ФГБОУ ВО «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

НАУЧНО-ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ «РЕЛЯЦИОННЫЕ ЭКСПЕРТНЫЕ СИСТЕМЫ»

SOLUTIONS AND SERVICES

DataArt – ВОРОНЕЖ

ИНФОРМАЦИОННА КОМПАНИЯ "ИНФОРМСВЯЗЬ · ЧЕРНОЗЕМЬЕ"

XX Международная конференция «Информатика: проблемы, методы, технологии» (IPMT-2020) и XI школа-конференция «Информатика в образовании» (INED-2020)

Способ сетевого планирования аудита информационной безопасности объектов критической информационной инфраструктуры

Авторы:

Платов Николай Евгеньевич

Медведев Андрей Николаевич

Указ Президента РФ от 5 декабря 2016 г. N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"

IV. Стратегические цели и основные направления обеспечения информационной безопасности

*22. Стратегическими целями обеспечения информационной безопасности в области государственной и общественной безопасности являются … **защита критической информационной инфраструктуры.***

23. Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:
*в) **повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования**, …;*
*г) **повышение безопасности функционирования объектов информационной инфраструктуры**, …;*

*26. **Стратегической целью обеспечения информационной безопасности** в области науки, технологий и образования является **поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности**, ….*

V. Организационные основы обеспечения информационной безопасности

34. Деятельность государственных органов по обеспечению информационной безопасности основывается на следующих принципах:
*г) **достаточность сил** и средств обеспечения информационной безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз;*

35. Задачами государственных органов в рамках деятельности по обеспечению информационной безопасности являются:
*б) **оценка состояния информационной безопасности**, прогнозирование и обнаружение информационных угроз, **определение приоритетных направлений их предотвращения** и ликвидации последствий их проявления;*
*в) **планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности**;*
*г) **организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-розыскного**, разведывательного, контрразведывательного, научно-технического, **информационно-аналитического, кадрового** и экономического обеспечения;*

Приказ ФСТЭК № 239 от 25.12.2017 г. «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. Приказа ФСТЭК России от 26.03.2019 г. №60)

Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации (ПЛН.0)

Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации(ПЛН.1)

Контроль выполнения мероприятий по обеспечению защиты информации (ПЛН.2)

Регламентация правил и процедур аудита безопасности (АУД.0)

Федеральный закон РФ № 187-ФЗ от 26.07.2017 г. «О безопасности критической информационной инфраструктуры» (в ред. Федерального закона № 193-ФЗ от 26.07.17, № 194-ФЗ от 26.07.19)

Статья 6. Полномочия ... органов государственной власти Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры

3. ФОИВ, уполномоченный в области обеспечения безопасности КИИ Российской Федерации:

*5) **осуществляет государственный контроль** в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, а также утверждает форму акта проверки, составляемого по итогам проведения указанного контроля.*

4. ФОИВ, уполномоченный в области обеспечения функционирования государственной СОПКА на информационные ресурсы Российской Федерации:

*4) **организует и проводит оценку** безопасности критической информационной инфраструктуры;*

Статья 11. Требования по обеспечению безопасности значимых объектов КИИ.

1. Требования по обеспечению безопасности значимых объектов КИИ, устанавливаемые ФОИВ, уполномоченным в области обеспечения безопасности КИИ Российской Федерации, дифференцируются в зависимости от категории значимости объектов КИИ и этими требованиями предусматриваются:

*1) **планирование, разработка, совершенствование и осуществление внедрения мероприятий** по обеспечению безопасности значимых объектов КИИ;*

АНАЛИЗ МЕТОДОВ СЕТЕВОГО ПЛАНИРОВАНИЯ МЕРОПРИЯТИЙ

Методы сетевого планирования

1) Детерминированные сетевые методы

- Диаграмма Ганта с дополнительным временным люфтом 10-20 %
- Метод критического пути (МКП)

2) Вероятностные сетевые методы

Альтернативные

- Метод графической оценки и анализа (GERT)

Неальтернативные

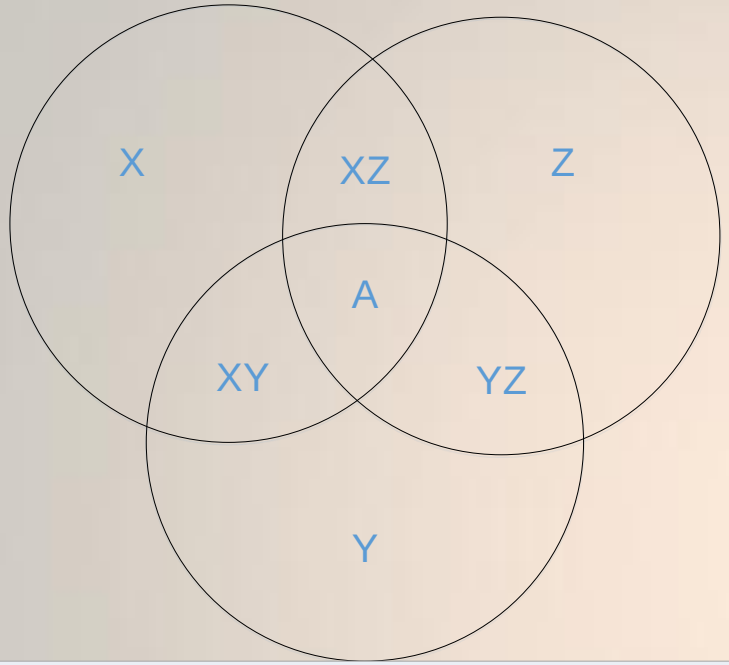
- Метод статистических испытаний (метод Монте-Карло)
- Метод оценки и пересмотра планов (ПЕРТ, PERT)

