ВОЕННАЯ АКАДЕМИЯ СВЯЗИ

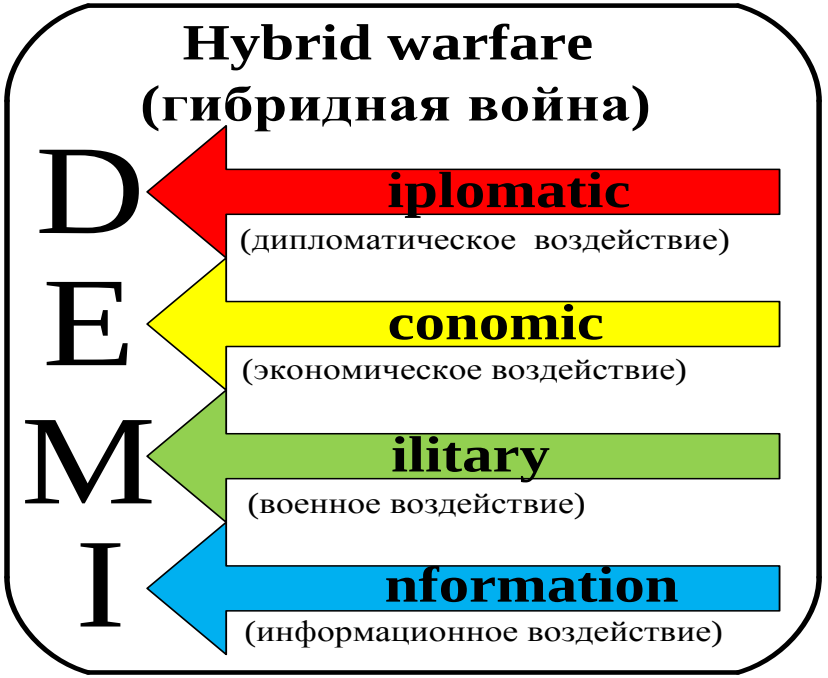
ПОДХОД К МОДЕЛИРОВАНИЮ КОМПЬЮТЕРНЫХ АТАК НА ОСНОВЕ СТОХАСТИЧЕСКИХ СЕТЕЙ

Преподаватель 32 кафедры
«Безопасности инфокоммуникационных систем специального назначения» Военной академии связи,
кандидат технических наук
ЛАУТА Олег Сергеевич

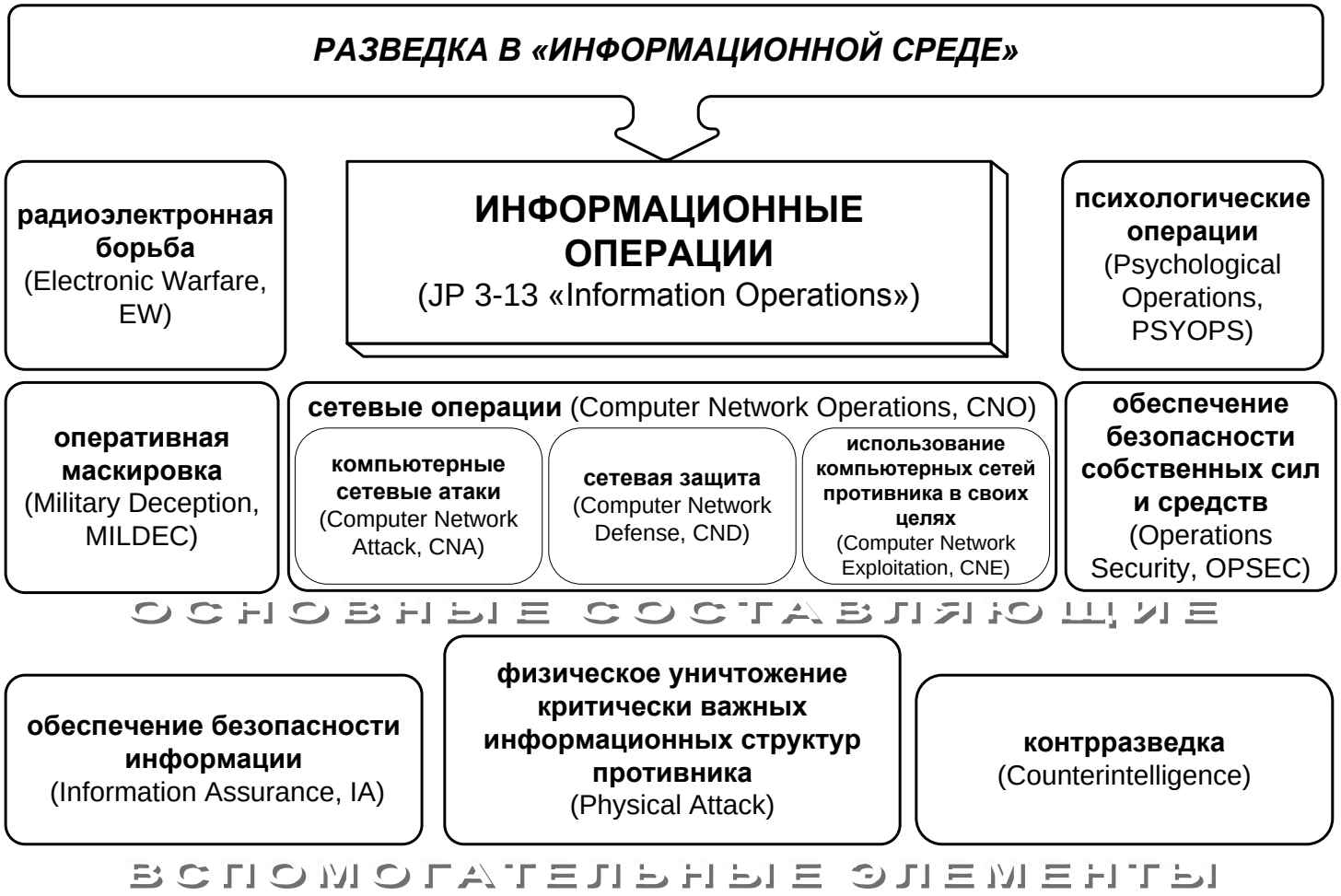
К определению понятия «гибридной» войны

Ведение гибридной войны в САР

Составные части «гибридной» войны:



