення співробітників та виявлення можливих прогалин у її безпеці. Запропонована модель може бути використана при проведенні аудитів кібербезпеки локальної мережі організації або відділами кібербезпеки для поглибленого вивчення *бездротових систем оповіщення та підвищення їх стійкості до мережевих атак* зловмисників.

Література

[1] Sergii Bozhatkin, Victoryia Guseva-Bozhatkina O.Patlaichuk, H.Serbulov Employees notification systems in the event of emergency situations through public wireless access points [Text] / Sergii Bozhatkin, Victoryia Guseva-Bozhatkina O.Patlaichuk, H.Serbulov // International Competition of Student Scientific Works: BLACK SEA SCIENCE 2020 (Odessa, ONAFT 2020) – from 259-270

[2] What is Cyber-Kill Chain and why it should be taken into account in the defense strategy. URL: https://habr.com/ru/company/panda/blog/327488/

[3] Information threat model. URL: https://it.wikireading.uk/1000009748

[4] O.Y. Matov, V.S. Vasylenko "Model of threats in distributed networks". URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/7538/09-Matov.pdf?sequence=1

[5] O.O. Ilyin, S.O. Serykh, V.V. Vyshnivsky "Analysis of the vulnerability of information resources of higher education and classification of information security threats". URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/1414

[6] Violators in information security. The model of the violator. URL: https://works.doklad.ru/view/0uSxB0lhk8I/2.html

[7] CIA Triad. URL: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

[8] Josh Fruhlinger. "Threat modeling explained: A process for anticipating cyber attacks". URL: https://www.csoonline.com/article/3537370/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html

[9] Що таке CIA тріада інформаційної безпеки? URL: https://uk.theastrologypage.com/cia-triad-information-security

[10] Mariëlle Zondervan-Zwijnenburg, Wenneke van de Schoot-Hubeek, Kimberley Lek, Herbert Hoijtink, and Rens van de Schoot. "Application and Evaluation of an Expert Judgment Elicitation Procedure for Correlations". URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5282462/

[11] Expert Judgement in Cost Estimating: Modelling the Reasoning Process https://journals.sagepub.com/doi/abs/10.1177/1063293X0100900404

MODEL OF THREAT OF CYBER SECURITY OF THE WIRELESS WARNING SYSTEM OF ENTERPRISE EMPLOYEES

Guseva-Bozhatkina V., Bozhatkin S., Ph.D. Farionova T., Dr.Sci. Zhuravska I., Pasiuk B.

Abstract. Modern warning systems are designed by using innovative technologies that improves the quality of life and safety of people. Currently, almost all organizations have at least one wireless network. Typical cybersecurity threat models for wireless alert systems are too uninformative, so they need to be refined at every level.

An analysis of existing models of cybersecurity threats of the wireless alert system was conducted. The work also analyzed existing models of cybersecurity threats to wireless systems and explored key components of cybersecurity threat models. A cybersecurity threat model for a warning system based on the Cyber Kill Chain model that has been proposed, which will increase the level of accuracy in determining preventive actions at each level of the cybersecurity threat model.

Keywords: Alerts System, Wireless Alert System, Public Wireless APs, Unauthorized Data Access, Emergencies, Cybersecurity, Model of Cybersecurity Threats, Cyber Kill Chain.

МОДЕЛЬ УГРОЗ КИБЕРБЕЗОПАСНОСТИ БЕСПРОВОДНОЙ СИСТЕМЫ ОПОВЕЩЕНИЯ СОТРУДНИКОВ ПРЕДПРИЯТИЯ

Гусева-Божаткина В. А., Божаткин С. М., к.т.н. Фарионова Т. А., д.т.н. Журавская И. М., Пасюк Б. Б.

Аннотация. Современные системы оповещения разработаны с использованием инновационных технологий для повышения качества жизни и безопасности людей. В настоящее время практически во всех учреждениях есть, по меньшей мере одна беспроводная сеть. Типичные модели угроз кибербезопасности для беспроводных систем оповещения слишком малоинформативны и нуждаются в доработке на каждом уровне.

