ИВАНОВ Валерий Петрович

МАТЕМАТИЧЕСКАЯ ОЦЕНКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Информация давно перестала быть просто необходимостью для производства и проявлением всякого рода деятельности. Информация приобрела ощутимую ценность, она четко определяется реальной прибылью, получаемой от ее использования, или размерами ущерба вследствие ее потери или несанкционированного доступа (НСД) к ней.
В настоящее время отечественная промышленность предлагает широкий выбор технических средств защиты информации от НСД, некоторые из них могут быть положены в основу построения надежной системы защиты информации. Если руководящие документы Гостехкомиссии России определяют функциональную наполняемость системы защиты информации средств вычислительной техники (СВТ), автоматизированных систем (АС) различных классов, то не обнаружено средств, которые могли бы ответить на вопрос: какова стойкость технического средства защиты информации от его злоумышленного изучения (своего рода составляющая морального старения системы защиты информации), и как ее оценивать. Решение данной задачи возможно путем использования принципов системотехники: изучаемый процесс описывается на языках теорий, которые наиболее развиты (результативны), и оценивается по показателям эффективности надсистемы – человека, определяющего полезность созданной системы защиты информации. При этом используемая система математических моделей имеет иерархическую структуру, где математические модели «нижних» уровней уточняют параметры моделей «высших» уровней.
Тот факт, что защищаемой системе присуща неопределенность (насколько совершенна созданная система защиты информации, а также какова ее временная стойкость в условиях «атак» злоумышленника) позволяет применить для оценки защищенности информации, показатели эффективности вероятностно-временной группы показателей:

- среднее время безопасного функционирования защищаемой системы;
- время безопасного функционирования защищаемой системы с вероятностью ее поражения НСД не выше заданной;
- экономическая эффективность созданной системы защиты информации.

Целью настоящей статьи является предложение методики оценки защищенности информации от злоумышленного изучения технических средств защиты информации для дальнейшего НСД к защищаемой информации (документам) в СВТ и АС на основании применения принципов системотехники и обоснование выводов (решений), связанных с эксплуатацией технических средств защиты информации.
В нашем случае задача оценки стойкости системы защиты информации от ее злоумышленного изучения может быть сформулирована следующим образом:
Пусть имеется система обработки данных (СОД), в которой реализована комплексная система защиты информации на основе технического средства защиты информации. Пусть к злоумышленникам попал экземпляр данного технического средства защиты и начался процесс злоумышленного изучения технического средства защиты. Требуется оценить стойкость системы защиты информации от ее злоумышленного изучения по выбранным показателям эффективности.
Думается, что данная статья только приоткрывает краешек возможностей, которые предоставляет исследователю системы защиты информации математический аппарат теории массового обслуживания и «теории катастроф».

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ЗЛОУМЫШЛЕННИКА, ИЗУЧАЮЩЕГО (РАСШИФРОВЫВАЮЩЕГО) ТЕХНИЧЕСКОЕ СРЕДСТВО ЗАЩИТЫ

Математическая модель злоумышленника должна ответить на вопрос – каковы численные характеристики вероятностей обнаружения попыток НСД на определенном интервале времени.
Решение задачи разработки модели злоумышленника, изучающего техническое средство защиты, предполагает поиск системы теорий:

1. Теории, которая позволила бы связать сложность реализованного разработчиком алгоритма защиты информации и находящегося в конкретном техническом средстве, и время, необходимое злоумышленнику для изучения (расшифровки) данного алгоритма.
2. Теории, которая могла бы связать найденное время изучения (расшифровки) алгоритма с вероятностью того, что злоумышленник сумел выполнить данную работу за некоторый интервал времени.

Анализ показывает, что задача первого рода может быть решена использованием линейной теории алгоритмов, изложенной Холстедом в [6].
Задача второго рода может быть решена использованием «теории катастроф», изложенной в теории массового обслуживания [7].
Рассмотрим линейную теорию алгоритмов и теорию «катастроф» применительно к поставленной задаче.

Линейная теория алгоритмов в решении задачи оценки времени, необходимого злоумышленнику для изучения системы защиты информации

Полагая, что задача изучения (расшифровки) программы длиной N, написанной на некотором алгоритмическом языке, по сложности соизмерима с написанием программы длиной N бит на том же языке, воспользуемся аппроксимацией уравнения времени, необходимого для написания программы, если известна только длина программы – N бит [6]. В этом случае среднее время изучения (расшифровки) программы – T можно найти как:

$$T = \frac{N_2^{\,2} \times \log_2 \eta}{4 \times S} \text{ [c]} \qquad (1)$$

где: η – алфавит языка текста программы;
S – число Страуда ($S = 4 \div 20$ операций в секунду), характеризует количество объектов, которыми может оперировать злоумышленник одновременно (своего рода характеристика быстродействия злоумышленника, изучающего текст программы);
N – длина текста программы (команды + операнды) в битах.

