ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ И НАУКЕ

УДК 004.042

Лысов Д.А.
старший преподаватель
Брянский государственный технический университет

ВОПРОСЫ ВЫБОРА ПРОГРАММНО-ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация: в статье рассматривается вопрос выбора программно-технических средств защиты информации.

Ключевые слова: информационная безопасность, защита информации, программная защита, техническая защита, программно-техническая защита информации, сети Петри.

Annotation: the article deals with the choice of software and hardware means of information protection.

Keywords: information security, information protection, software protection, technical protection, software and technical protection of information, Petri nets.

В наше время информация является не менее, а зачастую и более важным ресурсом нежели материальные активы. Защищенность значимой сведений рассматривается как составная часть понятия качества информации. Особую актуальность приобретают вопросы обеспечения целостности, доступности и конфиденциальности защищаемых данных.

Мировая статистика инцидентов информационной безопасности говорит о том, что большая часть угроз приходится на удалённый доступ. Уязвимости, способствующие реализации такого класса угроз связаны с отсутствием или малой эффективностью работы программно-технической системы защиты информации (ПТСЗИ). Система такого рода призвана обеспечить:

– защиту локальных автоматизированных рабочих мест (АРМ);
– безопасность физически изолированных сегментов локально-вычислительной сети;
– безопасное взаимодействие защищенных АРМ с сетями общего пользования и открытыми ресурсами;
– своевременное обнаружение и блокирование зловредного программного обеспечения;
– разграничение доступа к ресурсам информационной системы;
– шифрование данных;
– обеспечение сохранности значимых данных;
– мониторинг и защита сетевых информационных потоков;
– обеспечение отказоустойчивости и многое другое.

Кроме того, существует проблема оценки эффективности принимаемых проектных решений при создании ПТСЗИ, что затрудняет процесс оценивания уровня защищенности разрабатываемых систем. Отсутствие инструментов, позволяющих автоматизировать процессы, как по проектированию, так и по оценке эффективности функционирования ПТСЗИ, делает выполнение описанных выше процессов ресурсозатратной задачей.

Подготовительные этапы перед выбором программно-технических средств защиты информации можно представить в виде схемы (рис. 1).

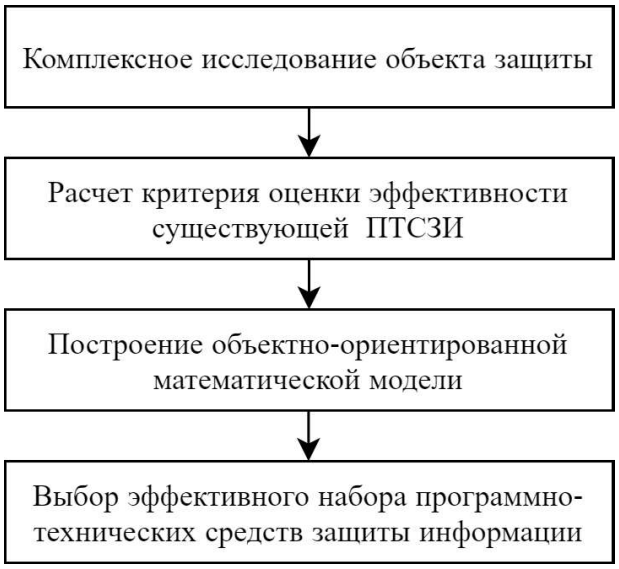

Рис. 1. Подготовительные этапы выбора средств ПТСЗИ

Для решения проблемы выбора средств ПТСЗИ была разработана математическая модель на основе сетей Петри, формализация которой представлена в виде формулы:

$$N =< S, ST, VL, MoC, DA > \quad (1)$$

где:

- S – источник угрозы;
- ST – угроза;
- VL – уязвимое звено;
- MoC – метод противодействия;
- DA – деструктивное воздействие.

Для расчета критерия оценки эффективности, существующей ПТСЗИ необходимо описать модель выявления уязвимостей. Для этого введем некоторые обозначения.

Источником угрозы информационной безопасности организации могут быть конкуренты, недобросовестные партнеры, персонал, хакеры и мошенники. Наименование источников угроз и их индексы, применяемые в математической модели представлены в таблице 1.

