Краснодарское высшее военное училище имени генерала армии С.М.Штеменко

«ОПРЕДЕЛЕНИЕ ОПТИМАЛЬНЫХ ПАРАМЕТРОВ ПРОАКТИВНОЙ ЗАЩИТЫ СЕРВИСА ЭЛЕКТРОННОЙ ПОЧТЫ ОТ СЕТЕВОЙ РАЗВЕДКИ»

Докладчик: Горбачев Александр Александрович

СТРАТЕГИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РФ
утверждена указом Президента РФ от 31.12.2015 г. № 683.

43. Основными угрозами государственной и общественной безопасности являются:

…….нарушения безопасности и устойчивости функционирования критической информационной инфраструктуры Российской Федерации;

113. При реализации настоящей Стратегии особое внимание уделяется обеспечению информационной безопасности с учетом стратегических национальных приоритетов.

ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
утверждена указом Президента РФ от 05.12.2016 г. № 646.

III. Основные информационные угрозы и состояние информационной безопасности

11. Одним из основных негативных факторов, влияющих на состояние информационной безопасности, является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях.

Одновременно с этим усиливается деятельность организаций, осуществляющих ТР в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса.

IV. Стратегические цели и основные направления обеспечения информационной безопасности

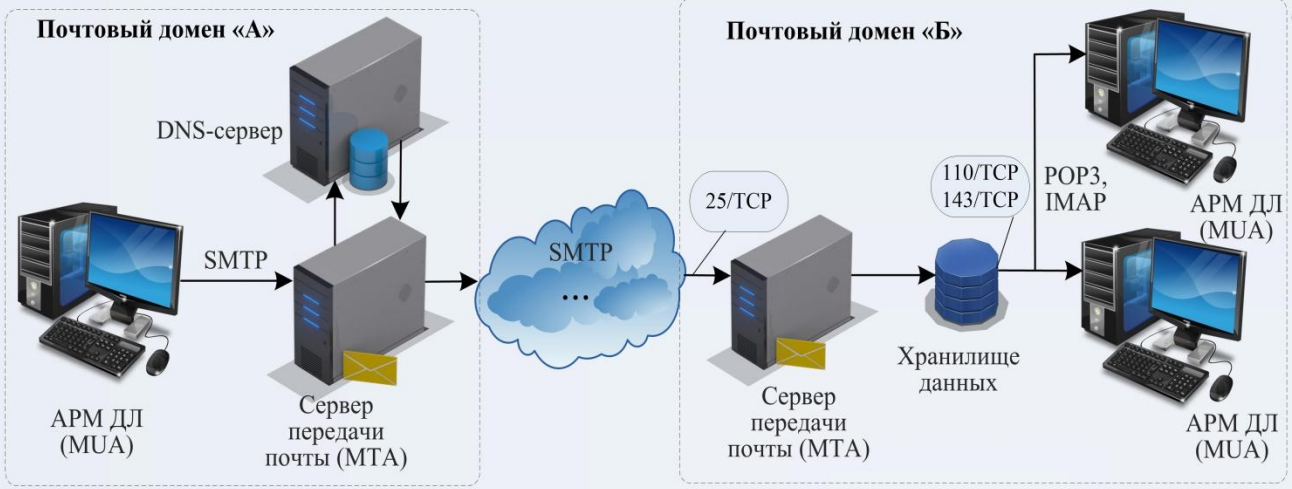
21. В соответствии с военной политикой Российской Федерации основными направлениями обеспечения информационной безопасности в области обороны страны являются:

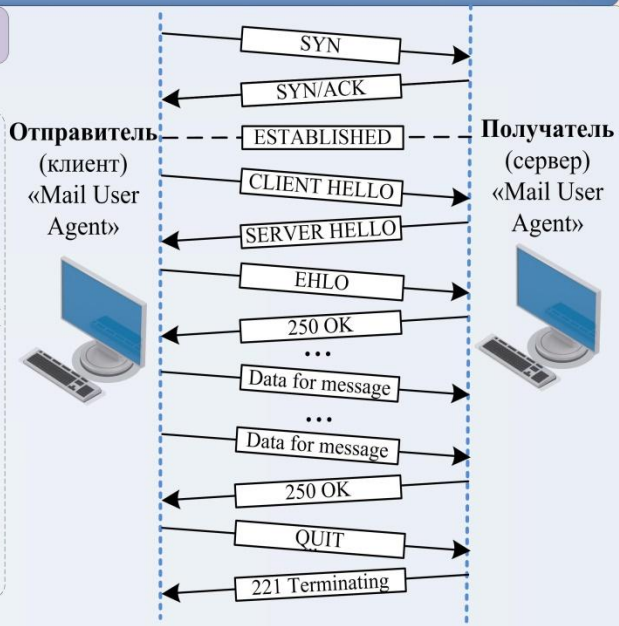
б) совершенствование системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства;

