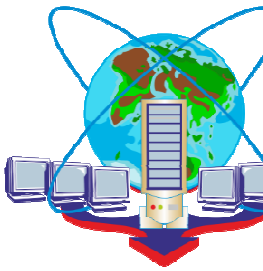
Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
Факультет радіотехнічних систем літальних апаратів
Кафедра комп'ютерних систем та мереж



Всеукраїнський конкурс студентських наукових робіт у галузі наук
„Інформаційна безпека” 2015/2016 н.р.

Моделі оцінювання кібербезпеки інформаційних систем

Виконала Стрєлкіна А.А.
Керівник Узун Д.Д.

Актуальність

Поточні тенденції

Головний пріоритет 41% компаній – захист конфіденційних даних від цільових атак

98% підприємств зіткнулися с інцидентами кібербезпеки

- Надходили ззовні
- На 3% більше, ніж на рік раніше
- Чверть компаній втратили дані

87% компаній постраждали від внутрішніх загроз

Майже чверть інцидентів призвели до втрати конфіденційних даних

Найчастіше компанії втрачають операційні дані про внутрішню діяльність, персональні дані клієнтів і фінансові відомості

Постановка задач

Мета	• оцінювання кібербезпеки інформаційних систем
Окремі задачі	• розроблення марковської моделі процесів кібербезпеки інформаційних систем • розроблення моделі оцінки потенційного збитку від вдалих кібератак, заснованої на методах теорії ігор. • розроблення IMECA таблиці атак на бездротові мережі

Марковська модель готовності системи с урахуванням загроз інформаційної безпеки

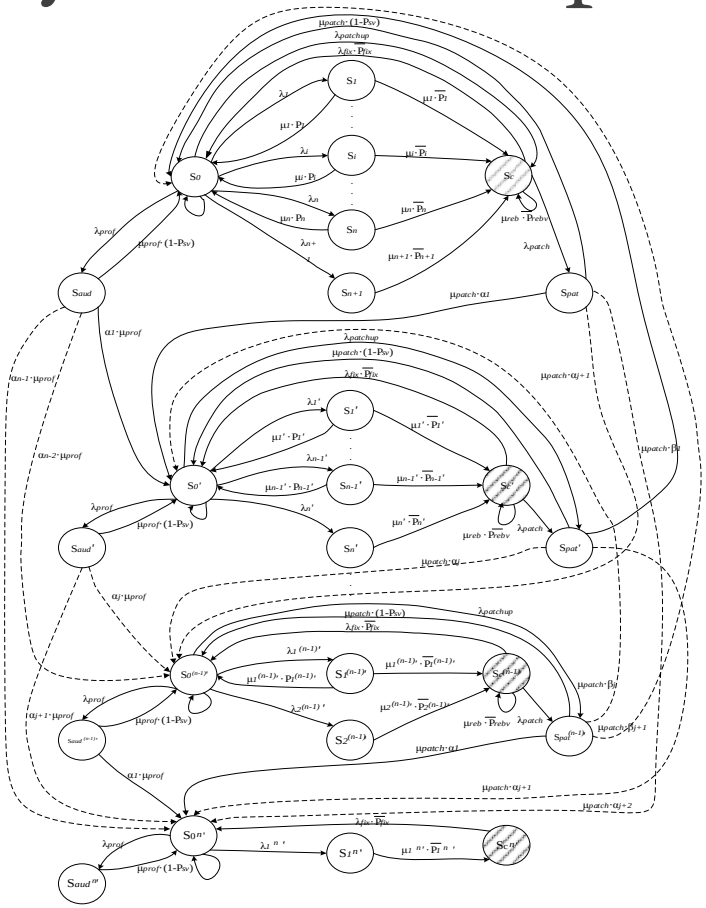


Рисунок 1 – Граф станів та переходів системи при впливі на неї n незалежних загроз та усуненні вразливостей

P_j і $\overline{P_j} = 1 - P_j$ – ймовірності успішного і неуспішного парирування виникл
j-ої атаки відповідно;

$\lambda_j, j = 1,n$ – інтенсивність атак на інформаційну систему;

μ_j – інтенсивність відображення наслідків j-ої атаки;

$\mu_j \cdot P_j$ – інтенсивність відображення атак на інформаційну систему;

$\mu_j \cdot \overline{P_j}$ – інтенсивність успішної реалізації атаки на інформаційну систему;

λ_{prof} – інтенсивність проведення профілактичних заходів аудита безпеки;

μ_{prof} – інтенсивність відновлення системи після профілактичних заход
аудиту безпеки;

P_{sv} – ймовірність усунення однієї вразливості;

μ_{reb} – інтенсивність перезапуску системи після атаки;

$\lambda_{patchup}$ – інтенсивність розроблення оновлень, в яких усуваютьс
вразливості;

λ_{patch} – інтенсивність розроблення патча на після атаки на вразливість;

μ_{patch} – інтенсивність відновлення системи після установки патча (а
оновлень);

λ_{fix} – інтенсивність усунення вразливості;

P_{fix} – ймовірність перезапуску з усуненням вразливості;

λ_a – зміна інтенсивності прояви дефектів в системі, обумовлена появою а
усуненням вразливостей в системі.

