Contribution ID: **307** Type: **not specified**

ЦИФРОВЫЕ ДВОЙНИКИ В СИСТЕМАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цифровой двойник (Digital twin, сокр. DT) —это виртуальное представление процессов, физических объектов или систем, которое используется в качестве оценки, диагностики, оптимизации и контроля их характеристик при проектировании, принятии решений в различных ситуациях и для эффективного управления реальными системами . В системах информационной безопасности концепция DT решает несколько задач:
1. Моделирование конечных параметров систем информационной безопасности с заданными начальными параметрами и ориентированными на конечные цели организации.
2. Оценка защищенности информационных систем на основе их DT по контролю параметров архитектуры системы информационной безопасности (ИБ).
3. Прогнозирование реакции системы управления информационной безопасностью (СУИБ) на возможные инциденты.
4. Расследование инцидентов информационной безопасности на модели DT.
5. Поддержка принятия решений на развитие системы информационной безопасности.
6. Оценка эффективности СУИБ по заданным критериям.
7. Формирование профессиональных компетенций по направлениям информационной безопасности на модели цифрового двойника за счет реакции системы ИБ на изменение настроек архитектуры ИБ, модели угроз и реализации сценариев атак на информационную систему.
В настоящее время идет активная работа по реализации первой модели цифрового двойника. Эта модель основана на оценке параметров рисков в виде возможных ущербов (Su) и затрат (Sz) на создание архитектуры системы ИБ

```
<Nt, Et, Nv, Ev, Na, Ea, M, V,  , Z, U, Sz, Su, U-Z>
```

где Nt, Nv, Na –наименования (коды) угроз, уязвимостей, активов;
Et, Ev, Ea –значения возможностей появления угроз, величин уязвимостей и ценностей активов в числовых значениях лингвистических переменных;
M - метрики рисков, определяются как сумма M = Et + Ev + Ea ;
V, C, Z, U, U-Z –вариант обработки рисков, контрмеры по защите, затраты, ущерб (риск), разница между двумя суммами U и Z.
Вариант решения задачи моделирования плана обработки рисков в условия ограниченного финансирования на СМИБ проводится с использованием следующей целевой функции

где s –стратегия управления рисками, позволяющая ранжировать их по приоритетам.
Дальнейшее развитие этой модели позволяет находить решения по оценке эффективности СУИБ по критериям максимальной добавленной ценности (Su - Sz) за счет предотвращенного ущерба от реализации угроз.

Summary

Primary author: BOBYLEVA, Sofia (Dubna State University)

Co-author: МИНЗОВ, Анатолий (Россия)

Presenter: BOBYLEVA, Sofia (Dubna State University)

Session Classification: Workshop ”Modern approaches to the modeling of research reactors, creation of the ”digital twins” of complex systems” (4-5 July)

Track Classification: Workshop ”Modern approaches to the modeling of research reactors, creation of the ”digital twins” of complex systems” (4-5 July)