конференция РусКрипто

ЦИФРОВЫЕ ДВОЙНИКИ В СИСТЕМАХ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

- **Невский Александр Юрьевич**, кандидат технических наук, заведующий кафедрой БИТ НИУ МЭИ
- **Минзов Анатолий Степанович**, доктор технических наук, профессор кафедры БИТ НИУ «МЭИ»
- **Баронов Олег Рюрикович**, кандидат технических наук, доцент кафедры безопасности БИТ НИУ МЭИ

15.03.2024

Что мы понимаем под термином «цифровой двойник»?

Термин «**цифровой двойник**» (Digital twin, сокр. DT) появился более десяти лет назад и до сих пор не имеет четкого определения.

1. Цифровой двойник изделия (ЦД) – система, состоящая из цифровой модели изделия и двусторонних информационных связей с изделием (при наличии) и (или) его составными частями.

ГОСТ Р 57700.37-2021 Компьютерные модели и моделирование Цифровые двойники изделий. Общие положения.

2. Цифровой двойник (ЦД, DT) - виртуальное или виртуально -физическое 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.

Кафедра БИТ НИУ «МЭИ»

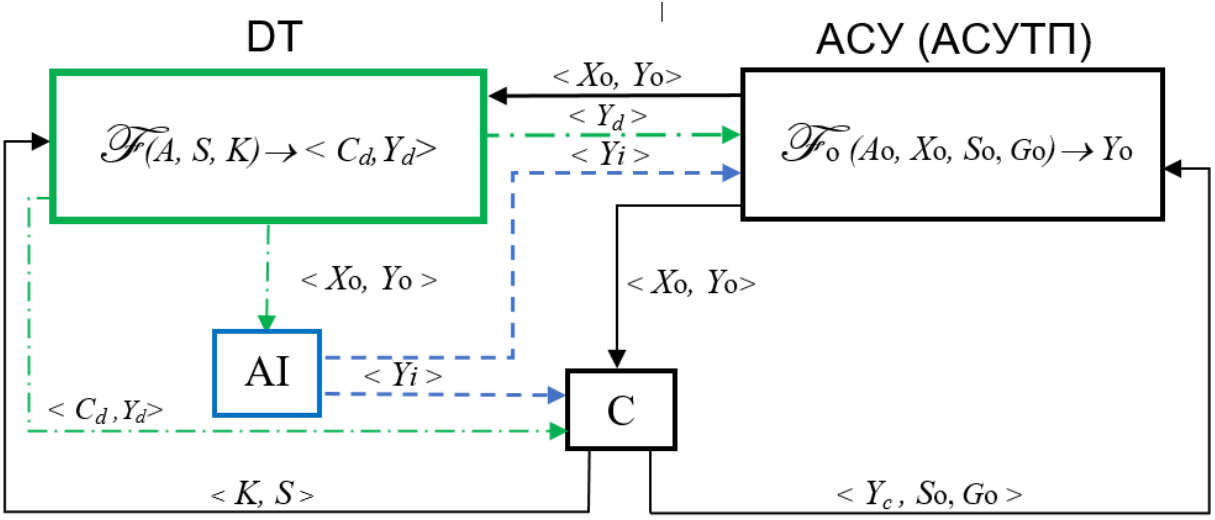
Преимущество нашего подхода заключается в:

- расширенном толковании термина ЦД;
- формировании перечня задач, для решения которых используется ЦД;
- наличии целеполагания использования ЦД;

Задачи управления ИБ, которые решаются в системе DT

1. Моделирование параметров систем информационной безопасности с заданными начальными параметрами и ориентированными на конечные цели организации результатами.
2. Оценка защищенности информационных систем по контролю заданных параметров архитектуры системы информационной безопасности.
3. Прогнозирование реакции системы управления информационной безопасностью (СУИБ) на возможные инциденты.
4. Расследование инцидентов информационной безопасности на модели DT.
5. Поддержка принятия решений на проектирование и развитие системы информационной безопасности.
6. Оценка эффективности СУИБ по заданным критериям.
7. Обучение специалистов методологии создания систем информационной безопасности.