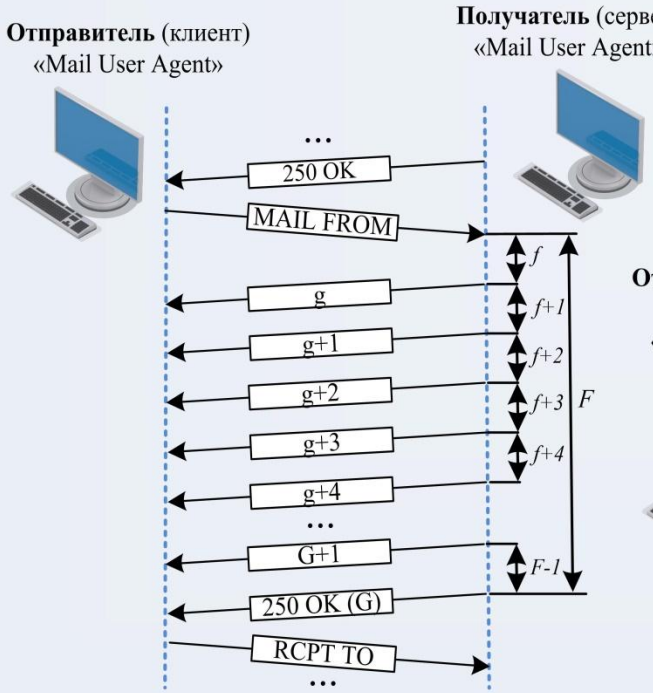
23. Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

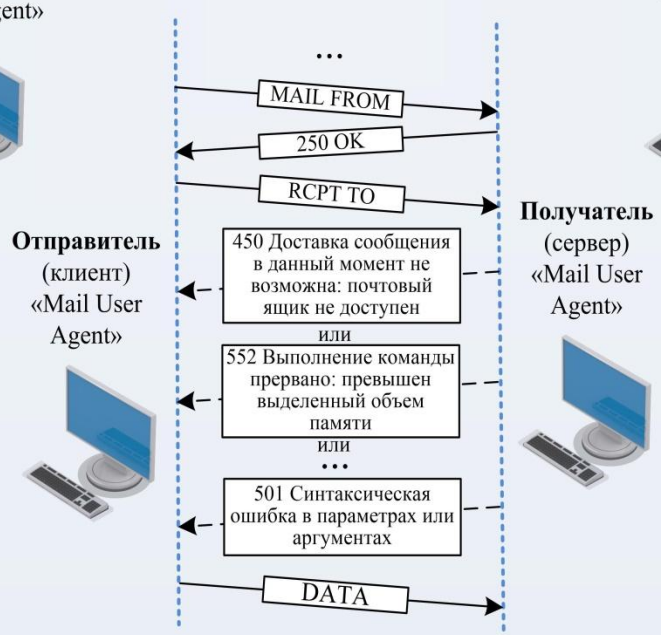
в) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и …

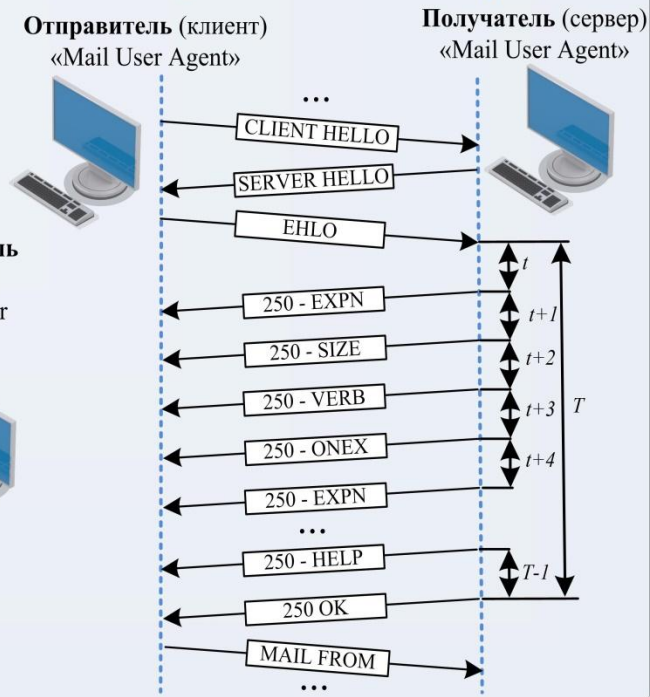
Проактивные средства защиты информационных систем