«По Холстеду», в случае, если приходится писать программу на машинном языке [6]

$T \approx N^2$, [c].

Поскольку программы защиты информации характеризуются большой длиной, а работа злоумышленника характеризуется утомляемостью введем поправку на утомляемость злоумышленника, тогда выражение для T будет иметь вид:

$$T \approx 3\, N^2, \text{ [c]} \qquad (2)$$

Теория катастроф в решении задачи оценки вероятности расшифровки текста программы на интервале времени

Теория безопасности информации, руководящие документы Гостехкомиссии России требуют рассматривать злоумышленника как субъекта высшей квалификации, что дает возможность поставить злоумышленному процессу изучения системы защиты информации функцию-распределение умного злоумышленника – экспоненциальное распределение с параметром

$$S = \frac{1}{T}\ [1/\text{с}]$$

Здесь T – среднее время расшифровки (изучения) текста программы.
В этом случае вероятность ($P_н$) нерасшифровки текста программы за некоторый интервал времени (не наступит катастрофа), распределенном в свою очередь по экспоненциальному закону с параметром β, можно представить согласно [7] как преобразование Лапласа-Стильтьеса функции распределения интервала времени на котором оценивается вероятность расшифровки (изучения) текста $B(t)$:

$$P_н = \int_0^\infty e^{-st}\ dB(t) = \frac{\beta}{\beta + s} \qquad (3)$$

Таким образом, нам удалось «плавно» перейти от длины текста программы N, написанной на некотором алгоритмическом языке, который «предусмотрел» для злоумышленника разработчик системы защиты информации, к вероятности нерасшифровки текста программы защиты за некоторый интервал времени, в свою очередь распределенный по экспоненциальному закону. Предполагается, что аппаратные средства системы защиты информации допускают «разворачивание» в текст программы конечной длины и «текст программы защиты» представляет собой сумму текстов программной и аппаратной частей.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ ВЗАИМОДЕЙСТВИЯ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ, СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, СИСТЕМЫ ОБРАБОТКИ ДАННЫХ И ЗЛОУМЫШЛЕННИКА

Процесс взаимодействия:

- злоумышленника, изучающего систему защиты информации и оценивающего успешность НСД;
- способности СОД обрабатывать (хранить) поступившие в нее документы, подлежащие защите;
- поступающих в СОД документов;
- созданной разработчиком системы защиты информации характеризуется конечным множеством возможных состояний

$$S = \{S1, S2, \ldots\ldots, Sr\}. \qquad (4)$$

Процесс в каждый момент времени t характеризуется только одним из этих состояний. Через некоторые интервалы времени имеют место переходы из одного состояние в другое (имеет место шаг процесса).
Вероятность того, что на очередном шаге система перейдет из состояния S_i в состояние S_j, в общем случае, зависит от начального состояния системы и от всех промежуточных состояний, вплоть до текущего состояния. В настоящее время наиболее подробно изучены цепи, обладающие Марковским свойством. В этом случае вероятность перехода на очередном шаге из состояния S_i в состояние S_j зависит только от состояния S_i, в котором цепь оказалась после предыдущего шага (поведение системы в будущем зависит от ее состояния в данный момент и не зависит от того, каким образом она пришла в это состояние).
Естественно предположить, что:

- вероятность одновременного изменения состояний двух и более элементов (например, наступило событие, связываемое с попыткой НСД и освобождение системы от данных, и т.п.) пренебрежимо мала;
- вероятности переходов из одного состояния в другое не зависят от времени.