Концептуальная модель цифрового двойника



Условные обозначения:

- ***A*** *– алгоритмы и модели DT;*
- ***S*** *– система ограничений;*
- ***K*** *– критерии эффективности;*
- C_d *– показатели эффективности системы управления;*
- Y_d *– результат моделирования управляющего воздействия по ситуации* X_d.
- A_0 *– алгоритмы, реализующие функции управления;*
- X_0 *– параметры, характеризующие состояние объекта управления;*
- S_0 *– система ограничений;*
- G_0 *– цели управления;*
- Y_0 *– результат управления.*

Практическая реализация концептуальной модели DT

Подход и модель используются в учебном процессе в форме деловой игры « **Управление рисками информационной безопасности объектов КИИ** ». При этом моделируются параметры системы информационной безопасности АСУ с заданными начальными параметрами и результатами, ориентированными на конечные цели организации, которые используются при проектировании и оценке ее эффективности.

Основные ограничения

- Рассматриваются риски только для умышленных угроз, что позволяет значительно уменьшить их число . Другие риски – природные и случайного характера требуют некоторых шаблонных действий.
- В модели ИС применяются правила корреляций между параметрами угроз, уязвимостей и ценностью информационных активов. Это в значительной степени позволяет повысить определенность оценки параметра угроз.

Физическая модель АСУ ТП и ее практическая реализация

$$\mathcal{F}_0 (Ao, Xo, So, Go) \rightarrow Yo$$

где *Ao* – алгоритмы, реализующие функции управления;

Xo = <*Nt, Et, Nv, Ev, Na, Ea* >

So – система ограничений;

Go – цели управления;

Yo = < *M, V, C, Z, U* >, результаты решения для обработки рисков.

Алгоритм реализуется на основе положений ГОСТ Р ИСО/МЭК 27005

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, M = *Et* + *Ev* + *Ea* ;

V, C, Z, U – вариант обработки рисков, контрмеры по защите, затраты, ущерб (риск).

Параметры модели первоначально оцениваются ручным способом, а затем с использованием машинного обучения

Модель цифрового двойника и ее реализация

$$\mathcal{F}(A,S,K) \rightarrow <C_d, X_d, Y_d> \quad ,$$

где A – алгоритмы и модели DT;
S – система ограничений;
K – критерии эффективности системы управления;
C_d – показатели эффективности системы управления;
Y_d – результат моделирования управляющего воздействия по ситуации X_d.

$$\boldsymbol{X_d = <Nt, Et, Nv, Ev, Na, Ea, M, V, C, Z, U>}$$

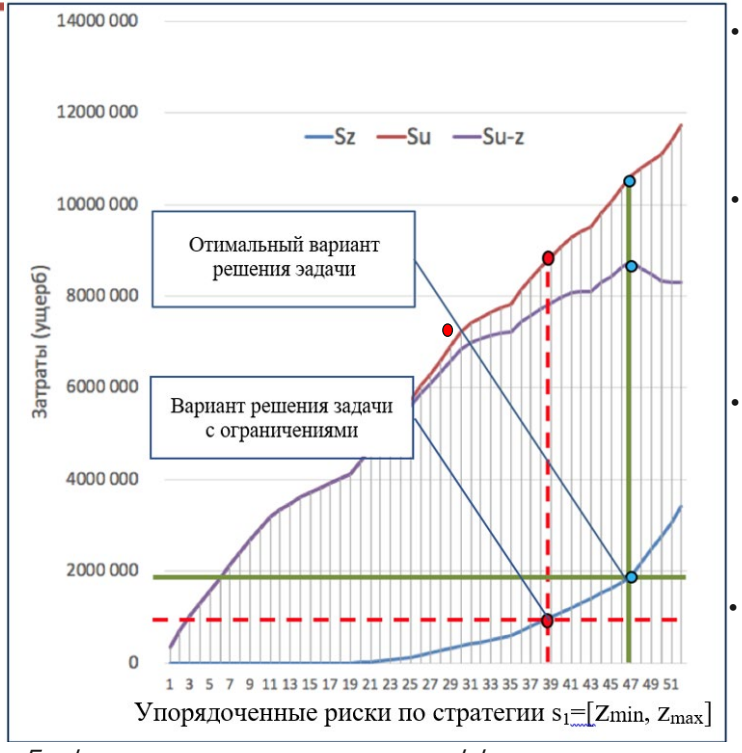
$$\boldsymbol{Y_d = <} s_z, s_u \boldsymbol{>, C_d ,}$$

