- Вибрати анімацію яку ви бажаєте використати та її додаткові параметри

Отже, анімація це корисний інструмент. Додавання анімації у вашу презентацію це простий спосіб зробити ваш текст цікавішим та кращим. Анімації те переходи допоможуть краще запам'ятати інформацію та покращать загальний вигляд вашої презентації чи тексту. Основне призначення анімації – створення передумов поглибленого розуміння слухачем матеріалу за допомогою різних параметрів, звуків та ефектів [4].

Додавати анімацію до слайдів настільки просто, що ви легко можете втратити контроль. Таким чином це може відвернути увагу аудиторії від основної думки яку ви намагаєтесь донести. Ось декілька вказівок, яких слід дотримуватися, додаючи анімацію в PowerPoint [5]:

- Простота. Прості анімації, як-от згасання чи поява, можуть бути не такими вражаючими як інші, але вони додають нотку елегантності вашим слайдам
- Обмежена кількість анімації на слайді. Достатньо однієї чи двох анімацій.
- Визначте час для своєї презентації. Переконайтеся що ваші об'єкти з'являються вчасно
- Пам'ятайте – що анімація, це весело та чудово, якщо її використовувати економно і з смаком.

Список літературних джерел

1. *Basic tasks for creating a PowerPoint presentation. May 22, 2017. 7-12 pages.*
2. *Animations for Infographics in Power Point presentation. June 13, 2020. 37-45 pages.*
3. *How to Create Custom Animations in PowerPoint, Url: https://www.ispringsolutions.com/blog/how-to-create-a-custom-animation-in-powerpoint*
4. *How to animate powerpoint slides, Url: https://slideuplift.com/blog/powerpoint-tutorials/how-to-animate-powerpoint-slides-powerpoint-tutorial/*
5. *Animation for powerpoint, Url: https://blog.udemy.com/animation-for-powerpoint/*

УДК 004.056.53:519.83

Діденко М.М., студентка 4 курсу спеціальності 125 «Кібербезпека»
Ніколюк П. К., д.т.н., професор, професор кафедри інформаційних технологій

ЗАСТОСУВАННЯ ТЕОРІЇ ІГОР І КІБЕРБЕЗПЕЦІ

Донецький національний університет імені Василя Стуса, м. Вінниця

Кібербезпека - це процес, спрямований на запобігання атакам несанкціонованих користувачів на комп'ютери, підключені до Інтернету, та конфіденційну інформацію, що міститься в них. Кібер-ризики розвиваються швидкими темпами разом зі зростанням кіберінфраструктури. Традиційні технології кібербезпеки зосереджені лише на добре відомих загрозах і не дуже добре підходять для інфраструктури з великим мережевим трафіком. Теорія ігор допомагає вирішувати проблеми кібербезпеки краще, ніж традиційні підходи.

Теорія ігор використовується в кібербезпеці для спостереження за природою кіберінциденту - коли захисники мережі, зловмисники і користувачі взаємодіють один з одним і досягають результату. Теорія ігор корисна тим, що вона моделює поведінку кожного гравця, його стратегії і фіксує взаємодію між гравцями-суперниками[1].

Теорія ігор використовується в кібербезпеці для спостереження за природою кіберінциденту - коли захисники мережі, зловмисники і користувачі взаємодіють один з одним і досягають результату. Теорія ігор корисна тим, що вона моделює поведінку кожного гравця, його стратегії і фіксує взаємодію між гравцями-суперниками.

У цій "ігровій" взаємодії протиборчих сил (чи то команд, чи то окремих осіб) кожна сила зацікавлена у виграші, або навпаки, в уникненні програшу.

Взагалі, кібербезпека є незбалансованою грою, оскільки захисники мережі завжди знаходяться в невигідному становищі. Незважаючи на всі технології кібербезпеки, вони не знають, коли, де і як зловмисники завдадуть удару. На інформації наведеній вище, чудово можна помітити, як кібербезпека пов’язана з теорією ігор, але розглянемо це ще на декількох прикладах[2].

Можна виділити дві широкі категорії застосування теорії ігор у сфері кібербезпеки:

1. Аналіз захисту від кібератак
2. Оцінка кібербезпеки

Моделюючи поведінку захисту у вигляді ігор, можна передбачити дії кібератакувальника в аналізі кібератакизахисту. Він також аналізує можливі стани рівноваги між атакою та захистом. Стратегії контрзахисту можуть бути визначені в ідеалі на основі стану рівноваги.

Рівноважний стан кібератаки-захисту може бути ретельно вивчений, а прогноз стратегій атаки та захисту може бути використаний для раціоналізації кібернетичної безпеки та оцінки. Завдяки кількісним аспектам ігрового аналізу безпека та надійність розглядається як кількісна оцінка, яка дає обчислення кібернетичної безпеки та надійності.

Класифікація методів теорії ігор у сфері кібернетичної безпеки була класифікована таким чином, як показано на Таблиці 1. Кібербезпека приймає некооперативну динамічну ігрову модель. Стратегії зловмисників при кібератаках не є статичною і для досягнення ідеального ефекту дуже важливим

є аналіз динамічної моделі, оскільки динамічні моделі дуже близькі до реальних проблем кібербезпеки в реальному часі. А для аналізу кіберзахисту використовується неповна інформаційно-ігрова модель [3].

<table>
<tr><td colspan="3">Ігрові моделі</td><td>Питання застосування та безпеки</td></tr>
<tr><td colspan="2">Кооперативні ігрові моделі</td><td>Статистичні ігрові моделі</td><td>Мобільні бездротові ad hoc моделі</td></tr>
<tr><td colspan="2" rowspan="5">Некооперативні ігрові моделі</td><td colspan="2">Статистичні ігрові моделі</td><td>Виявлення несанкціонованого проникнення</td></tr>
<tr><td colspan="2"></td><td>Оптимізація безпеки</td></tr>
<tr><td rowspan="3">Динамічні ігрові моделі</td><td rowspan="2">Повні інформаційні ігрові моделі</td><td>Механізм безпекового стимулювання</td></tr>
<tr><td>Оптимізація безпеки</td></tr>
<tr><td>Не повні інформаційні ігрові моделі</td><td>Аналіз кібератаки-захист</td></tr>
</table>

Таблиця 1. Класифікація методів теорії ігор у сфері кібернетичної безпеки[3].

Підводячи підсумки, можна сказати, що теорія ігор в літературі має доведені результати щодо її здатності вирішувати проблеми. З огляду на це, в даній роботі зроблена спроба розкрити питання важливості вивчання аспектів теорії ігор в такій, на перший огляд не пов’язаній галузі, як кібербезпека.

Список літератури

1. *Fighting Cyber Attacks With Game Theory. Threatpost | The first stop for security news. URL: https://cutt.ly/m1YYRNF (дата звернення: 30.11.2022).*
2. *Game-theoretic approach to the network security problem. PROBLEMS IN PROGRAMMING. 2017. No. 3. p. 149–160. URL: https://doi.org/10.15407/pp2017.03.149 (date of access: 30.11.2022).*
3. *G. Owen, Game Theory, New York: Academic Press, 3rd ed., 2001, p. 46.*

УДК 004.01

Калько Д. Р., студент 1 курсу спеціальності 122 «Комп’ютерні науки»
Ніколюк П. К., д-р фіз.-мат. наук, Професор кафедри комп’ютерних наук

МЕТОДИ ТА ЗАДАЧІ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ

Донецький національний університет імені Василя Стуса, м. Вінниця