ФОРМАЛИЗОВАННАЯ ПОСТАНОВКА ЗАДАЧИ

S – моделируемая **система** (сервис электронной почты информационных систем военного назначения), характеризующаяся **внутренними параметрами** S_i и Λ_{ij}

$S_i = \{S_1, \ldots, S_9\}$, (1)
если случайный процесс - **марковский**, то:
$\Lambda_{ij} = \{\lambda_{11}, \lambda_{12}, \ldots, \lambda_{99}\}$,
если случайный процесс - **полумарковский**, то:
$\Lambda_{ij} = \{F_{11}(t), F_{12}(t), \ldots, F_{99}(t)\}$,
где S_i – состояния сервиса электронной почты, характеризующие этап процесса передачи сообщений электронной почты;
λ_{ij} – интенсивности потоков событий, инициирующие переход из состояния i в состояние j;
$F_{ij}(t)$ – функции распределения времени ожидания наступления событий, инициирующих переход системы из состояния i в состояние j.

$x(t)$ – **вектор фазовых переменных** системы S

$x(t)=\{p_1(t), p_2(t), \ldots, p_9(t)\}$, где $p_i(t)$ – вероятность пребывания системы в состоянии i в момент времени t. (2)

$u(t)$ – **вектор управлений**, представляющий собой интенсивности потоков событий, посредством которых осуществляются управляющие воздействия на вектор фазовых переменных $x(t)$ системы S

$u(t)=\{u_1(t), u_2(t), u_3(t), u_4(t)\}$, (3)
$u_1(t)=\lambda_{43}(t)=1/(d\cdot T)$, $u_2(t)=\lambda_{45}(t)=1/(d\cdot T)$, (4)
$u_3(t)=\lambda_{67}(t)=1/(n\cdot m\cdot T)$, $u_4(t)=\lambda_{88}(t)=1/(m\cdot F)$, (5)
где : $T = [0, 2, \ldots, 10]$ – значение времени задержки промежуточных откликов от сервера электронной почты на команды клиента, [с];
$d = [1, \ldots, 1000]$ – общее количество ответных промежуточных откликов, которые будут направлены клиенту от сервера электронной почты, [шт];
$n = [1, \ldots, 100]$ – общее количество ответных откликов, от сервера электронной почты на команды клиента, содержащих сообщения об ошибках, [шт];
$m = [1, \ldots, 1000]$ – общее количество фрагментов, на которые разбиваются ответные отклики от сервера электронной почты, направляемые клиенту, [шт];
$F = [0, \ldots, 10]$ – значение времени задержки между отправкой фрагментов отклика клиенту сервиса электронной почты, [с].

Начальное (краевое) условие – распределение вероятностей пребывания системы в состояниях в начальный момент времени

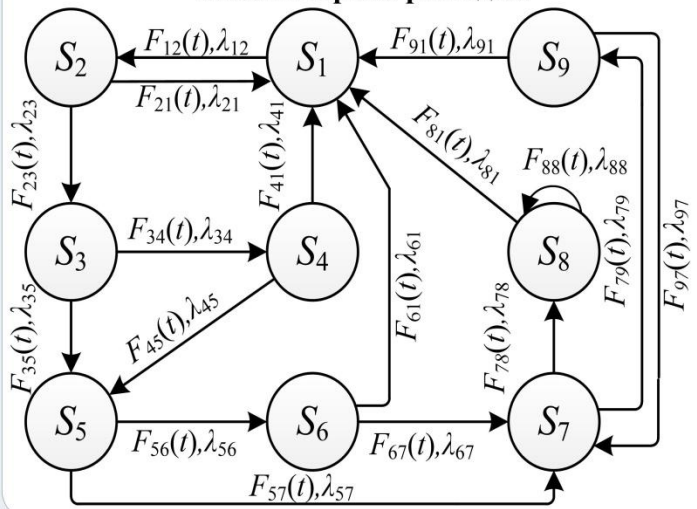
$x(t)=\{p_1(0), p_2(0), \ldots, p_9(0)\}$ (6)

Допустимые значения вектора фазовых переменных $x(t)$ и вектора управления $u(t)$

$0 \le p_i(t) \le 1$; $10^{-4} \le u_1(t) \le 1$; $10^{-4} \le u_2(t) \le 1$; $0{,}67\cdot 10^{-6} \le u_3(t) \le 1$; $0{,}67\cdot 10^{-4} \le u_4(t) \le 1$ (7)

МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ СЕРВИСА ЭЛЕКТРОННОЙ ПОЧТЫ

Граф состояний процесса функционирования сервиса электронной почты ИС ВН в условиях компьютерной разведки



Порядок использования модели:

Статистическая **гипотеза об экспоненциальности** функции распределения случайных величин длительности ожидания случайного события $F_{ij}(t)$ подтверждается?