где $\boldsymbol{U}$ – возможные значения ущерба (риска), выраженные в абсолютных значениях, например в денежных эквивалентах.

s_z, s_u - суммарные значения затрат на принятие мер защиты и возможного ущерба;

$\boldsymbol{C_d}$ – показатели эффективности системы управления рисками информационной безопасности.

Результаты моделирования параметров СУИБ на этапе ее проектирования



Графическая интерпретация оценки эффективности плана обработки риска по вариантам с ограничением по затратам:

- ***Cd₂** (оптимальный вариант);*
- ***Cd₃** (лучший вариант)*

- План обработки рисков при ограничениях на затраты (***Cd*$_1$**)

$$Cd_1 = \left(\sum_{i=1}^{k} z_i^s < z_0 \right), i = \overline{1,k}, s = \overline{1,n}.$$

- План обработки рисков при максимальной разнице между оценками возможного ущерба и затрат (***Cd*$_2$**)

$$Cd_2 = \max_s \left(\sum_{i=1}^{k} (u_i^s - z_i^s) \right), i = \overline{i,k}, s = \overline{1,n}$$

- План обработки рисков при максимальном значении возможного ущерба и ограничениях на затраты

$$Cd_3 = \max_s \left(\sum_{i=1}^{k} (u_i^s - z_i^s) \right), \left(\sum_{i=1}^{k} z_i^s < z_0 \right), i = \overline{1,k}, s = \overline{1,n}.$$

- План обработки рисков при максимальном значении предотвращенного ущерба и ограничениях на затраты

$$Cd_4 = \max_s \left(\sum_{i=1}^{k} u_i^s \right), \left(\sum_{i=1}^{k} z_i^s < z_0 \right), i = \overline{1,k}, s = \overline{1,n}$$

Заключение

Профессор Мичиганского университета Майкл Гривз,

В 2002 году он впервые ввел термин DT и определил его содержание

1. В докладе, на основе анализа, было уточнено содержание термина «цифровой двойник», определено его использование и возможные области применения в сфере информационной безопасности (СУИБ). Это позволило разработать вариант концептуальной модели цифрового двойника и описать его входные и выходные параметры.
2. На примере моделирования конечных параметров систем информационной безопасности с заданными начальными данными и целями был показан механизм разработки модели DT. Эта модель может быть использована при проектировании системы управления информационной безопасностью КИИ.
3. Предложенная концептуальная модель DT позволяет накапливать базу знаний по результатам моделирования и автоматизировать получение оценок параметров плана обработки рисков с использованием методов машинного обучения.

Спасибо за внимание!

Невский Александр Юрьевич, кандидат технических наук, заведующий кафедрой БИТ НИУ МЭИ, NevskyAY@mpei.ru

Минзов Анатолий Степанович, доктор технических наук, профессор кафедры БИТ НИУ «МЭИ», MinzovAS@mpei.ru

Баронов Олег Рюрикович, кандидат технических наук, доцент кафедры безопасности БИТ НИУ МЭИ, BaronovOR@mpei.ru