– за бесконечно малый промежуток времени невозможен переход в некоторое «соседнее» состояние и возврат из него,

тогда рассматриваемый процесс взаимодействия математически характеризуется полумарковским процессом [4]:

с матрицей вероятностей переходов поглощающей цепи (поглощающее состояние характеризует тот факт, что злоумышленник по его мнению изучил (расшифровал) систему защиты информации и готов на практике реализовать попытку НСД к защищаемой информации):

$$\boldsymbol{P} = \begin{vmatrix} P_{11} & P_{12} & \ldots\ldots\ldots P_{1r} \\ P_{21} & P_{22} & \ldots\ldots\ldots P_{2r} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ P_{r1} & P_{r2} & \ldots\ldots\ldots P_{rr} \end{vmatrix} \qquad (5)$$

$S1$ – множеством невозвратных состояний полумарковского процесса;

$N=|n_{ij}||$ – фундаментальной матрицей вложенной поглощающей Марковской цепи;

m_i – средним временем однократного пребывания полумарковского процесса в невозвратных состояниях $S_i \in S$.

$N^*= ||n_{ij}^*||$ – матрицей средних времен n_{ij}^* пребывания полумарковского процесса в состоянии $S_i \in S$ до поглощения при условии, что начальным было состояние $S_i \in S$.

$T^* = ||t_i^*||$ – матрица-строка средних времен t_i^* пребывания полумарковского процесса во множестве невозвратных состояний при начальном состоянии $S_i \in S$ до перехода в соседнее состояние.

t^* – средним временем пребывания полумарковского процесса в множестве невозвратных состояний при произвольном начальном распределении вероятностей состояний – $P(0)$.

В общем случае, рассматриваемая система формально представляет собой СОД, на вход которой поступает информация (документы), подлежащие защите. Поступление документов характеризуется пуассоновским потоком с параметром – β.

Документы пребывают в СОД некоторое время, время пребывания документа в СОД характеризуется параметром – γ.

«Интерес» злоумышленника к документам, подлежащим защите, характеризуется потоком попыток НСД с параметром НСД – λ.

«По Холстеду» и использованием «теории катастроф» мы получим численные значения вероятностей:

P_1 – вероятность обнаружения попытки НСД в моменты времени, когда в системе нет защищаемой информации;

P_2 – вероятность обнаружения попытки НСД на этапе аутентификации принятого документа;

P_3 – вероятность обнаружения попытки НСД на этапе обработки (хранения) поступившего документа;

Известны:

– доход – $C1$ единиц ценности, получаемый от обработки защищаемой информации (документа);
– ущерб – $C2$ единиц ценности от НСД к защищаемой информации (документу).

Тогда задача оценки эффективности защиты сводится к оценке среднего времени пребывания полумарковского процесса во множестве невозвратных состояний до поглощения и использовании его для получения вероятностно-временных характеристик показателей эффективности.

Вывод математического выражения оценки среднего времени безопасного функционирования исследуемой системы

Поскольку рассматриваемая система характеризуется поглощающим состоянием – состоянием, когда злоумышленник обнаружил, что для него нет секретов и он готов

реализовать свое «злодейское дело», то математическое выражение среднего времени безопасного функционирования исследуемой системы можно определить как среднее время пребывания рассматриваемой системы во множестве невозвратных состояний. В соответствии с [4] среднее время – *t* пребывания исследуемого процесса во множестве невозвратных состояний может быть найдено как произведение матриц:

$$t = P(0)\ N^*\ E\,, \qquad (6)$$

где: $P(0)$ – матрица-вектор начального состояния, из которого начался исследуемый процесс.
$N^* = \| n_{ij}^* \|$ – матрица средних времен n_{ij}^* пребывания полумарковского процесса в состоянии $S_i \in S$ до поглощения при условии, что начальным было состояние $S_j \in S$.
$N^* = \| n_{ij}\ m_j \|$.
m_j – среднее время однократного пребывания полумарковского процесса в невозвратных состояниях $S_i \in S$.
n_{ij} – элемент фундаментальной матрицы $N = \| n_{ij} \|$, получается из выражения
$N = (I - Q)^{-1}$
I – единичная диагональная матрица.
Q – матрица переходов в невозвратном множестве состояний.
E – вектор-столбец единичных элементов.
Таким образом, для того, чтобы определить среднее время безопасного функционирования исследуемой системы необходимо:
1. Из матрицы переходов исследуемого процесса $\boldsymbol{P}$ получить матрицу переходов в невозвратном множестве состояний $\boldsymbol{Q}$ и m_j – средние времена однократного пребывания полумарковского процесса в невозвратных состояниях $S_i \in S$.
2. Получить фундаментальную матрицу $N = \| n_{ij} \|$ согласно выражению:
$N = (I - Q)^{-1}$.
3. Получить матрицу средних времен n_{ij}^* пребывания полумарковского процесса в состоянии $S_i \in S$ до поглощения при условии, что начальным было состояние $S_j \in S$:
$N^* = \| n_{ij}\ m_j \|$.
4. Конкретизировать вектор-столбец начального состояния, из которого начался исследуемый процесс.
5. Использованием выражения $t = P(0)\ N^*\ E$ получить численное значение среднего времени безопасного функционирования защищаемой системы.

