XXVII научно-практическая конференция «Комплексная защита информации»
с/п Дороховское, Московская обл., 25 – 26 мая 2022 г.

Язов Ю.К., Гефнер И.С., Соловьев С.В.

Перспективы развития методического обеспечения государственного регулирования в сфере защиты информации в информационных системах Беларуси и России

Докладчик:
доктор техн. наук, проф. Язов Юрий Константинович,
ФАУ «ГНИИИ ПТЗИ ФСТЭК России», г. Воронеж

Структура методического обеспечения деятельности по технической защите информации в информационных системах

Методическое обеспечение (МО) деятельности по защите информации (ЗИ) в информационных системах (ИС)

- МО прогнозирования уязвимостей и угроз безопасности информации
  - МО прогнозирования разработки и применения новых информационных технологий
  - МО выявления, анализа и прогнозирования возникновения новых уязвимостей системного и прикладного ПО ИС и экплойтов
  - МО прогнозирования возникновения новых угроз безопасности информации в ИС
  - МО экспериментальных исследований новых угроз БИ в ИС
  - ---
- МО анализа и ведения банка данных угроз безопасности информации в ИС
  - МО оценки рисков реализации угроз безопасности информации
    - Модели, алгоритмы и программные комплексы оценки ущербов от реализации угроз безопасности информации
    - Модели, алгоритмы и программные комплексы оценки возможностей реализации угроз безопасности информации в ИС, в том числе в условиях применения мер и средств ЗИ
  - Методики выявления актуальных угроз безопасности информации в различных классах ИС
  - МО ведения банка данных угроз безопасности информации
  - ---
- МО обоснования требований по ЗИ в ИС
  - МО категорирования и инвентаризации информационных ресурсов и классификации ИС по классам защищенности
  - МО оценки эффективности ЗИ
  - МО количественного обоснования требований по ЗИ и к мерам и средствам ЗИ
  - МО количественного обоснования требований системам защиты информации в ИС
  - МО количественного обоснования требований к SIEM-системам, SOC-, DLP-системам, и др.
  - ---
- МО построения систем защиты информации (СЗИ)
  - Методика выбора базового набора и компенсирующих мер для СЗИ
  - МО выбора средств для реализации требуемых технических мер ЗИ
  - МО построения СЗИ с различными принципами построения (централизованным, децентрализованным, смешанным)
  - МО построения SIEM-систем, SOC-систем, DLP-систем, и иных распределенных систем ЗИ
  - ---
- МО организации и ведения контроля эффективности ЗИ
  - Математические модели и методики выборочного контроля защищенности информации в ИС и эффективности ЗИ
  - Математические модели проведения аттестации ИС и сертификационных испытаний средств ЗИ информации
  - Математические модели выявления инцидентов безопасности информации в функционирующих ИС по результатам контроля
  - ---