Был проведен анализ существующих моделей угроз кибербезопасности для беспроводной системы оповещения. В ходе работы был также выполнен анализ существующих моделей угроз кибербезопасности беспроводных систем оповещения и исследованы ключевые компоненты моделей угроз кибербезопасности. Предложенную модель угроз кибербезопасности для беспроводной системы оповещения построено на основе модели «Цепочка кибер-убийства», что позволило повысить уровень точности при определении превентивных действий на каждом уровне модели угроз кибербезопасности.

Ключевые слова: Системы оповещения, беспроводные системы оповещения, общедоступные беспроводные точки доступа, несанкционированный доступ к данным, чрезвычайные ситуации, кибербезопасность, модель угроз кибербезопасности, «Цепочка кибер-убийства».

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ. СОСТОЯНИЕ И ПЕРСПЕКТИВЫ

ИНФОРМАЦИЯ ОБ АВТОРАХ

БАРМАК Александр Владимирович, доктор технических наук, профессор, [illegible] национальный университет, *alexander.barmak@gmail.com,* [illegible] 0000-0003-0739-9678

БОЖАТКИН Сергей Михайлович, Национальный университет кораблестроения им. [illegible] Макарова, *sergii.bozhatkin@nuos.edu.ua,* orcid.org/ 0000-0002-4653-8880

БОРОДКИН Георгий Алексеевич, Национальный университет биоресурсов и [illegible] использования, *george.borodkin@gmail.com,* orcid.org/ 0000-0002-6488-6512

БОРОДКІНА Ірина Лаврентіївна, кандидат технических наук, доцент, Киевский [illegible] национальный университет культуры и искусств, *borir@ukr.net,* [illegible] 0000-0003-3667-3728

ВОЛОШИН Вячеслав Степанович, доктор технических наук, профессор, ректор, [illegible] государственный университ, ул. Университетская, 7, Мариуполь, 87500, [illegible] *752@outlook.com,* orcid.org/0000-0002-8423-2663

ВОРОНОЙ Сергей Михайлович, кандидат технических наук, доцент, Одесский [illegible] национальный политехнический университет, проспект Шевченко, 1, Одесса, 65044, [illegible] *s.m@op.edu.ua*, orcid.org/0000-0001-8564-1103

ВЫЧУЖАНИН Владимир Викторович, доктор технических наук, профессор, [illegible] заведующий кафедрой информационных технологий, Одесский национальный [illegible] технический университет, проспект Шевченко, 1, Одесса, 65044, *vint532@yandex.ua,* [illegible] 0000-0002-6302-1832

ГУСЕВА-БОЖАТКИНА Виктория Анатолеевна, Национальный университет [illegible] кораблестроения им. Адмирала Макарова, *GusevaBozh@meta.ua,* [illegible] 0000-0002-1117-3391

ДРОЗД Александр Валентинович, доктор технических наук, профессор, Одесский [illegible] национальный политехнический университет, проспект Шевченко, 1, Одеса, 65044, [illegible] *ukr.net*, orcid.org/0000-0003-2191-6758

ДРОЗД Мирослав Александрович, Одесский национальный политехнический [illegible] университет, проспект Шевченко, 1, Одесса, 65044, *myroslav.drozd@opu.ua,* [illegible] 0000-0003-0770-6295

ЕГОШИНА Анна Анатольевна, кандидат технических наук, доцент, Одесский [illegible] национальный политехнический университет, проспект Шевченко, 1, Одесса, 65044, [illegible] *na.h.a@op.edu.ua*, orcid.org/ 0000-0002-2381-1231

ЖУРАВСКАЯ Ирина Николаевна, доктор технических наук, профессор, [illegible] Николаевский национальный университет, Николаев, *iryna.zhuravska@chmnu.edu.ua,* [illegible] 0000-0002-8102-9854

ЗАЩЕЛКИН Константин Вячеславович, доктор технических наук, профессор, [illegible] национальный политехнический университет, проспект Шевченко, 1, Одесса, [illegible] *const-z@te.net.ua,* orcid.org/ 0000-0003-0427-9005