Виды информационных операций (по взглядам зарубежных специалистов)



Виды основных компьютерных атак (1/3)

Вид компьютерной атаки	Способ реализации компьютерных атак	Область проявления
I. Техническая компьютерная разведка		
1.1 Анализ сетевого трафика.	1.1.1 Анализ пакетов данных на канальном уровне	Канал связи
	1.1.2 Анализ пакетов данных на сетевом уровне	
1.2 Сканирование сети и её уязвимостей.	1.2.1 Сканирование пакетом TCP с флагом SYN	Коммутатор Маршрутизатор ПЭВМ Серверы
	1.2.2 Сканирование пакетом TCP с флагом FIN	
	1.2.3 Сканирование пакетом TCP с флагом ACK	
	1.2.4 Сканирование пакетом TCP с флагом XMAS	
	1.2.5 Сканирование пакетом TCP с флагом NULL	
	1.2.6 Сканирование пакетом UDP	
	1.2.7 Сканирование пакетом ICMP	
1.3 Сканирование протоколов передачи данных сети.	1.3.1 Сканирование по протоколу RIP	Коммутатор Маршрутизатор ПЭВМ Серверы
	1.3.2 Сканирование по протоколу OSPF	
	1.3.3 Сканирование по протоколу SNMP	
	1.3.4 Сканирование по протоколу HTTP	
	1.3.5 Сканирование по протоколу SNMP	
	1.3.6 Сканирование по протоколу SAMBA	
	1.3.7 Сканирование по протоколу TELNET	
	1.3.8 Сканирование по протоколу POP3	
	1.3.9 Сканирование по протоколу NNTP	
	1.3.10 Сканирование по протоколу FINGER	
	1.3.11Сканирование по протоколу FTP	
	1.3.12 Сканирование по протоколу TFTP	
	1.3.13 Сканирование по протоколу RLOGIN	
	1.3.14 Сканирование по протоколу IDENT	
	1.3.15 Сканирование по протоколу IMAP	
	1.3.16 Сканирование по протоколу RPC	

Виды основных компьютерных атак (2/3)

II. Вредоносные коды		
2.1 Локальное проникновение в критически важный информационный сегмент	2.1.1 Ransomware	ПЭВМ Серверы
	2.1.2 Tollkit	
	2.1.3 Badware	
	2.1.4 Rootkit	
	2.1.5 Троянский конь	
	2.1.6 Spyware	
2.2 Удалённое проникновение в критически важный информационный сегмент	2.2.1 Knobe	ПЭВМ Серверы
	2.2.2 XML-бомба	
	2.2.3 Средства удаленного администрирования	
	2.2.4 Phishing	
	2.2.5 Атаки нулевого уровня	
	2.2.6 Browser Hijackers	
	2.2.7 Bot-коды	
III. Хищение, удаление и/или искажение информации		
3.1 Взлом паролей.	3.1.1 Вирусы изменения системных файлов	ПЭВМ Серверы
	3.1.2 Аппаратные закладки	
	3.1.3 Метод перебора данных в файлах SAM и SYSTEM	
	3.1.4 Программа сброса паролей	
	3.1.5 Программа взлома паролей	
	3.1.6 Программные закладки	
3.2 Ввод ложной информации.	3.2.1 Аппаратные закладки	ПЭВМ Серверы
	3.2.2 Программные закладки	
3.3 Проникновение в спец. базы данных и размещение ложной информации	3.2.3 Средства удаленного администрирования	
	3.2.4 Вирусы	
	3.2.5 Хищение удаленных файлов «Нортон-утилитами»	
3.4 Разрушение информации и программного обеспечения	3.2.6 Несанкционированный доступ и воровство жесткого диска	

Виды основных компьютерных атак (3/3)

IV. Отказ в обслуживании		
4.1 Локальный отказ в обслуживании.	4.1.1 «Тяжелый пакет»	Маршрутизатор Коммутатор ПЭВМ Серверы
	4.1.2 Mac-flooding	
4.2 Удалённый отказ в обслуживании.	4.1.3 Smurf	
	4.1.4 Fraggle	
	4.1.5 SYN-flooding	
4.3 «Спам».	4.3.1 Рассылка большого числа пакетов сообщений	ПЭВМ Сервер
4.4 Логическое отключение абонентов	4.4.1 Перехват IP	ПЭВМ
V. Перенаправление трафика		
5.1 Логическая подмена сервера.	5.1.1 Запросы по протоколу RIP	Маршрутизатор ПЭВМ Серверы
	5.1.2 Запросы по протоколу OSPF	
5.2 Перенаправление пакетов данных	5.1.3 Запросы по протоколу SNMP	
	5.1.4 Запросы по протоколу ICMP	
	5.1.5 Запросы по протоколу SAP	
	5.1.6 Запросы по протоколу ARP	
	5.1.7 Запросы по протоколу DNS	
	5.1.8 Передача заранее подготовленного ложного ответа	

Профильная модель КА типа «Анализ сетевого трафика»

- запуск аппаратно-программного комплекса (сетевого сканера) за среднее время $\overline{t}_{зап}$ с функцией распределения времени *W(t)*;
- ввод параметров, определяющих перехват информации за среднее время $\overline{t}_{инф}$ с функцией распределения времени *M(t)*;
- перехват информации с вероятностью P_n за среднее время $\overline{t}_{пер}$, с функцией распределения времени *L(t)*;
- статистический анализ и подготовка отчета за среднее время $\overline{t}_{стат.анализ}$ с функцией распределения времени *D(t)*;

Если информация не перехвачена, то с вероятностью $(1\text{-}P_n)$ сетевой сканер запускается повторно за среднее время $\overline{t}_{повт}$ и функцией распределения времени *Z(t)*.