Таблица 1. Наименование источников угроз и их индексы

Наименование источника угрозы (Source)	Индекс
Конкуренты	S_1
Недобросовестные партнеры	S_2
Персонал организации	S_3
Хакеры, мошенники	S_4

Более 200 угроз ИБ можно рассмотреть в банке данных угроз безопасности информации ФСТЭК РФ. Для упрощения демонстрации работы модели рассмотрим лишь некоторые из них, а именно: инсталляция и запуск вирусов, несанкционированный доступ, DDOS-атаки, перехват трафика, проникновение во внутреннюю сеть, внешнее сканирование, проникновение через сервисы, спам и подмена сообщений/отправителя. Наименование угроз и их индексы, применяемые в математической модели представлены в таблице 2.

Таблица 2. Наименование угроз и их индексы

Наименование угрозы (Security threat)	Индекс
Инсталляция и запуск вирусов	ST_1
Несанкционированный доступ	ST_2
DDOS-атаки	ST_3
Перехват трафика	ST_4
Проникновение во внутреннюю сеть	ST_5
Внешнее сканирование	ST_6
Проникновение через сервисы	ST_7
Спам, подмена сообщений/отправителя	ST_8

На рисунке 2 представлены источники угроз с угрозами, которые могут быть реализованы через тот или иной источник.

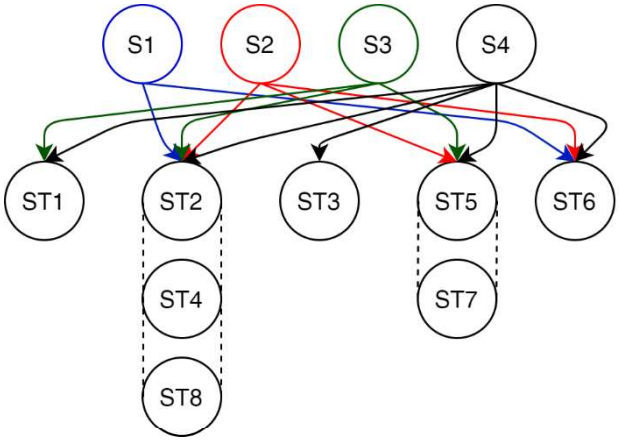

Рисунок 2. Модель уязвимостей ПТСЗИ. Соотношение источника угрозы с угрозами ИБ

Уязвимыми звеньями в системе организации можно считать: нештатное дополнительное ПО (драйверы, утилиты), наличие устаревших версий ПО или версий, имеющих уязвимости, допустимость установки не декларируемого ПО, наличие процедуры обхода администратором установленных правил и режимов безопасности в сети, внешние носители информации, открытые ОС, отсутствие средств защиты ЛВС. Наименование уязвимых звеньев и их индексы, применяемые в математической модели представлены в таблице 3.

Таблица 3. Наименование уязвимых звеньев и их индексы

Наименование уязвимых звеньев (Vulnerable Link)	Индекс
Нештатное дополнительное ПО (драйверы, утилиты)	VL_1
Наличие устаревших версий ПО или версий, имеющих уязвимости	VL_2
Допустимость установки не декларируемого ПО	VL_3
Наличие процедуры обхода администратором установленных правил и режимов безопасности в сети	VL_4
Внешние носители информации	VL_5
Открытые ОС	VL_6
Отсутствие средств защиты ЛВС	VL_7

Методами противодействия будем считать такие средства, как: антивирус, межсетевой экран, honey port, демилитаризованная зона ЛВС, система обнаружения вторжений, системы (настройки) администрирования, резервное копирование, программная защита информации от НСД, шифрование трафика, цифровая подпись, DDOS фильтры. Наименование методов противодействия и их индексы, применяемые в математической модели представлены в таблице 4.

Таблица 4. Методы противодействия и их индексы

Методы противодействия (Method of counteraction)	Индекс
Антивирус	A
Межсетевой экран	FW
Honey Port	HP
Демилитаризованная зона ЛВС	DZ
Система обнаружения вторжений	IDS
Системы (настройки) администрирования	AD
Резервное копирование	R
Программная защита информации от НСД	L
Шифрование трафика	TE
Цифровая подпись	DS
DDOS фильтры	DD

К деструктивным действиям, возникающих в следствии реализации угроз информационной безопасности можно отнести: копирование (чтение), перехват, уничтожение, модификация, блокирование и хищение информации. Наименование деструктивных действий и их индексы, применяемые в математической модели представлены в таблице 5.