ИВАНОВСКАЯ Ольга Владимировна. кандидат технических наук, доцент, [illegible] национальный аэрокосмический університет «Харьковский авиационный інститут», [illegible] *ska@khai.edu,* orcid.org/ 0000-0003-1530-259X

КОСЕНКО Сергей Ильич, кандидат физико-математических наук, доцент, Одесский [illegible] национальный политехнический университет, проспект Шевченко, 1,Одесса, 65044, [illegible] *218@gmail.com,* orcid.org/ 0000-0002-7082-5644

КРАК Юрий Васильевич, доктор физико-математических наук, профессор, Институт [illegible] кибернетики им. В. М. Глушкова, Киевский национальный университет им. Т. Г. Шевченко, [illegible] *@gmail.com,* orcid.org/0000-0002-8043-0785

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ. СОСТОЯНИЕ И ПЕРСПЕКТИВЫ

КУДРЯ Владимир Нринорьевич, доктор технических наук, профессор, Одесский национальный политехнический университет, проспект Шевченко, 1, Одесса, 65044, kvg@opu.ua, orcid.org/0000-0001-6839-8287

ЛИСЕЦКИЙ Юрий Михайлович, доктор технических наук, профессор, генеральный директор ДП «ЭС ЭНД ТИ УКРАИНА», *Yurii.Lysetskyi@snt.ua,* orcid.org/ 0000-0002-5080-1856

ЛИСИЦКАЯ Ирина Викторовна, доктор технических наук, профессор, Государственный университет имени В.Н. Каразина; Харьков, *lisitskaiv@ukr.net*

МАЗУРЕЦЬ Александр Викторович, кандидат технических наук, доцент, Хмельницкий национальный университет, *exe.chong@gmail.com, o*rcid.org/0000-0002-8900-0650

МАНЗЮК Эдуард Андреевич. кандидат технических наук, доцент, Хмельницкий национальный университет, *eduard.em.km@gmail.com,* rcid.org/ 0000-0002-7310-2126

МАРТЫНЮК Александр Николаевич, кандидат технических наук, доцент, Одесский национальный политехнический университет, проспект Шевченка, 1, Одеса, 65044, *anmartynyuk@ukr.net,* orcid.org/ 0000-0003-1461-2000

МИРОНЕНКО Дмитрий Сершеевич, кандидат технических наук, доцент, Приазовский государственный университ, ул. Университетская, 7, Мариуполь, 87500, *mironenko_ds@ukr.net,* orcid.org/ 0000-0001-6022-7395

ОТРАДСКАЯ Татьяна Васильевна, кандидат технических наук, директор частного учебного заведения «Одесский колледж компьютерных технологий «Сервер», Багрицкого, 12б, Одеса, 65026, *tv_61@ukr.net*, orcid.org/0000-0002-5808-5647

ПЕТРОВ Игорь Михайлович, кандидат технических наук, профессор, Национальный университет «Одесская морская академия», ул. Дидрихсона, 8, Одесса, 65029, *firmness@list.ru*, orcid.org/0000-0002-8740-6198

ПЕТРОСЯН А.Р., Государственный университет "Житомирская Политехника", *xckaytz@gmail.com,* orcid.org/ 0000-0003-0960-8461

ПЕТРОСЯН Р.В., Государственный университет "Житомирская Политехника", *e_rvs@ukr.net,* orcid.org/ 0000-0002-0388-8821

ПИГНАСТЫЙ Олег Михайлович, доктор технических наук профессор, Национальный технический университет «Харьковский политехнический институт», ул. Кирпичова, 2, Харьков, 61000, pihnastyi@gmail.com, orcid.org/ 0000-0002-5424-9843

ПИЛЬКЕВИЧ Игорь Анатольевич, доктор технических наук, профессор, Житомирский военный институт имени С. П. Королева, *igor.pilkevich@meta.ua*, orcid.org/ 0000-0001-5064-3272