Да

Используется математическая модель, основанная на математическом аппарате **марковской цепи** с непрерывным временем

Нет

Используется математическая модель, основанная на математическом аппарате **полумарковской цепи** с непрерывным временем

Определение значения **вектора управления** $u(t)$, исходя из оценки значений **функционала качества** $J(t)$

Дискретные состояния случайного процесса

S_1 – клиент находится в состоянии простоя, не принимает и не передает сообщения электронной почты

S_2 – инициализация сетевого соединения клиента с почтовым сервером на транспортном уровне, проверка счетчика общего количества подключений клиентов к серверу

S_3 – инициализация почтовой транзакции, получение почтовым сервером от клиента команды EHLO и проверка идентификаторов отправителя сообщений электронной почты (доменное имя)

S_4 – получение клиентов от почтового сервера множества промежуточных откликов, направляемых через изменяемые интервалы времени их задержки

S_5 – получение почтовым сервером от клиента команды MAIL, проверка идентификаторов отправителя сообщений электронной почты

S_6 – получение клиентом перед ответным откликом сервера ответных откликов, содержащих код ошибки

S_7 – получение почтовым сервером от клиента команды RCPT, проверка идентификаторов получателей электронной почты (имя почтового ящика и домена, а также количество получателей сообщений электронной почты)

S_8 – получение клиентом ответного отклика, содержащего код ошибки о невозможности дальнейшей передачи, разделенного на фрагменты, направляемые через интервалы времени их задержки

S_9 – получение почтовым сервером от клиента команды DATA и передача текста сообщения электронной почты

Результаты расчетов оптимальных параметров проактивной защиты

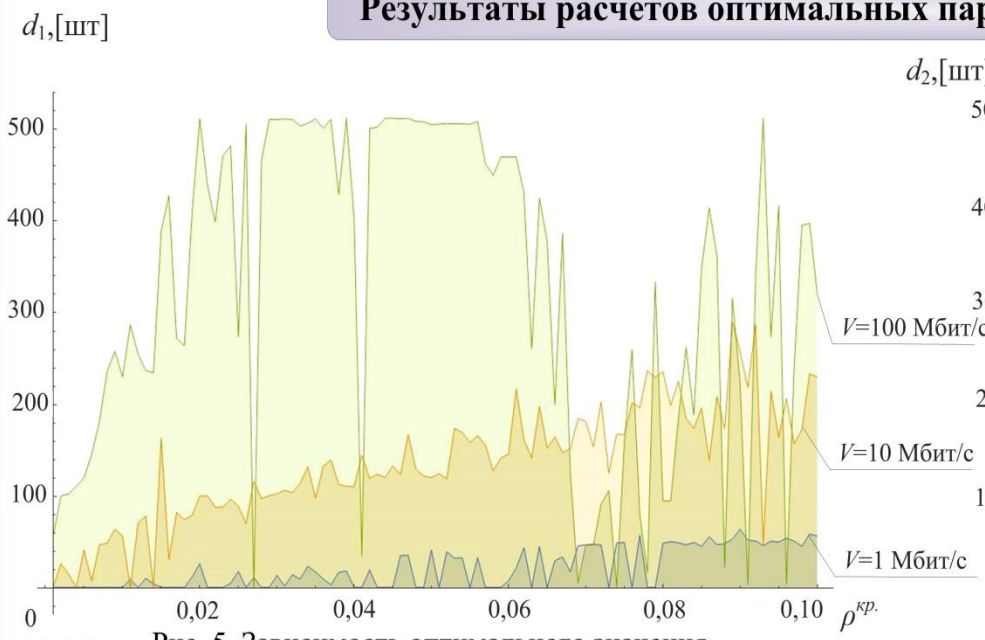


Рис. 5. Зависимость оптимального значения параметра d_1 от ресурсных ограничений $\rho^{кр.}$