Модель оцінки потенційного збитку на основі теорії ігор

Таблиця 1 - Таблиця матричної гри

		y_1	y_2	y_3	…	y_m
x_1	$p(x_1)$	a_{11}	a_{12}	a_{13}	…	a_{1m}
x_2	$p(x_2)$	a_{21}	a_{22}	a_{23}	…	a_{2m}
x_3	$p(x_3)$	a_{31}	a_{32}	a_{33}	…	a_{3m}
…	…	…	…	…	…	…
x_n	$p(x_n)$	a_{n1}	a_{n2}	a_{n3}	…	a_{nm}

Стратегія зловмисника рядки $x_i(i = \overline{1,n})$

Стратегія адміністратора безпеки стовпці $y_j(j = \overline{1,m})$

Показник a_{ij} - результат гри

Умовою ефективного захисту є правило: вартість засобів захисту повинна бути менше вартості втрат, понесений при вдалій реалізації атак

Результат кількісної оцінки збитку від можливої атаки

Таблиця 2 - Матриця ймовірностей відбиття атак

Атаки/захист	Ймовірність атаки	Засоби захисту			
		Немає засобів захисту	Firewall	IDS	Резервування каналу зв'язку
		Ймовірність відбиття атаки			
UDP-флуд	0,0783	0	0,80	0,95	0,80
SYN-флуд	0,0778	0	0,60	0,93	0,75
TCP-флуд	0,0275	0	0,80	0,99	0,80
ICMP-флуд	0,013	0	0,80	0,95	0,83

Таблиця 3 - Вартість засобів захисту в у.е. (дотримана пропорція)

Атаки/захист	Немає засобів захисту	Firewall	IDS	Резервування каналу зв'язку
	0	1	50	20

Таблиця 4 - Матриця коефіцієнтів ефективного захисту при величині збитку D = 500 у.е. з вибором засобів ефективного захисту

Атаки/захист	Ймовірність атаки	Засоби захисту			
		Немає засобів захисту	Firewall	IDS	Резервування каналу зв'язку
		Коефіцієнти ефективного захисту			
UDP-флуд	0,0783	0	0,1277	25,5428	2,5543
SYN-флуд	0,0778	0	0,0643	18,3621	2,0566
TCP-флуд	0,0275	0	0,3636	363,6364	7,2727
ICMP-флуд	0,013	0	0,7692	153,8462	18,0995
Мінімум по стовпцю			0,0643	18,3621	2,0566
Максимум по строчці <1			**0,0643**		

IMECA таблиця атак бездротові мережі

Таблица 5 – Фрагмент IMECA таблиці атак

Gap №	Режим атаки	Природа атаки	Причина атаки		Вероятность возникновения	Тяжесть последствия	Вид последствия	Контрмеры
			Объективная	Субъективная				
1	Атаки направленные на модификацию или манипуляцию данными	Активная	- Не используются методы для гарантии целостности данных	Добавление, изменение или удаление корпоративных данных, нарушение целостности информации	Средняя	Высокая	Получение, изменение или удаление злоумышленником информации	- Использование цифровых подписей для гарантии, что данные не были модифицированы во время передачи по сети или при сохранении куда-либо; - Использование листов контроля доступа ACL (Access Control Lists) для реализации раздельных прав доступа к данным; - Регулярное резервное копирование важной информации; - Включение специального кода в приложения, который может проверять вводимые данные
2	Атаки на прослушивание (Eavesdropping)	Пассивная	- Транзакции проходят в открытом виде; - Не установлено дополнительное ПО для	Получение несанкционированного доступа к информации	Высокая	Высокая	Получение секретной информации злоумышленником	- Применение IPSec (Internet Protocol Security) для шифрования данных до их отправки в сеть; - Применение политик и процедур безопасности, которые не дадут возможности атакующему установить программу-сниффер в сети; - Установка антивирусного ПО (и модифицированного ПО для поиска