Таблица 5. Деструктивные действия и их индексы

Наименование деструктивного действия	Индекс
Копирование (чтение) информации	DA_1
Перехвати информации	DA_2
Уничтожение информации	DA_3
Модификация информации	DA_4
Блокирование информации	DA_5
Хищение информации	DA_6

В результате анализа функциональных связей рассматриваемого класса объектов была построена математическая имитационная модель функционирования ПТСЗИ на основе аппарата раскрашенных сетей Петри. Разработанная сеть является раскрашенной, вероятностной и ингибиторной, что позволяет реализовать следующие возможности:

– вероятностная сеть позволяет учесть, как средства нападения, так и средства отражения угроз безопасности за счет настройки вероятностей совершения переходов;
– раскрашенная сеть Петри позволяет идентифицировать фишки, ассоциируемые с угрозами безопасности и методами противодействия;
– ингибиторная сеть Петри обеспечивает реализацию механизма предотвращения угроз безопасности методами противодействия.

Построенная сеть (рис. 3) является небезопасной – так как небезопасна каждая её позиция (число фишек в ней может быть больше 1). Сеть не обладает свойством живучести (сохранения) – так как общее число фишек в сети не является постоянной величиной (что, однако, и не требуется). Более того, сеть не является строго сохраняющей, так как число входов на каждом переходе не равно числу выходов.

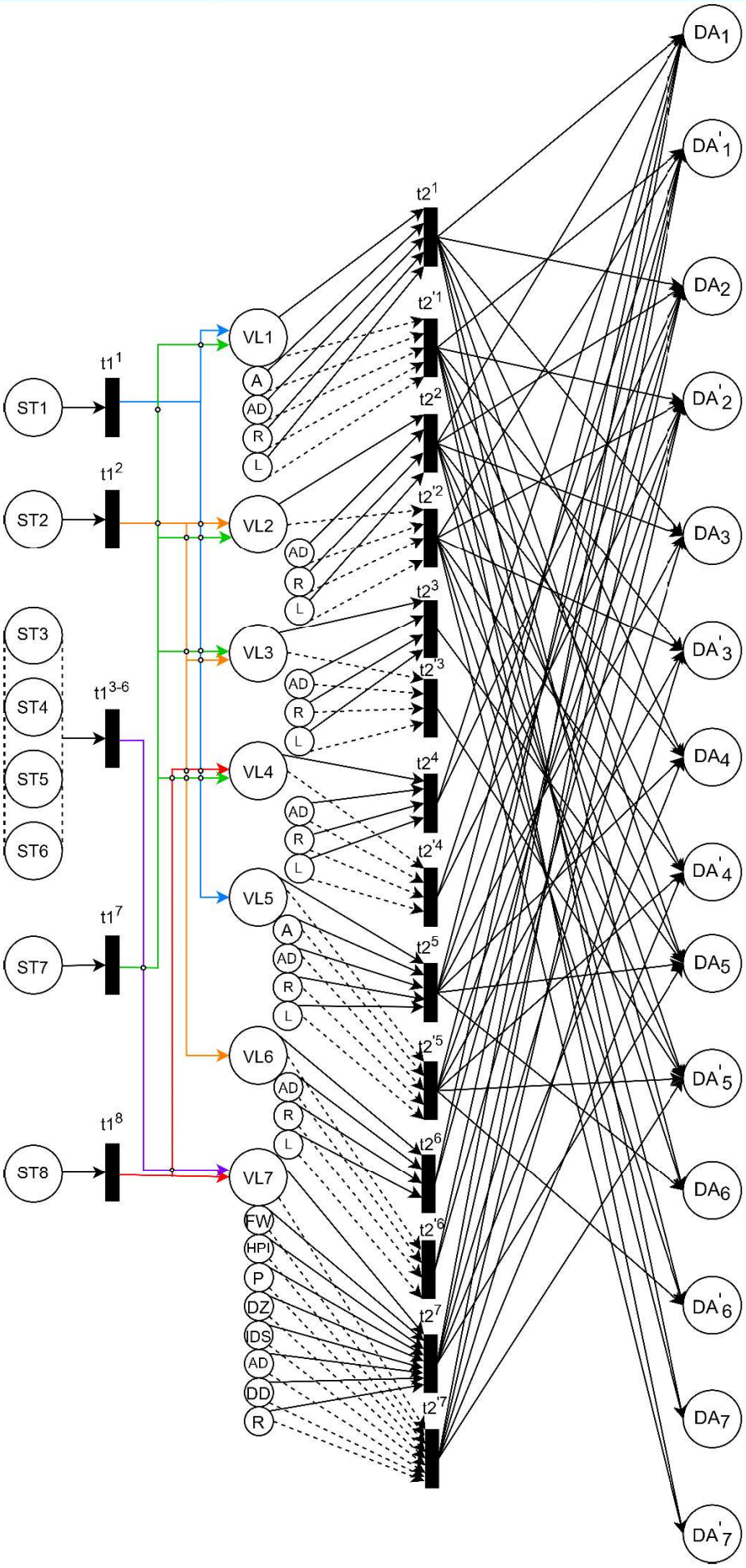
ST1
ST2
ST3
ST4
ST5
ST6
ST7
ST8
t1 1
t1 2
t1 3-6
t1 7
t1 8
VL1
VL2
VL3
VL4
VL5
VL6
VL7
A
AD
R
L
FW
HPI
P
DZ
IDS
DD
t2 1
t2 2
t2 3
t2 4
t2 5
t2 6
t2 7
t2'1
t2'2
t2'3
t2'4
t2'5
t2'6
t2'7
DA1
DA2
DA3
DA4
DA5
DA6
DA7
DA'1
DA'2
DA'3
DA'4
DA'5
DA'6
DA'7