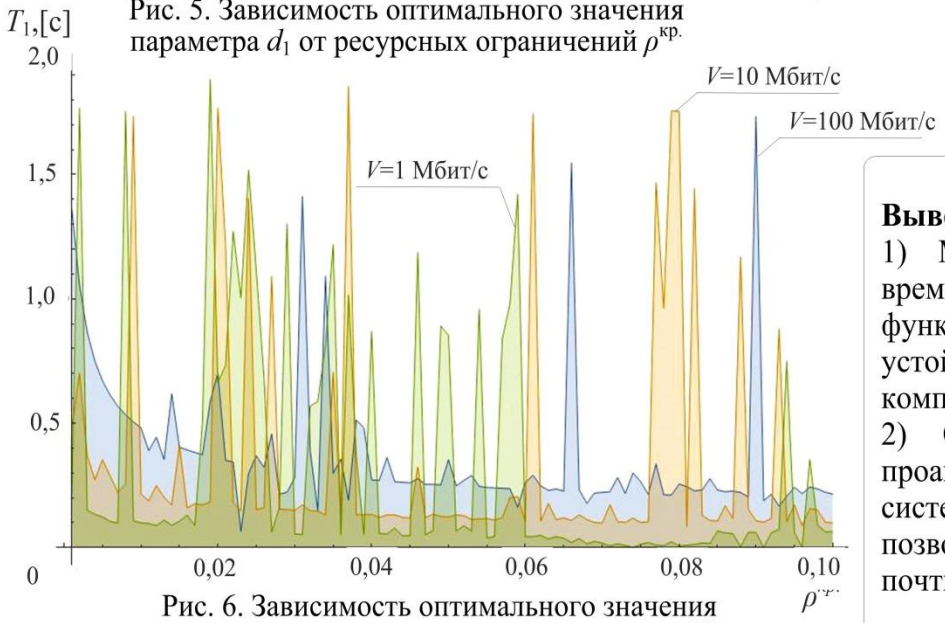


Рис. 6. Зависимость оптимального значения параметра T_1 от ресурсных ограничений $\rho^{кр.}$

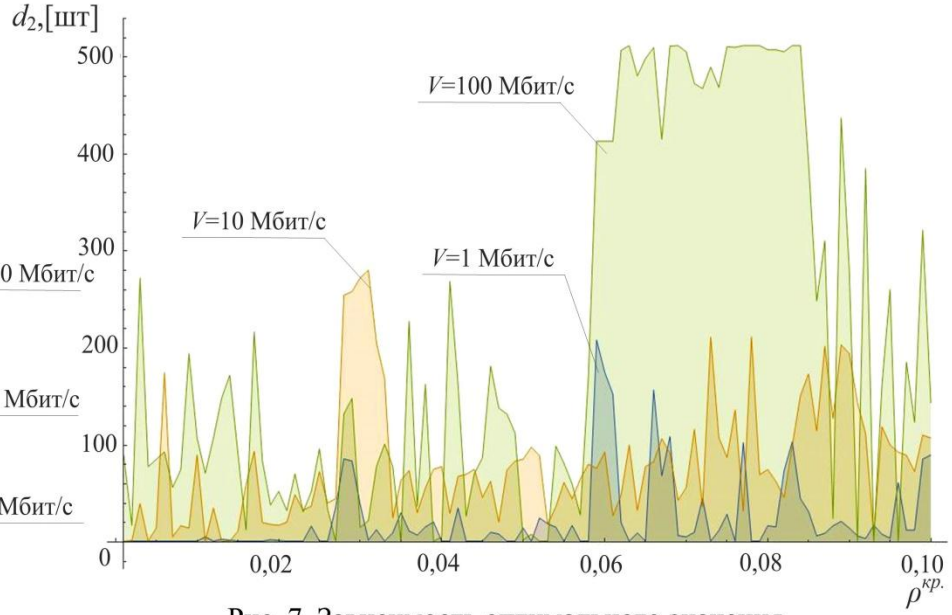


Рис. 7. Зависимость оптимального значения параметра d_2 от ресурсных ограничений $\rho^{кр.}$

Вывод:

1) Математическая модель позволяет: оценить вероятностно-временные характеристики, описывающие процесс функционирования сервиса электронной почты ИС ВН с учетом устойчивости к возмущениям исходных данных в условиях компьютерной разведки;

2) Определение оптимальных значений параметров средств проактивной защиты сервиса электронной почты информационных систем военного назначения в условиях компьютерной разведки позволяет повысить результативность защиты сервиса электронной почты при обеспечении заданного уровня ресурсных затрат.

СПАСИБО ЗА ВНИМАНИЕ!