Балльный метод оценки риска реализации угроз

Риск реализации угрозы ⇒ $R_u(t) = \overline{\zeta_u} \cdot P_u(t)$

$\overline{\zeta_u}$ - математическое ожидание возможного ущерба

$P_u(t)$ - Вероятность реализации угрозы за заданное время

Балльный метод

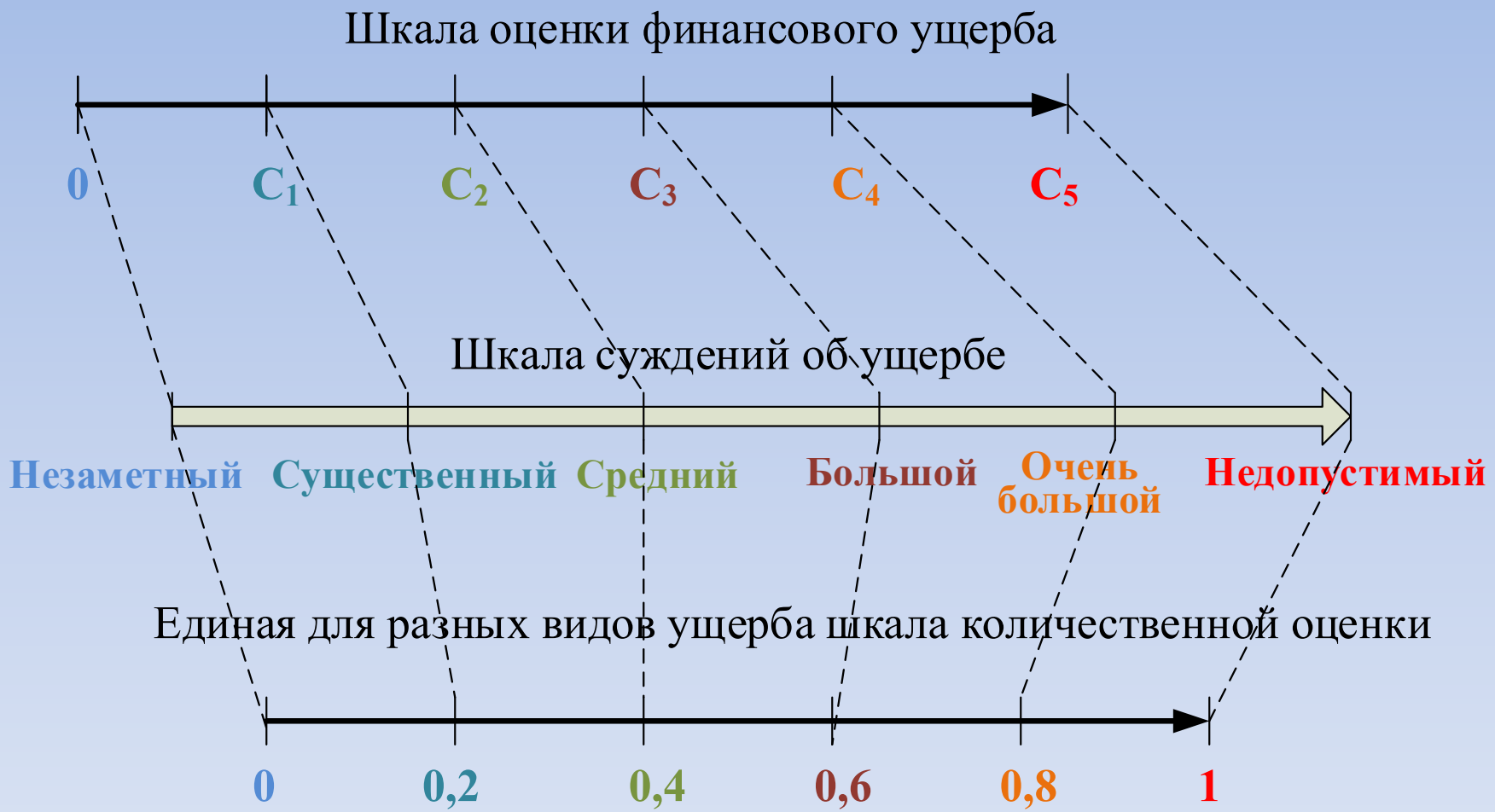
Программные продукты

COBRA	CRAMM (CCTA Risk Analysis & Management Method)	RiskWatch	---	АванГард

Пример формирования шкалы оценки ущерба

Вид ущерба	Величина ущерба в баллах			
	2 балла	---	6 баллов	10 баллов
Ущерб репутации организации	Негативная реакция отдельных чиновников, общественных деятелей		Критика в СМИ с последствиями в виде крупных скандалов, парламентских слушаний	Негативная реакция на уровне Президента и Правительства
Ущерб для здоровья персонала	Минимальный ущерб, не связанный с госпитализацией		Серьезные последствия (госпитализация, инвалидность и т.п.)	Гибель людей
Дезорганизация деятельности из-за недоступности данных	До 15 минут		От 1 часа до 3 часов	Более 1 суток

Единая для всех видов ущерба шкала оценки



Примечание: Оценка ущерба является условной, так как предельный ущерб отражает представление конкретного обладателя информации о ее важности для самого обладателя.

Формальные модели процессов реализации угроз

Формальные модели оценки возможностей реализации угроз безопасности информации

По средствам описания

- Аналитические модели
- Имитационные модели

По учету фактора времени

- Без учета времени (стационарные модели)
- С учетом фактора времени (динамические модели)

По фактору учета неопределенности условий и данных

- Детерминированные модели
- Модели, учитывающие факторы неопределенности

По виду учитываемой неопределенности

- Модели на основе теории субъективной вероятности
- Стохастические (вероятностные) модели
- Модели на основе теории нечетких множеств (нечетких чисел)

По используемому аппарату

- Формальные модели безопасности
- Нестохастические модели теории исследования операций
- Нестохастические модели теории игр
- Детерминированные модели на основе классических сетей Петри
- Детерминированные модели на основе теории конечных автоматов и логических сетей
- Функциональные математические модели
- Модели на основе реляционных языков логико-лингвистического описания (синтагматических сетей, RX-кодов, семантических сетей, и др.)
- Модели на основе использования предикатов и предикатных сетей
- Нестохастические эпидемиологические модели
- Графовые нестохастические модели

. . .