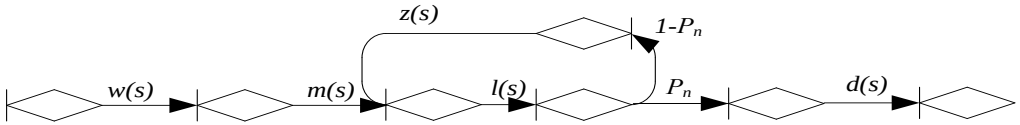
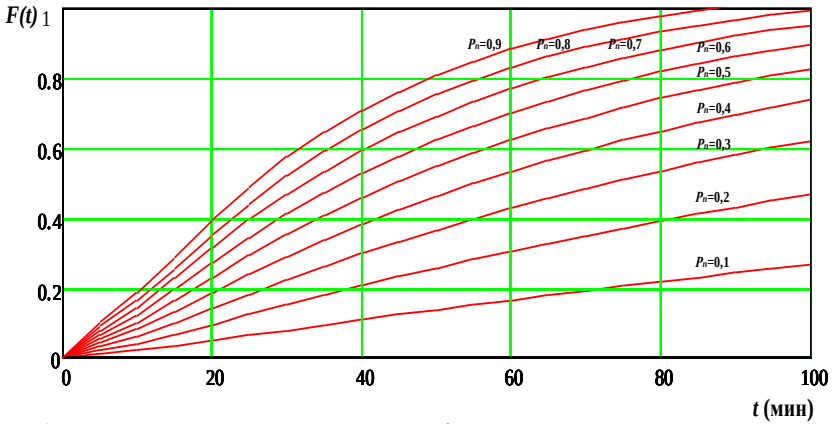
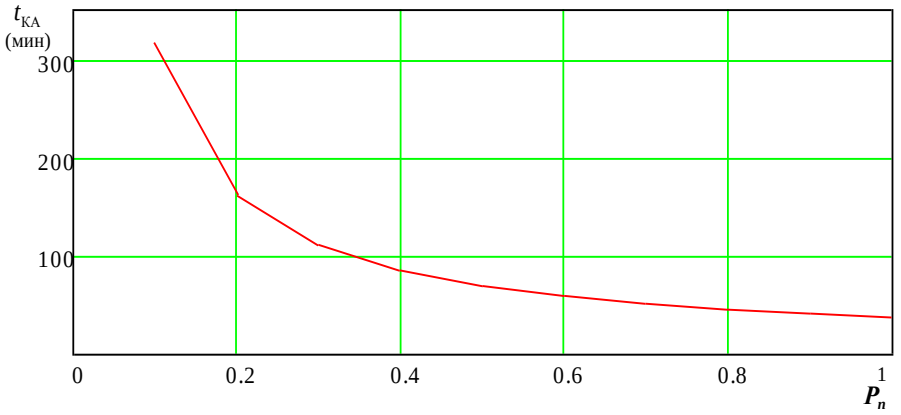


Рисунок 1 - Стохастическая сеть компьютерной атаки типа «Анализ сетевого трафика»



а) зависимость интегральнои функции распределения вероятности от времени реализации компьютерной атаки



б) зависимость среднего времени от вероятности реализации компьютерной атаки

Рисунок 2 - Вероятностно-временные характеристики компьютерной атаки типа «Анализ сетевого трафика»

Результаты моделирования основных КА (1/3)

Номер Группы	Способ реализации компьютерных атак	Рекуррентные выражения для расчета ВВХ	Результаты расчетов $\overline{t_{КА}}$ (мин) при $P_n=0,8$	Результаты расчетов $F(t)$ при $P_n=0,8$
1	1.1.1 Анализ пакетов данных на канальном уровне	$F(t)=\sum_{k=1}^{5}\frac{w\cdot m\cdot P_n\cdot d\cdot l\cdot(z+s_k)}{\varphi'(s_k)}\cdot\frac{1-\exp[s_k t]}{-s_k}$ $\overline{t_{КА}}=\sum_{k=1}^{5}\frac{w\cdot m\cdot P_n\cdot d\cdot l\cdot(z+s_k)}{\varphi'(s_k)}\cdot\frac{1}{(-s_k)^2}$	25	0,8
	1.1.2 Анализ пакетов данных на сетевом уровне		25	0,8
	1.2.1 Сканирование пакетом TCP с флагом SYN		5	0,7
	1.2.2 Сканирование пакетом TCP с флагом FIN		5	0,7
	1.2.3 Сканирование пакетом TCP с флагом ACK		5	0,7
	1.2.4 Сканирование пакетом TCP с флагом XMAS		5	0,7
	1.2.5 Сканирование пакетом TCP с флагом NULL		5	0,7
	1.2.6 Сканирование пакетом UDP		5	0,7
	1.2.7 Сканирование пакетом ICMP		5	0,7
	2.1.1 Ransomware		30	0,75
	2.1.3 Badware		25	0,7
	2.1.4 Rootkit		27	0,6
	2.1.6 Spyware		32	0,65
	2.2.1 Knobe		7	0,65
	2.2.2 XML-бомба		13	0,71
	2.2.3 Средства удаленного администрирования		5	0,54
	2.2.4 Phishing		10	0,62
	2.2.5 Атаки нулевого уровня		11	0,67
	2.2.6 BrowserHijackers		8	0,54
	2.2.7 Bot-коды		7	0,6
	3.1.4 Программа сброса паролей		10	0,63
	3.2.4 Хищение удаленных файлов «Нортон-утилитами»		6	0,73
	3.2.5 Несанкционированный доступ и воровство жесткого диска		17	0,7
	4.3.1 Рассылка большого числа пакетов сообщений		10	0,6
	4.4.1 Перехват IP		8	0,58