Рисунок 3. Модель уязвимостей ПТСЗИ

Функционирование разработанной модели сводится к следующей последовательности шагов:

1. Формирование расчётных показателей вероятностей возникновения и реализации угроз (настройка вероятности срабатывания перехода t1).
2. Формирование расчётных показателей вероятностей отражения угроз конкретными методами противодействия (настройка вероятности срабатывания перехода t2).
3. Просчёт модели накопления статистики отражённых угроз по сформированным комплектам средств защиты.
4. Выявление наиболее эффективных наборов средств защиты на основе накопленного коэффициента отражения угроз в два этапа.
5. Сравнение сформированных наборов по стоимостным характеристикам.
6. Выбор набора решение на основании предыдущих шагов.
7. Выявление уязвимостей в выбранном набора.

Для формализации работы сети Петри применяется правило обхода представленное с помощью терминальных языков:

$$ST_i \rightarrow \tau_w = t1^a\left(F_{ST_i}\right), t2^i\left(F_{VL_j}, \varphi(CoR_n)\right), t2'^b\left(F_{VL_j}, F_{R_k}, \varphi(CoN_n)\right) \rightarrow DA_m, DA'_m$$

где:

- τ – правило срабатывания перехода;
- $(\dots)$ – условия срабатывания перехода;
- $t1$ – первый переход от угрозы к звену при наличии угрозы;
- $t2$ – второй переход от уязвимого звена до состояний отражения или реализации деструктивного действия;
- F_{ST} – функция, отражающая наличие фишки в позиции ST_i;
- F_{VL} – функция, отражающая наличие фишки в позиции VL_j;
- CoR/CoN – вероятность реализации/нейтрализации угрозы;

– $\varphi(CoR/CoN)$ – функция, отражающая реализацию/нейтрализацию n-й угрозы с вероятностью CoR/CoN;
– F_{R_k} – функция, отражающая наличие фишки в позициях средств защиты.

Приведем фрагмент обхода графа для ST_1, где DA_m – не реализованное деструктивное действие, а $DA_m{}'$ – реализованное деструктивное действие.

