УДК 004.056.5:004.738.5:004.42

Череватий Б.С., магістрант,
Шушура О.М., д.т.н., професор,
Соломаха С.А., к.е.н., доцент
Державний університет інформаційно-комунікаційних технологій

СИСТЕМА ЗАБЕЗПЕЧЕННЯ МОНІТОРИНГУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНИХ TELEGRAM-ЧАТІВ

Активне поширення цифрових інструментів комунікації в корпоративному середовищі зумовило зростання ролі месенджерів як основного засобу оперативної взаємодії між співробітниками. Однією з найбільш універсальних платформ є Telegram, що завдяки високій продуктивності, гнучкій інфраструктурі та можливостям інтеграції через боти все частіше використовується в організаціях різного масштабу. Проте збільшення обсягів обміну інформацією у таких середовищах супроводжується підвищенням ризиків витоку конфіденційних даних, несанкціонованого доступу, внутрішніх інцидентів та помилок користувачів. Це формує об'єктивну необхідність створення спеціалізованих систем контролю та моніторингу інформаційної безпеки корпоративних чатів.

Постановка задачі

Telegram став одним із провідних інструментів корпоративної комунікації завдяки простоті використання, можливості автоматизації процесів та підтримці швидкого обміну даними. Однак відсутність централізованих механізмів контролю безпеки, неконтрольоване поширення службової інформації, ризики соціальної інженерії та користувацькі помилки створюють загрозу для інформаційної безпеки підприємств.

Проблема полягає у відсутності ефективного інструменту, який би забезпечував комплексний моніторинг дотримання політик безпеки в корпоративних чатах Telegram та дозволяв би своєчасно виявляти потенційні інциденти без необхідності ручного контролю з боку адміністратора.

Мета дослідження

Метою роботи є розроблення системи моніторингу інформаційної безпеки для корпоративних чатів Telegram, що забезпечує автоматизований контроль за дотриманням політик безпеки, виявлення порушень та інформування відповідальних осіб у режимі реального часу.

Для досягнення цієї мети визначено такі основні завдання:

- дослідити Telegram як платформу корпоративної взаємодії;
- ідентифікувати ключові загрози та ризики інформаційної безпеки;
- сформувати архітектуру системи моніторингу та розробити відповідні алгоритми обробки подій;
- створити та протестувати робочий прототип системи на основі Telegram Bot API.

Результати дослідження

У ході дослідження розроблено архітектуру системи моніторингу інформаційної безпеки, що включає такі ключові модулі:

- модуль збору даних;
- модуль аналізу безпеки;
- модуль логування та сповіщення.

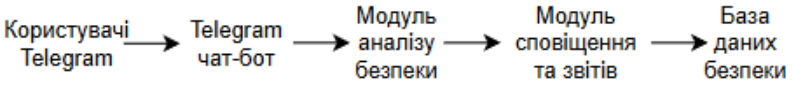

Рисунок 1 - Схема архітектури системи моніторингу

Висновки та перспективи

Розроблена система моніторингу інформаційної безпеки корпоративних чатів Telegram забезпечує можливість оперативного контролю за дотриманням політик безпеки без втручання у приватне листування користувачів. Отримані результати демонструють потенціал такого рішення для інтеграції у корпоративні середовища з метою зменшення ризиків витоку даних, запобігання загрозам та підвищення загального рівня кібербезпеки.

Подальші перспективи роботи включають:

- розширення можливостей аналізу з використанням NLP і машинного навчання;
- адаптацію моделі моніторингу до інших месенджерів;
- впровадження механізмів автоматичного реагування на інциденти.

Список використаних джерел:

1. Горовий В. М. Інформаційні фактори розвитку інформаційних ресурсів у контексті сучасного національного інформаційного комплексу // Національна бібліотека України імені В. І. Вернадського. 2024. URL: https://irbis-nbuv.gov.ua/E_LIB/PDF/er-0004857.pdf

2. Bahramali A., Soltani R., Houmansadr A., Goeckel D., Towsley D. Practical Traffic Analysis Attacks on Secure Messaging Applications. URL: https://arxiv.org/abs/2005.00508.