Результаты моделирования основных КА (2/3)

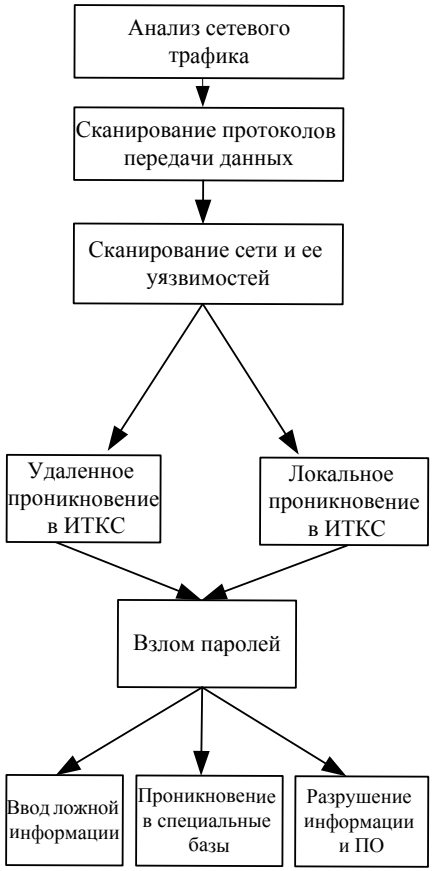
2	1.3.1 Сканирование по протоколу RIP	$F(t)=\sum_{k=1}^{4}\frac{w\cdot P_n\cdot m\cdot d\cdot(z+s_k)}{\varphi'(s_k)}\cdot\frac{1-\exp[s_k t]}{-s_k}$ $\overline{t_{KA}}=\sum_{k=1}^{4}\frac{w\cdot P_n\cdot m\cdot d\cdot(z+s_k)}{\varphi'(s_k)}\cdot\frac{1}{(-s_k)^2}$	6	0,68
	1.3.2 Сканирование по протоколу OSPF		6	0,68
	1.3.3 Сканирование по протоколу SNMP		6	0,68
	1.3.4 Сканирование по протоколу HTTP		6	0,68
	1.3.5 Сканирование по протоколу SNMP		6	0,68
	1.3.6 Сканирование по протоколу SAMBA		6	0,68
	1.3.7 Сканирование по протоколу TELNET		6	0,68
	1.3.8 Сканирование по протоколу POP3		6	0,68
	1.3.9 Сканирование по протоколу NNTP		6	0,68
	1.3.10 Сканирование по протоколу FINGER		6	0,68
	1.3.11 Сканирование по протоколу FTP		6	0,68
	1.3.12 Сканирование по протоколу TFTP		6	0,68
	1.3.13 Сканирование по протоколу RLOGIN		6	0,68
	1.3.14 Сканирование по протоколу IDENT		6	0,68
	1.3.15 Сканирование по протоколу IMAP		6	0,68
	1.3.16 Сканирование по протоколу RPC		6	0,68
	3.1.1 Вирусы изменения системных файлов		16	0,52
	3.1.2 Аппаратные закладки		16	0,55
	3.1.5 Программа взлома паролей		35	0,61
	3.1.6 Программные закладки		16	0,52
	4.1.1 «Тяжелый пакет»		6	0,7
	4.1.2 Mac-flooding		12	0,7
	4.1.3 Smurf		12	0,7
	4.1.4 Fraggle		12	0,7
	4.1.5 SYN-flooding		12	0,7
	Доразведка		8	0,6

Результаты моделирования основных КА (3/3)

3	2.1.2 Tollkit	$F(t) = \sum_{k=1}^{6} \frac{w \cdot m \cdot P_n \cdot d \cdot l \cdot q \cdot (z + s_k)}{\varphi'(s_k)} \cdot \frac{1 - \exp[s_k t]}{-s_k}$ $\overline{t_{KA}} = \sum_{k=1}^{6} \frac{w \cdot m \cdot P_n \cdot d \cdot l \cdot q \cdot (z + s_k)}{\varphi'(s_k)} \cdot \frac{1}{(-s_k)^2}$	15	0,65
	2.1.5 Троянский конь		18	0,72
	5.1.1 Запросы по протоколу RIP		10	0,55
	5.1.2 Запросы по протоколу OSPF		10	0,55
	5.1.3 Запросы по протоколу SNMP		10	0,55
	5.1.4 Запросы по протоколу ICMP		10	0,55
	5.1.5 Запросы по протоколу SAP		10	0,55
	5.1.6 Запросы по протоколу ARP		10	0,55
	5.1.7 Запросы по протоколу DNS		10	0,55
	5.1.8 Передача заранее подготовленного ложного ответа		8	0,6
4	3.1.3 Метод перебора данных в файлах SAM и SYSTEM	$F(t) = \sum_{k=1}^{8} \frac{P_н \cdot w \cdot o \cdot P_n^3 \cdot h \cdot b \cdot q \cdot d \cdot m \cdot (z + s_k)^3}{\varphi'(s_k)} \cdot \frac{1 - \exp[s_k t]}{-s_k}$ $\overline{t_{KA}} = \sum_{k=1}^{8} \frac{P_н \cdot w \cdot o \cdot P_n^3 \cdot h \cdot b \cdot q \cdot d \cdot m \cdot (z + s_k)^3}{\varphi'(s_k)} \cdot \frac{1}{(-s_k)^2}$	25	0,7
5	Комплекс ТКР	$F(t) = \sum_{k=1}^{8} \frac{w \cdot l \cdot m \cdot b \cdot d \cdot n \cdot [(o + s_k) \cdot P_П + (1 - P_П) \cdot o \times}{\varphi'(s)}$ $\frac{\times[(z+s_k) \cdot P_{КТ} + (1-P_{КТ}) \cdot z \cdot P_M]]}{} \cdot \frac{1 - \exp[s_k t]}{-s_k}$ $\overline{t_{KA}} = \sum_{k=1}^{8} \frac{w \cdot l \cdot m \cdot b \cdot d \cdot n \cdot [(o + s_k) \cdot P_П + (1 - P_П) \cdot o \times}{\varphi'(s)}$ $\frac{\times[(z+s_k) \cdot P_{КТ} + (1-P_{КТ}) \cdot z \cdot P_M]]}{} \cdot \frac{1}{(-s_k)^2}$	210	1

