аналогічною тій, яку користувачі практикують у звичайному житті або ж така, яка є неможливою в реальному світі [1, с.122]. Зазвичай в Інтернеті люди здійснюють пізнавальну, комунікативну та ігрову діяльність [3, с.160].

Віртуальна реальність несе для людства безліч можливостей, має практичне значення в житті суспільства, а також відіграє значну роль у розвитку особистості. Але вона й негативно впливає на людей та суспільство. Наприклад, поширеною сучасною проблемою є Інтернет-залежність [4]. Цей психічний розлад поділяють на п'ять видів: комп'ютерну залежність, компульсивну навігацію в мережі (компульсивний пошук інформації у віддалених базах даних), перевантаженість інформацією (патологічна схильність до опосередкованих інтернетом азартних ігор, онлайн-аукціонів, електронних покупок), кіберкомунікативну залежність (залежність від спілкування в соціальних мережах, чатах) [3, с.158].

Отже, необхідно більш детально досліджувати й вивчати питання, що стосуються віртуалістики, її ознак та властивостей, впливу на людей та суспільство тощо. Ця тема є актуальною, важливою та малодосліджуваною. Ми вважаємо, що дослідження віртуального простору необхідно проводити з інформаційної, соціологічної, культурологічної та філософської точок зору.

Список використаних джерел:

1. Волинець В.О. Віртуальна реальність у соціокультурному просторі сучасності В.О. Волинець // Культура України. – 2016.р – Вип. 52. – С. 120-128.

2. Дзьобань О. П. Сучасний віртуальний простір: конгеніальність віртуальності й міфу / В.О. Волинець // Стратегічні пріоритети. – 2017. – № 3 (44). – С. 163-170.

3. Литвинчук Л. Соціальні патології особистості як технологічні адиктивні тенденції сучасного соціокультурного середовища / Л. Литвинчук // Зб. наук. праць Нац. акад. держ. прикордон. служби України. Серія: Психологічні науки. – 2019. – № 2 (13). – С. 158-169.

4. Мацьоха Т. Інтернет-залежність української молоді: сучасний стан проблеми. Спільне: журнал соціальної критики. – 2017. – Режим доступу: https:// commons.com.ua /uk /internet-zalezhnist /. – Назва з екрана.

5. Немеш О.М. Віртуальна діяльність особистості: структура та динаміка психологічного змісту: монографія / О. М. Немеш. К.,: Слово, 2017. – 391 с.

УДК 004.056.5

Кузьо М. – аспірант
Тернопільський національний технічний університет імені Івана Пулюя

ЗАСТОСУВАННЯ СТЕКУ ELK В ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ ДЛЯ КІБЕРБЕЗПЕКИ

Науковий керівник: к.т.н. Кареліна О. В.

Kuzyo M.
Ternopil Ivan Puluj National Technical University

USING THE ELK STACK IN CYBERSECURITY SOFTWARE

Supervisor: Karelina Olena

Ключові слова: ELK Stack, кібербезпека
Key words: ELK Stack, cybersecurity

Модель та масштаб кіберзагроз для організацій швидко еволюціонують. Будь-яка установа потребує запровадження систем для моніторингу IT-інфраструктури та швидкого реагування на інциденти задля забезпечення запуску і подальшої роботи необхідних їй мережевих систем і сервісів

Сучасні порушники постійно намагаються вдосконалювати свої методи та інструменти для успішного проведення кібератак, а стрімке збільшення інформаційного потоку змушує організації розглядати нові варіанти захисту інформації, забезпечуючи стабільність та захищеність інформаційної системи.

В процесі створення захищеної інфраструктури, спеціалістам потрібно приймати до уваги величезну кількість подій які відбуваються в системі. Для покращення процесів моніторингу за подіями та превентивного підходу до дій порушників, компанія Elastic розробила ряд рішень під назвою ELK Stack, які поєднують інструменти для інтегрування інформації про захищеність, події та журнали визначення інцидентів та аномальних подій. Зазвичай організації вибирають ELK Stack тому що цей продукт має модульну основу і містить декілька інструментів які можна вилучити або модифікувати у разі необхідності. Інтегруючи компоненти Elasticsearch, Logstash і Kibana до інфраструктури організації вони будуть відповідати за наступні функції:

- Elasticsearch – це ядро всієї системи, яке поєднує в собі функції бази даних, пошукової та аналітичної системи;
- Logstash – це конвеєр обробки даних на стороні сервера, який отримує дані з декількох джерел одночасно, обробляє лог, а потім відправляє в базу даних Elasticsearch;
- Kibana дозволяє користувачам візуалізувати дані за допомогою діаграм і графіків в Elasticsearch, а також адмініструвати базу даних через зручний інтерфейс.

Організації можуть використовувати ELK Stack для управління загрозами, виявленням та розслідуванням кіберінцидентів, щоб швидко передавати інформацію про події та усувати наслідки. Потреба в залучені команди аналітиків для реагування на кількість кібератак та їх організацію послугувала причиною розгляду методів та засобів, які можуть автоматизувати процеси для скорочення часу як на стримування інцидентів, так і на повне усунення нападу, що стосується кібербезпеки.

Отже, за допомогою програмних продуктів компанії Elastic можна створити чіткий механізм, який реалізовував би захист інформації для усунення слабких місць в інфраструктурі організації та швидке реагування на інциденти.

Література:

1. Elastic Stack[Електронний ресурс] - Режим доступу до ресурсу: https://www.elastic.co/elasticstack
2. Deploying of infrastructure and technologies for a SOC as a Service (SOCasS) [Електронний ресурс] – Режим доступу до ресурсу: https://medium.com/@ibrahim.ayadhi/deploying-of-infrastructure-andtechnologies-for-a-soc-as-a-service-socass-8e1bbb885149