$$ST_1 \to \tau_1 = t1^1(F_{ST_1}), t2^1(F_{VL_1}, F_A, F_{AD}, F_R, F_L, \varphi(CoR_n)) \to DA_1$$

$$ST_1 \to \tau_2 = t1^1(F_{ST_1}), t2^1(F_{VL_1}, F_A, F_{AD}, F_R, F_L, \varphi(CoR_n)) \to DA_2$$

$$ST_1 \to \tau_3 = t1^1(F_{ST_1}), t2^1(F_{VL_1}, F_A, F_{AD}, F_R, F_L, \varphi(CoR_n)) \to DA_3$$

$$ST_1 \to \tau_4 = t1^1(F_{ST_1}), t2^1(F_{VL_1}, F_A, F_{AD}, F_R, F_L, \varphi(CoR_n)) \to DA_4$$

$$ST_1 \to \tau_5 = t1^1(F_{ST_1}), t2^1(F_{VL_1}, F_A, F_{AD}, F_R, F_L, \varphi(CoR_n)) \to DA_5$$

$$ST_1 \to \tau_6 = t1^1(F_{ST_1}), t2^1(F_{VL_1}, F_A, F_{AD}, F_R, F_L, \varphi(CoR_n)) \to DA_6$$

$$ST_1 \to \tau_7 = t1^1(F_{ST_1}), t2^1(F_{VL_1}, F_A, F_{AD}, F_R, F_L, \varphi(CoR_n)) \to DA_7$$

$$ST_1 \to \tau_8 = t1^1(F_{ST_1}), t2'^1(F_{VL_1}, F_A, F_{AD}, F_R, F_L, \varphi(CoN_n)) \to DA'_1$$

$$ST_1 \to \tau_9 = t1^1(F_{ST_1}), t2'^1(F_{VL_1}, F_A, F_{AD}, F_R, F_L, \varphi(CoN_n)) \to DA'_2$$

$$ST_1 \to \tau_{10} = t1^1(F_{ST_1}), t2'^1(F_{VL_1}, F_A, F_{AD}, F_R, F_L, \varphi(CoN_n)) \to DA'_3$$

$$ST_1 \to \tau_{11} = t1^1(F_{ST_1}), t2'^1(F_{VL_1}, F_A, F_{AD}, F_R, F_L, \varphi(CoN_n)) \to DA'_4$$

$$ST_1 \to \tau_{12} = t1^1(F_{ST_1}), t2'^1(F_{VL_1}, F_A, F_{AD}, F_R, F_L, \varphi(CoN_n)) \to DA'_5$$

$$ST_1 \to \tau_{13} = t1^1(F_{ST_1}), t2'^1(F_{VL_1}, F_A, F_{AD}, F_R, F_L, \varphi(CoN_n)) \to DA'_6$$

$$ST_1 \to \tau_{15} = t1^1(F_{ST_1}), t2'^1(F_{VL_1}, F_A, F_{AD}, F_R, F_L, \varphi(CoN_n)) \to DA'_7$$

$$ST_1 \rightarrow \tau_{16} = t1^1\left(F_{ST_1}\right), t2^5\left(F_{VL_5}, F_A, F_{AD}, F_R, F_L, \varphi(CoR_n)\right) \rightarrow DA_1$$

$$ST_1 \rightarrow \tau_{17} = t1^1\left(F_{ST_1}\right), t2^5\left(F_{VL_5}, F_A, F_{AD}, F_R, F_L, \varphi(CoR_n)\right) \rightarrow DA_2$$

$$ST_1 \rightarrow \tau_{18} = t1^1\left(F_{ST_1}\right), t2^5\left(F_{VL_5}, F_A, F_{AD}, F_R, F_L, \varphi(CoR_n)\right) \rightarrow DA_3$$

$$ST_1 \rightarrow \tau_{19} = t1^1\left(F_{ST_1}\right), t2^5\left(F_{VL_5}, F_A, F_{AD}, F_R, F_L, \varphi(CoR_n)\right) \rightarrow DA_4$$

$$ST_1 \rightarrow \tau_{20} = t1^1\left(F_{ST_1}\right), t2^5\left(F_{VL_5}, F_A, F_{AD}, F_R, F_L, \varphi(CoR_n)\right) \rightarrow DA_5$$

$$ST_1 \rightarrow \tau_{21} = t1^1\left(F_{ST_1}\right), t2^5\left(F_{VL_5}, F_A, F_{AD}, F_R, F_L, \varphi(CoR_n)\right) \rightarrow DA_6$$

Таким образом, с помощью представленной модели возможно автоматизировать процесс как по проектированию программно-технической системы защиты информации, так и по оценке эффективности функционирования ПТСЗИ, что позволяет сократить затрачиваемые ресурсы на решение вышеописанных задач.