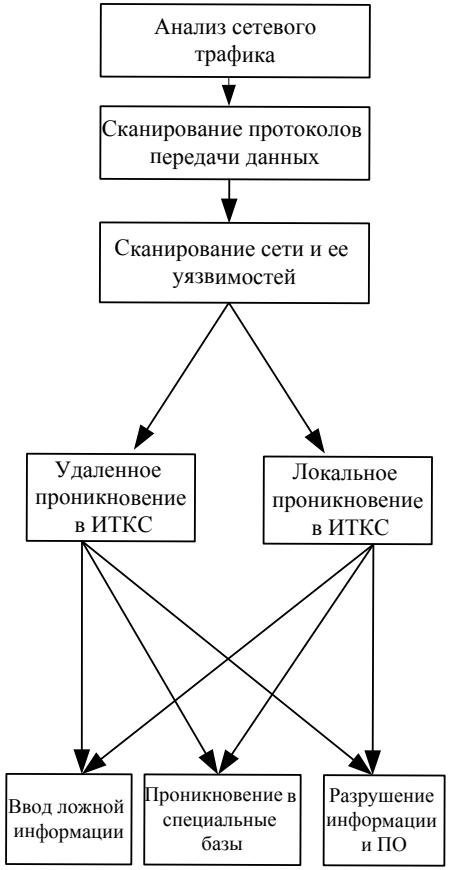
Профильные модели комплексных КА (1/2)

Хищение, удаление и/или искажение информации



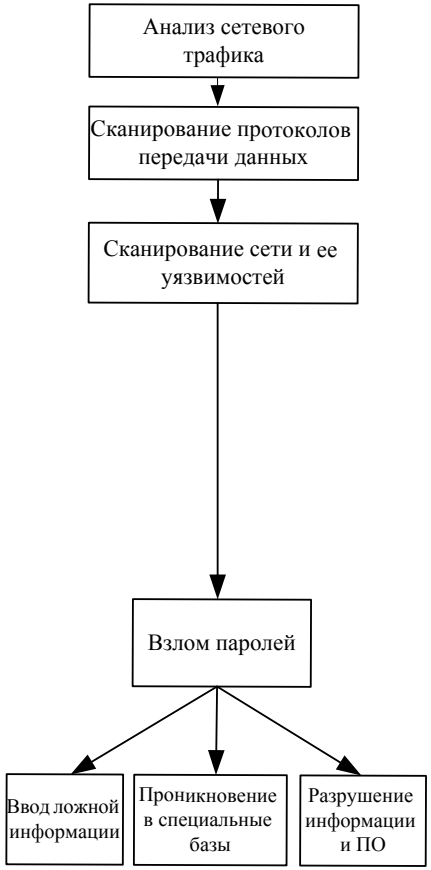
Последовательно: $\overline{t_{КА}} = 23$ мин $F(t)=0,6$

Параллельно: $\overline{t_{КА}} = 18$ мин. $F(t)=0,8$



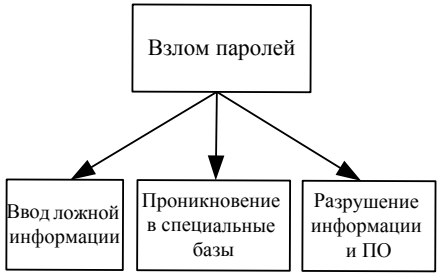
Последовательно: $\overline{t_{КА}} = 21$ мин. $F(t)=0,63$

Параллельно: $\overline{t_{КА}} = 17$ мин. $F(t)=0,67$



Последовательно: $\overline{t_{КА}} = 19$ мин. $F(t)=0,63$

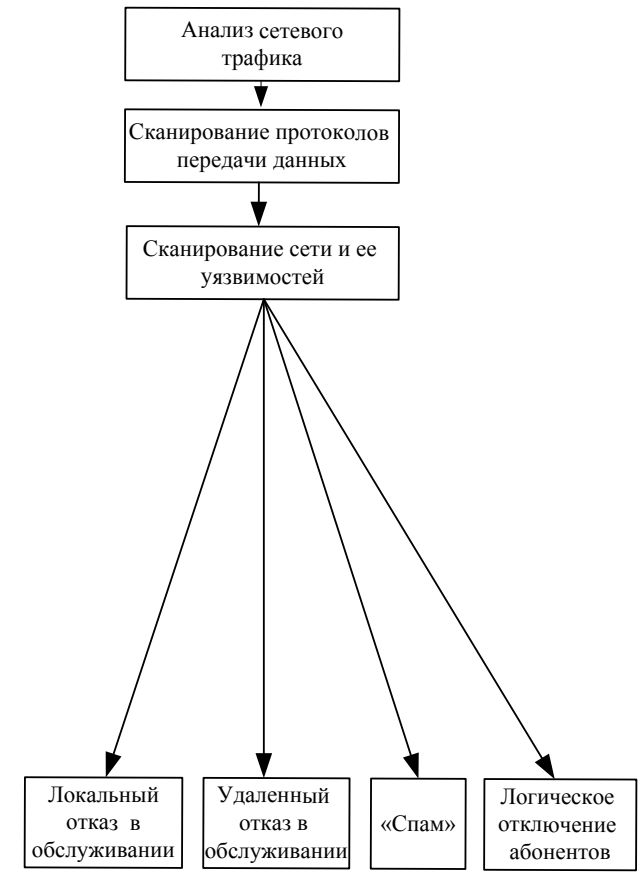
Параллельно: $\overline{t_{КА}} = 15$ мин. $F(t)=0,67$