Рисунок 2 – Матриця критичності

Взаємозв'язок розроблених моделей

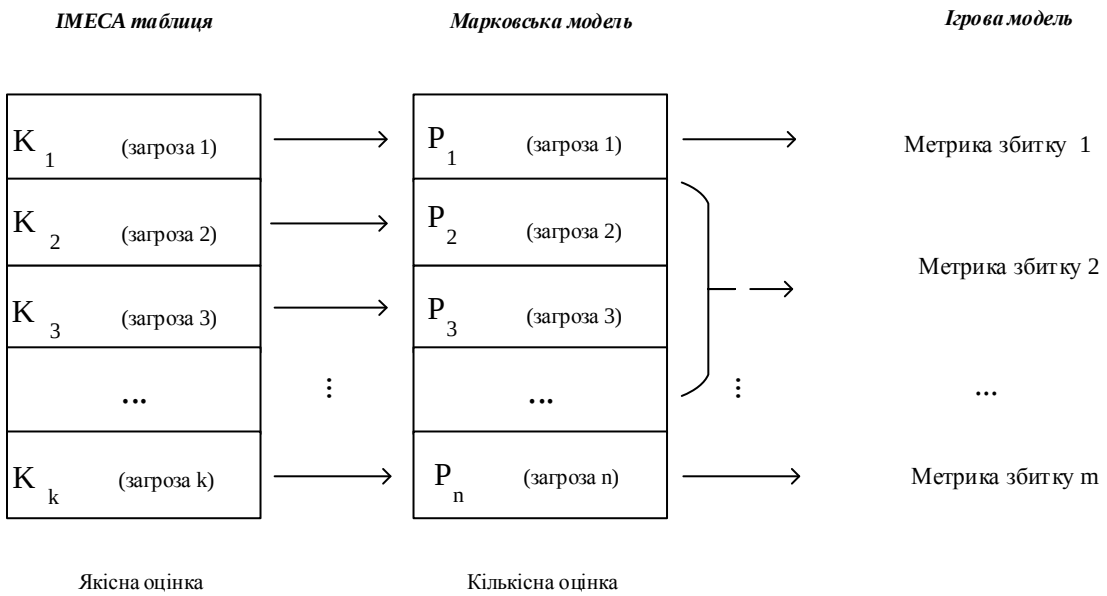


Рисунок 3 – Варіант взаємодії розроблених моделей

Висновки

Представлено марковський граф впливів на систему загроз і усунення вразливостей.

Запропоновано модель оцінки потенційного збитку при вдалій атаці на систему, основану на методах теорії ігор.

Розроблено IMECA таблицю основних типів атак на бездротові мережі.

Запропоновані моделі можуть бути використані для оцінки та аналізу рівня інформаційної безпеки на різних підприємствах.

Публікації

rvice for vulnerabilities analysis and security assessment of open source systems / A. rielkina, A. Tetskyi, B. Selin, O. Solovyov, D. Uzun // CERes Journal, Volume 1, Issue 2, 15 – Режим доступу до ресурсу: http://ceres-journal.eu/iss150102 (на англійській)

арковська модель процесів кібербезпеки інформаційних систем / А. А. Стрелкина, Д. Узун // Відкриті інформаційні і комп'ютерні інтегровані технології. - 2015. - Вип. 70 200-206. (на російській)

ези конференцій

сследование ущерба, модели нарушителя, модели атаки и функционала устройства дл стирования на проникновение Wi-Fi сетей // Всеукраїнська науково-технічна нференція ІКТМ: Тези доповідей. – Харків: НАУ ім. М.Є. Жуковського «ХАІ», 2015. ом 2-195 с.

Список використаної літератури

ормационная безопасность бизнеса [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: http://media.kaspersky.com/pdf/IT_risk_report_Russia_201

стренко В. А. Безопасность информационных систем и технологий / В. А. Майстренко, В. Г. Шахов. – Омск: Изд-во ОмГТУ, 2006. – 232 с.

енко А. П. Применение марковских случайных процессов с дискретным параметром для оценки уровня информационной безопасности / А. П. Рос

естия Южного федерального университета. Технические науки. – 2009. – №11.

обьев А.А. Методы оценивания и обеспечения гарантированного уровня защиты информации от несанкционированного доступа в вычислительно

матизированной системы управления: Автореф. дис. к-та техн. наук / А.А. Воробьев. СПб., 1997. 15 с.

теров С.А. Разработка методов и средств проектирования инфраструктуры обеспечения информационной безопасности автоматизированных систем: Ав

к-та техн. наук / С.А. Нестеров. СПб., 2002. 18 с.

ричные игры / Под. ред. Н.Н. Воробьева. М : ФМ, 1961. 280 с.

ний Т.В., Гуц А.К. Теоретико-игровой подход к выбору оптимальных стратегий защиты информационных ресурсов // Математические структ

елирование. 2009. №. 19. С. 104-107.

н Г. Теория игр / Г. Оуэн. – Москва: Мир, 1971.

жевич М.А.Т93 Экономико-математические методы (исследование операций). Изд. 2, испр. и доп. - Кемерово, 2000. -177 с. ISBN 5-89070-043-X.

oS-атаки во втором квартале 2015 года [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: https://securelist.ru/analysis/malware-quarterly/2646

-vo-vtorom-kvartale-2015-goda/.

овы ИТ-инженерии безопасности критических инфраструктур: [Текст] практикум / Е.В. Брежнев, А.А. Орехова, О.А. Ильяшенко / под ред. В.С. Харч

ЛП Лысенко И.Б., 2013. – 185

Дякую за увагу!