По используемому аппарату

- Модели на основе марковских процессов
- Модели на основе полумарковских процессов
- Модели на основе методов прогнозирования
- Вероятностные модели теории исследования операций и теории игр
- Модели на основе теории систем массового обслуживания
- Стохастические модели на сетях Петри
- Модели на основе аппарата сетей Петри-Маркова
- Стохастические эпидемиологические модели
- Модели на основе теории статистических решений (обнаружения, распознавания, различения)
- Графовые стохастические модели

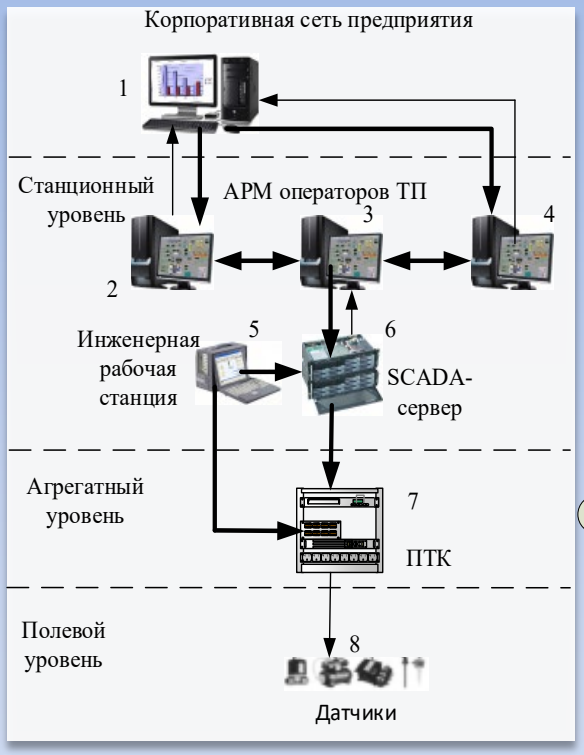
. . .

По приему моделирования

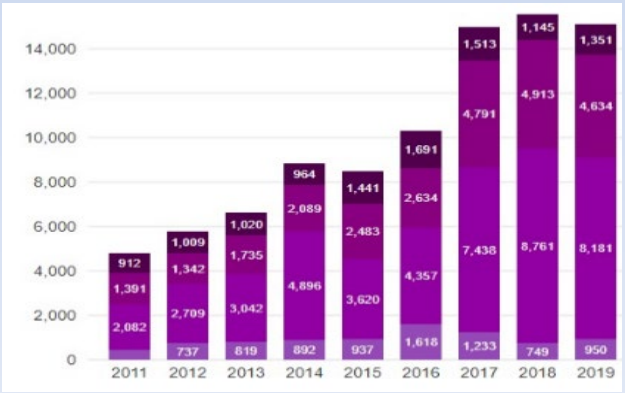
- Нечеткие модели на основе множества правил импликации (модели типа Мандами, Такаги-Сугено и др.)
- Иные нечеткие модели (самонастраивающиеся, самоорганизующиеся и т.д.)

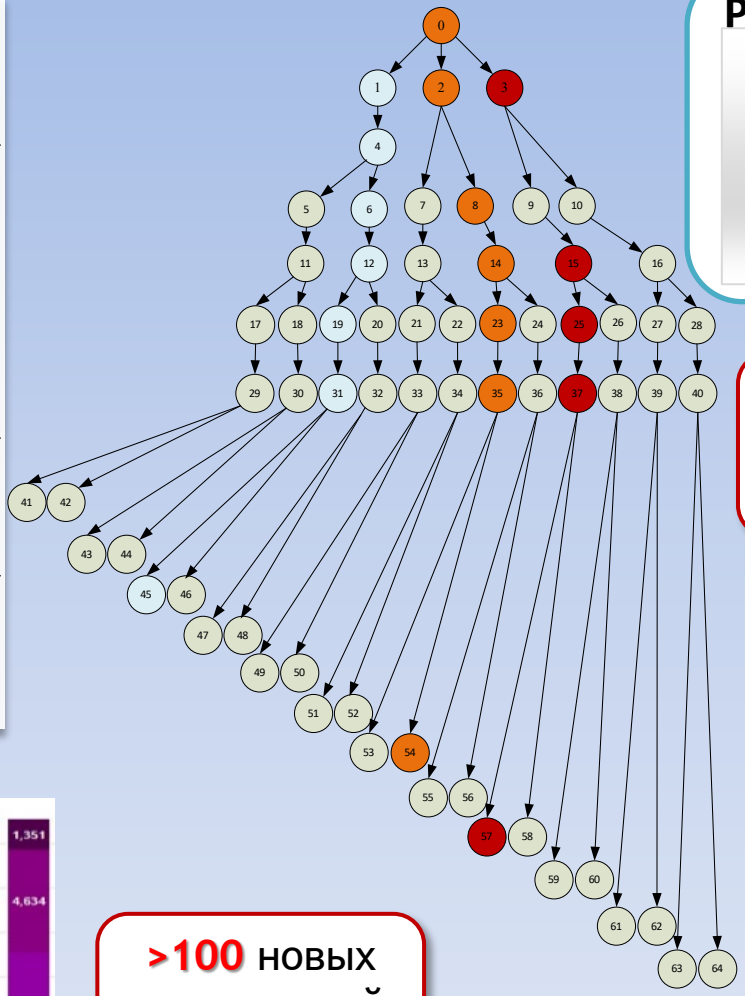
. . .