Последовательно: $\overline{t_{КА}} = 8$ мин. $F(t)=0,81$

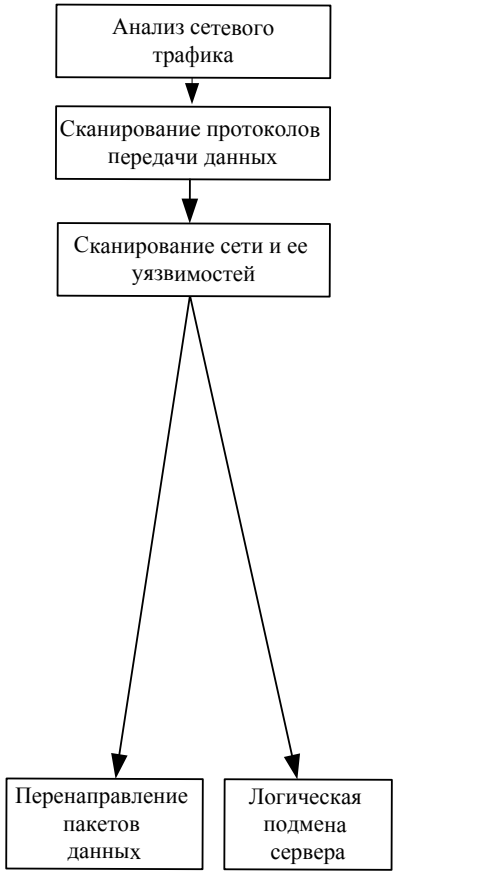
Профильные модели комплексных КА (2/2)

Отказ в обслуживании и перенаправление трафика



Последовательно: $\overline{t_{КА}} = 22$ мин. $F(t)=0,65$

Параллельно: $\overline{t_{КА}} = 17$ мин. $F(t)=0,7$



Последовательно: $\overline{t_{КА}} = 22$ мин. $F(t)=0,7$

Параллельно: $\overline{t_{КА}} = 17$ мин. $F(t)=0,73$

Результаты моделирования комплексных КА

№ п/п	Цели воздействия	Последовательность реализации КА	(мин)		F(t)	
			послед	парал	послед	парал
	Хищение, удаление и/или искажение информации	1. Анализ сетевого трафика; 2. Сканирование протоколов передачи данных; 3. Сканирование сети и ее уязвимостей; 4. Проникновение в ИТКС ОЗУ; 5. Взлом паролей; 6. Хищение, удаление и/или искажение информации.	23	18	0,6	0,8
		1. Анализ сетевого трафика; 2. Сканирование протоколов передачи данных; 3. Сканирование сети и ее уязвимостей; 4. Проникновение в ИТКС ОЗУ; 5. Хищение, удаление и/или искажение информации.	20	16	0,63	0,67
		1. Анализ сетевого трафика; 2. Сканирование протоколов передачи данных; 3. Сканирование сети и ее уязвимостей; 4. Взлом паролей; 5. Хищение, удаление и/или искажение информации.	20	16	0,63	0,67
		1. Взлом паролей; 2. Хищение, удаление и/или искажение информации.	8		0,81	
		1. Хищение, удаление и/или искажение информации.	1,5		0,55	
	Отказ в обслуживании	1. Анализ сетевого трафика 2. Сканирование протоколов передачи данных 3. Сканирование сети и ее уязвимостей 4. Отказ в обслуживании	22	17	0,65	0,7
		1. Отказ в обслуживании	2,5		0,63	
	Перенаправление трафика	1. Анализ сетевого трафика 2. Сканирование протоколов передачи данных 3. Сканирование сети и ее уязвимостей 4. Перенаправление трафика	22	17	0,7	0,73
		1. Перенаправление трафика	1,5		0,5	

Оценка киберустойчивости ИТКС на основе стохастического моделирования КА

Цель: разработка научно-методического аппарата обеспечения устойчивости ИТКС в условиях сетевых компьютерных атак.

Назначение: оценка устойчивости ИТКС в условиях комплексного воздействия компьютерных атак.