РУДНИЧЕНКО Николай Дмитриевич, кандидат технических наук, доцент кафедры информационных технологий, Одесский национальный политехнический университет, проспект Шевченко, 1, Одесса, 65044, *nickolay.rud@gmail.com*, orcid.org/ 0000-0002-7343-8076

СИТНИКОВ Валерий Степанович, доктор технических наук, профессор, Одесский национальный политехнический университет, проспект Шевченко, 1, Одесса, 65044, *sit-nvs@gmail.com,* orcid.org/0000-0003-3229-5096

СТРЕЛЬЦОВ Олег Васильевич, кандидат технических наук, доцент, Одесский национальный политехнический университет, проспект Шевченко, 1, Одесса, *ovstreltsov@gmail.com,* orcid.org/ 0000-0002-4691-5703

СТУПЕНЬ Павел Вячеславович, кандидат технических наук, доцент, Одесский национальный политехнический университет, проспект Шевченко, 1, Одесса, *stek2000@gmail.com,* orcid.org/0000-0003-1952-6144

УХИНА Анна Владимировна, кандидат технических наук, доцент, Одесский национальный политехнический университет, проспект Шевченко, 1, Одесса, 65044, *ukhinanna@gmail.com,* rcid.org/ 0000-0003-3797-1460

ФАРИОНОВА Татьяна Анатолеевна, кандидат технических наук, доцент, Национальный университет кораблестроения им. Адмирала Макарова, *tetyana.farionova@nuos.edu.ua,* orcid.org/0000-0003-3384-4712

ФЕДОСОВА Ирина Васильевна, доктор педагогических наук, профессор, ректор, Приазовский государственный университ, ул. Университетская, 7, Мариуполь, 87500, *irivasilevna1964@gmail.com,* orcid.org/0000-0003-3923-8270

ЧУПРИНКА Виктор Иванович, доктор технических наук, профессор, Киевский национальный университет технологий и дизайна, ул. Немировича-Данченко, 2, Киев, 01011, Chuprinka_V_I@ukr.net, orcid.org/ 0000-0001-6869-3091

ЧУПРИНКА Наталья Викторовна, кандидат технических наук, Киевский национальный университет технологий и дизайна, ул. Немировича-Данченко, 2, Киев, 01011, Natasha-chup@ukr.net, orcid.org/0000-0003-1507-489X

ШИБАЕВА Наталья Олеговна, кандидат технических наук, доцент, Одесский национальный политехнический университет, проспект Шевченко, 1, Одесса, 65044, *nati.shibaeva@gmail.com*, orcid.org/ 0000—0002—7869—9953

ШИБАЕВ Денис Сергеевич, аспирант кафедры технической кибернетики и информационных технологий, Одесский национальный морской университет, ул. Мечникова 34, Одесса, 65044, *denscreamer@gmail.com*, orcid.org/ 0000-0002-3260-5843

Наукове видання

**ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ.
СТАН І ПЕРСПЕКТИВИ.**

Монографія

Під наук. ред. проф. В. Вичужаніна

Укр., рос. та англ. мовами

Підп. до друку 22.09.2021.
Формат 60x84/16. Папір офсет.
Гарнітура Times New Roman. Ум. друк. арк. 11,97.
Тираж 300 пр. Зам. № И21-09-82

НУ «ОМА»
65029, м. Одеса, Дідріхсона, 8.
Тел./факс (0482) 34-14-12
publish-r@onma.edu.ua
Свідоцтво суб'єкта видавничої справи
ДК № 1292 від 20.03.2003

Інформаційні системи та технології. Стан і перспективи: моно-
И74 графія / Бармак О., Божаткін С. та ін .; під наук. ред. проф.
В. Вичужаніна. – Одеса: НУ «ОМА», 2021. – 206.
Укр., рос. та англ. мовами
ISBN 978-617-7857-11-1

У монографії відображені результати наукових досліджень в області інформаційонних систем, інтелектуальних систем і аналізу даних, моделювання і розробки програм. Матеріали монографії будуть корисними для аспірантів, магістрантів, викладачів вищих навчальних закладів, що спеціалізуються в області IT-технологій.

УДК 681.518.54