Рост размерности задачи анализа уязвимостей и угроз

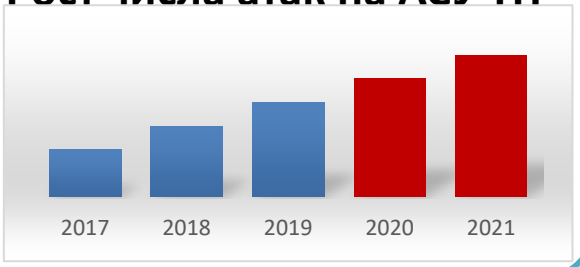


Рост числа уязвимостей по годам





Рост числа атак на АСУ ТП



>140 тысяч компьютерных атак за 2021 г.

Выбор из > **300** элементарных действий (техник) реализации атак.
Возможных комбинаций техник: > 10^5

>100 новых уязвимостей в неделю

Время анализа экспертом: > **100** дней

Порядок определения мер защиты информации в ИС
(на примере ГИС в соответствии с Приказом ФСТЭК России от 11.02.2013 г. №17)

Классификация ИС по классам защищенности

Определение состава актуальных угроз БИ

Выбор мер ЗИ

Определение базового набора мер по ЗИ для установленного класса ИС

→ Адаптация базового набора мер с учетом характеристик ИС, информационных технологий, особенностей функционирования ИС

→ Уточнение адаптированного базового набора мер ЗИ с учетом не выбранных ранее мер в интересах нейтрализации всех актуальных угроз

Дополнение уточненного адаптированного базового набора мер мерами, обеспечивающими выполнение требований к ЗИ, установленными иными нормативными правовыми актами

→ Разработка на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер иных (компенсирующих) мер, направленных на нейтрализацию актуальных угроз при невозможности технической реализации отдельных выбранных ранее мер

XXVII научно-практическая конференция «Комплексная защита информации»
с/п Дороховское, Московская обл., 25 – 26 мая 2022 г.

Ситуационный исследовательский центр

Исходная информация

Общедоступные источники

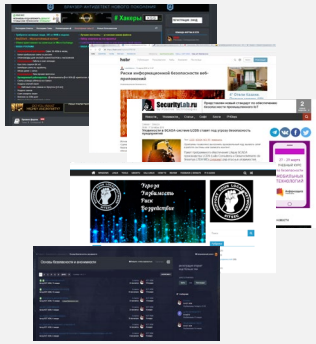
- Сайты разработчиков ПО
- Новостные сайты
- Сайты баз данных уязвимостей
- Сайты баз данных эксплойтов

Закрытые источники

- Сводки от ФОИВ
- Отчеты от исследовательских лабораторий

Дополнительные источники

- Форумы
- Блоги
- …



Подсистемы СИЦ

Подсистема мониторинга, сбора, анализа и обобщения данных об угрозах и уязвимостях

Подсистема прогнозирования угроз БИ и компьютерных атак

Подсистема анализа средств реализации компьютерных атак и эксплуатации уязвимостей

Подсистема ведения БДУ ФСТЭК России

Подсистема выявления уязвимостей в ПО

Подсистема организации устранения уязвимостей

Полигоны СИЦ

- Макеты типовых ГосИС
- Макеты АСУ ТП

Подсистема визуализации выходных результатов

Выходная информация

Прогнозы угроз БИ и компьютерных атак

Отчеты о НИР

ФСТЭК России

Описания угроз БИ

Паспорта известных уязвимостей

Паспорта уязвимостей «нулевого дня»

БДУ ФСТЭК России

Адрес сайта БДУ
BDU.fstec.ru

Адрес нового раздела по угрозам: BDU.fstec@fstec.ru/threat-section

Спасибо за внимание!

Язов Юрий Константинович