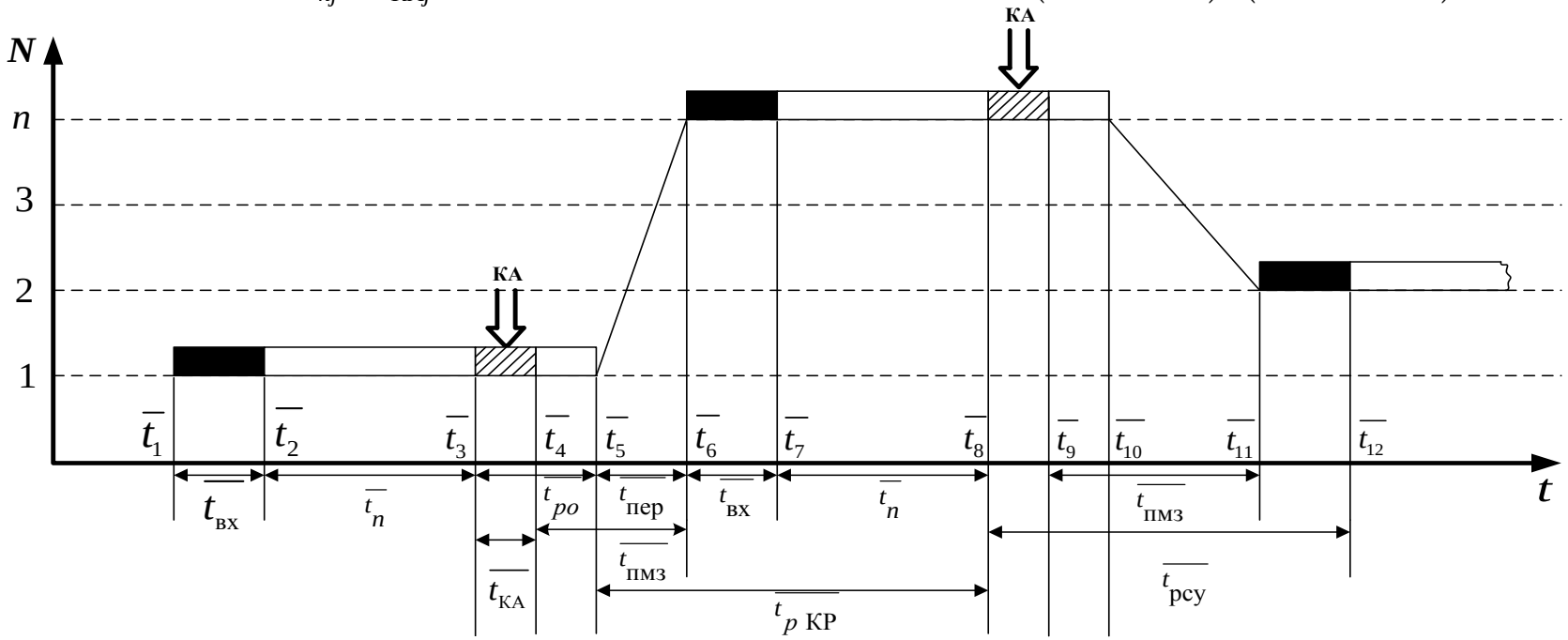
Структура методики

1. Ввод исходных данных
2. Определение вероятностно-временных характеристик компьютерных атак
3. Определение вероятностно-временных характеристик эквивалентных компьютерных атак
4. Определение коэффициента связности *i*-го информационного направления связи
   - 4.1 Определение веса *j*-го маршрута в информационном обмене ИНС
5. Определение коэффициента исправного действия *i*-го информационного направления связи
   - 5.1 Определение коэффициента исправного действия *j*-го маршрута
   - 5.2 Определение вероятности воздействия на *j*-ый маршрут
6. Определение коэффициента связности ИТКС
   - 6.1 Определение веса *i*-го ИНС в информационном обмене ИТКС
7. Определение коэффициента исправного действия ИТКС
8. Вывод результатов

Основные математические выражения для оценки киберустойчивости ИТКС (1/2)

$$K_{\text{икуМ}j} = \frac{\overline{t}_{nj}}{\overline{t}_{nj} + \overline{t}_{\text{КА}j}} \qquad (1)$$

$$P_{\text{возд}} = 1 - \frac{\overline{t}^{\,2}_{\text{р КР}j}}{\left(\overline{t}_{\text{р КР}j} + \overline{t}_{\text{вх}j}\right) \cdot \left(\overline{t}_{\text{р КР}j} + \overline{t}_{\text{пмз }j}\right)} \qquad (2)$$



$\overline{t}_{\text{вх}}$ - среднее время вхождения в связь операторами ИТКС;

$\overline{t}_{\text{КА}}$ - среднее время воздействия КА;

$\overline{t}_n$ - среднее время передачи полезной информации;

$\overline{t}_{\text{пмз}} = \overline{t}_{\text{пер}} + \overline{t}_{\text{ро}}$ - среднее время принятия мер защиты;

$\overline{t}_{\text{ро}}$ - среднее время реакции операторов по обнаружению КА;

$\overline{t}_{р\ \text{КР}}$ - среднее время реакции комплекса КР

$\overline{t}_{\text{пер}}$ - среднее время перехода на новый маршрут;

Основные математические выражения для оценки киберустойчивости ИТКС (2/2)

$$K_{\text{иИТКС}} = K_{\text{и жИТКС}} \cdot K_{\text{и пуИТКС}} \cdot K_{\text{и нИТКС}} \cdot K_{\text{и куИТКС}}. \quad (1)$$

$$K_{\text{икуИТКС}} = K_{\text{свИТКС}} \cdot \left(1 - \left[\left(\prod_{i=1}^{M}\left(1 - K_{\text{иНС}i}\right)\right)\right]\right); \quad (2)$$

$$K_{\text{икуНС}i} = K_{\text{свНС}i} \cdot \left(1 - \left[\left(\prod_{j=1}^{N}\left(\left(1 - K_{\text{иСМ}j}\right) \cdot P_{\text{возд}}\right)\right)\right]\right); \quad (3)$$

$K_{\text{икуСМ}j} = \prod_{j=1}^{O} K_{\text{икуМ}j}$ – коэффициент исправного действия составного маршрута; (4)

$K_{\text{свИНС}i} = \frac{1}{M} \cdot \sum_{i=1}^{M} \alpha_j \left(\frac{H_j}{M+O} + \frac{O}{M}\right)$ – коэффициент связности *i*-го НС; (5)

$K_{\text{свИТКС}} = \frac{1}{N} \cdot \sum_{i=1}^{N} \alpha_i \left(\frac{G_i}{N+M_i} + \frac{M_i}{N}\right)$ – коэффициент связности ИТКС. (6)