Стандарт / метод	Типы целей компьютерных атак										Проводимые мероприятия						
	Информация	Бизнес-процессы	Технические средства	Программное обеспечение	Каналы и сети	Персонал	Помещения	Организационная структура	Обеспечивающие системы	Третьи стороны	Интервьюирование	Опросные листы	Анализ документации	Физический осмотр	Анализ инцидентов	Использование инструментальных средств	Мозговой штурм
ISO/IEC серий 27000 и 31000	+	+	+	+	+	+	+	+	–	–	+	+	+	+	+	+	–
NIST SP 800 серии	+	+	+	+	+	+	–	–	–	–	+	+	+	–	+	+	–
РС БР ИББС-2.2-2009	+	+	+	+	+	–	+	–	–	–	+	+	–	–	–	–	–
MAGERIT	+	+	+	+	+	+	+	–	+	+	+	+	–	–	+	–	+
EBIOS	+	–	+	+	+	+	+	–	–	+	+	+	+	+	–	+	–
PCI DSS	+	+	+	+	+	+	–	–	–	–	+	+	–	–	+	–	–
OCTAVE	+	–	+	+	+	+	+	–	–	–	+	+	–	–	–	+	+
CRAMM	+	+	+	+	–	+	–	–	–	–	+	+	–	–	–	–	–
ГРИФ	+	+	+	+	+	+	–	+	–	–	+	+	–	–	–	–	–
RiskWatch	+	–	+	+	+	+	–	–	–	–	+	+	–	–	+	+	–
Microsoft	+	–	+	+	+	–	–	–	–	–	+	+	–	–	–	+	–

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СТАНДАРТОВ И МЕТОДОВ АНАЛИЗА РИСКОВ ИБ

Стандарт / метод	Виды оценки		Оценка вероятности события								Категории последствий					
			Параметры			Учитываемые факторы										
	Качественная	Количественная	Вероятность	Частота	Актуальность	Мотивация источника угроз	Возможности источника угроз	Осведомленность	Уязвимости	Реализованные защитные меры	Прямые материальные	Косвенные	Правовые	Репутационные	Ущерб жизни и здоровью	Ущерб окружающей среде
ISO/IEC серий 27000 и 31000	+	+	+	–	–	+	+	–	+	+	+	+	+	+	+	+
NIST SP 800 серии	+	+	+	–	–	+	+	–	+	+	+	+	–	+	+	–
РС БР ИББС-2.2-2009	+	+	+	–	–	+	+	–	–	+	+	+	+	+	–	–
BSI-Standard 100-3	+	–	–	–	+	–	–	–	–	+	–	–	–	–	–	–
MAGERIT	+	–	+	+	–	–	–	–	–	+	+	+	+	+	+	+
EBIOS	+	–	+	–	–	+	+	–	+	+	+	+	–	–	–	–
PCI DSS	+	+	+	–	–	+	+	–	+	+	+	–	–	–	–	–
OCTAVE	+	–	+	–	–	+	–	–	+	+	+	+	+	+	+	–
CRAMM	+	+	–	+	–	–	–	–	+	+	+	+	+	+	+	–
ГРИФ	+	+	+	–	–	–	–	–	+	+	+	–	–	–	–	–
RiskWatch	–	+	–	+	–	–	–	–	+	+	+	+	–	+	+	–
Microsoft	+	+	–	+	–	–	–	–	+	+	+	+	+	+	–	–

СПОСОБ СЕТЕВОГО ПЛАНИРОВАНИЯ АУДИТА ИБ



X – Множество стандартов и методов аудита и оценки рисков ИБ

Y – Множество методов СПУ, в которое входят элементы: метод критического пути и метод графической оценки и анализа (GERT))

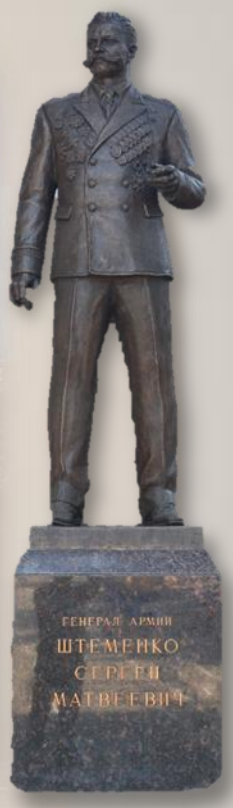
Z – Множество переменных отношения величины объёма аудита ИБ к количеству экспертов в составе комиссии

XY – подмножество зависимостей методов СПУ аудита ИБ от методов (стандартов) аудита и оценки рисков ИБ

YZ – подмножество зависимостей методов СПУ аудита ИБ от переменных отношения величины объёма аудита ИБ к количеству экспертов в составе комиссии

XZ – подмножество зависимостей методов (стандартов) аудита и оценки рисков ИБ от переменных отношения величины объёма аудита ИБ к количеству экспертов в составе комиссии

A – как элемент достижения способа проведения аудита ИБ



Спасибо за внимание