Результаты оценки киберустойчивости ИТКС

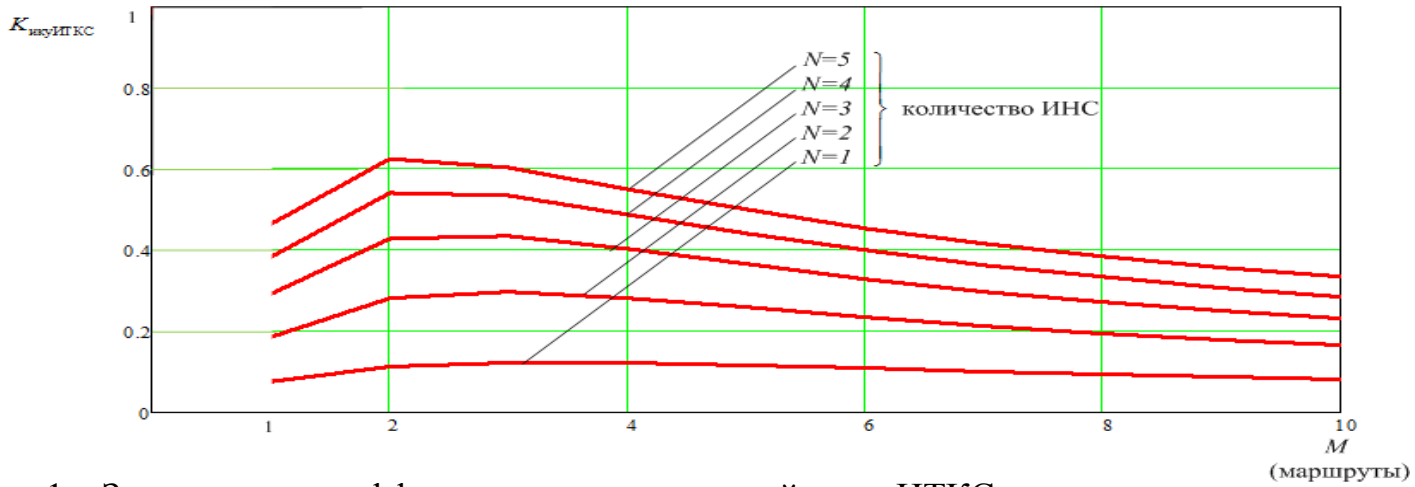


Рисунок 1 – Зависимость коэффициента исправного действия ИТКС от количества маршрутов и НС

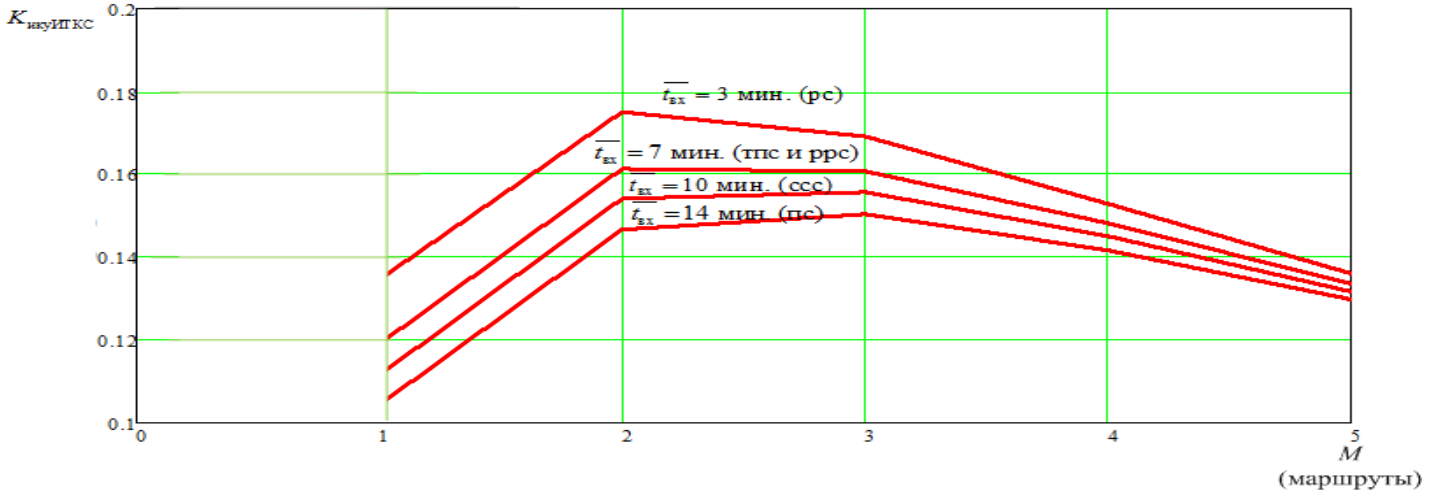


Рисунок 2 – Зависимость коэффициента исправного действия ИТКС от количества маршрутов и времени вхождения в связь

Заключение

1. С точки зрения оперативности, рассмотренные атаки можно сгруппировать как КА, у которых среднее время реализации до 15 мин и выше. К КА, реализуемым до 15 минут, относятся финитные КА, а к реализуемым свыше 15 минут относятся те, которые позволяют изучить противнику логику работы ИТКС, конфигурацию программно-аппаратного обеспечения и организовать канал утечки.

2. Коэффициент исправного действия ИТКС принимает рациональное значение при использовании для передачи информации от 2 до 5 маршрутов в направлении связи, а маршруты должны включать не более одного интервала.

3. Маршруты, образованные радиосредствами, обладают наибольшей оперативностью, в связи с чем для них коэффициент исправного действия принимает максимальное значение.

СПАСИБО ЗА ВНИМАНИЕ!