Вывод математического выражения оценки интервала времени, на котором вероятность исключения НСД защищаемой информации не ниже заданной величины

Выражение (6) позволяет оценить среднее время безопасного функционирования защищаемой системы. Однако система защиты информации должна эксплуатироваться. Эксплуатация должна включать проверку исправности системы защиты информации по достижении системой некоторого порога доверия – вероятности исключения НСД к защищаемой информации ниже заданного.
Аппроксимируем функцию – распределения времени, на котором доверие к системе защиты информации не ниже заданного, а также функцию распределения времени безопасного функционирования экспоненциальными распределениями с параметрами **s** и $\boldsymbol{\mu}$ соответственно.
$\mu = \frac{1}{T}$

Поскольку согласно теории «катастроф» вероятность исключения НСД – $P_{нсд}$ на интервале, распределенном по экспоненциальному закону с параметром – $\boldsymbol{s}$ составит

$$\mathrm{P}_{\text{НСД}} = \int_0^{\infty} e^{-\mu t} dS(t) = \frac{s}{s+\mu} \qquad (7)$$

Тогда *T0* – среднее время безопасного функционирования защищаемой системы с вероятностью исключения НСД не ниже $P_{нсд}$ можно найти как:

$$T0 = \frac{1}{s} = \frac{t(1 - P_{НСД})}{P_{НСД}} \qquad (8)$$

Из выражения (8) следует, что по истечении времени – *T0* для поддержания доверия к созданной системе защиты информации необходимо проведение «регламентных работ» по проверке работоспособности системы защиты информации с целью возвращения «доверия» к системе защиты информации. Методика проведения регламентных работ должна быть достаточно эффективной.
В качестве формы возвращения «доверия» к системе защиты информации может быть и внедрение очередной версии технического средства защиты информации. Этим мы как бы ставим злоумышленника перед необходимостью изнурительной работы по освоению каждый раз все нового технического средства защиты
Таким образом, для того, чтобы оценить среднее время между проведениями регламентных работ необходимо:
1. В соответствии с выражением (6) получить численное значение среднего времени безопасного функционирования защищаемой системы.
2. Оценить требуемый уровень защиты информации нижним порогом доверия к системе защиты информации – $P_{нсд}$.
3. Использованием выражения (8) получить численное значение интервала времени, в течение которого обеспечивается защищенность документов не ниже заданного нижнего порога.

Вывод математического выражения оценки дохода от использования системы защиты информации
Как отмечалось выше, информация давно перестала быть просто необходимостью для производства и проявлением всякого рода деятельности. Информация приобрела ощутимую ценность, она четко определяется реальной прибылью, получаемой от ее использования, или размерами ущерба вследствие ее потери или НСД к ней. Положим этот постулат в основу вывода математического выражения оценки дохода, получаемого от использования системы защиты информации.
Поскольку процесс функционирования исследуемой системы через равномерные интервалы времени включает проведение регламентных работ (предполагается, что достигнут уровень доверия к системе защиты информации, равный нижнему порогу доверия – $P_{нсд}$), то обработка каждого поступившего документа с вероятностью – $P_{нсд}$ приносит доход – в *C1* единиц стоимости, а с вероятностью ($1 - P_{нсд}$) – ущерб в *C2* единиц стоимости. В данном случае математическое выражение дохода – *Д*, приносимого каждым поступившим документом составит:

$$Д = C1 * P_{нсд} - C2 * (1 - P_{нсд}) \qquad (9)$$

Естественно считать, что в случае $Д > 0$ применение технического средства защиты информации приносит доход.

ПРИМЕР ОЦЕНКИ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ЕЕ ЗЛОУМЫШЛЕННОГО ИЗУЧЕНИЯ

Пусть имеется СОД. В ней реализована комплексная система защиты информации на основе некоторого программно-аппаратного средства защиты информации.
Комплексная система защиты информации оценивается длинами (команды + операнды) программных модулей (аппаратная часть тоже оценена некоторыми длинами и они включены в понятие длины программных модулей):
N1 – длина программного модуля защиты информации на интервале времени, отсутствия в СОД документов;
N2 – длина программного модуля защиты информации на интервале времени приема документа в СОД;
N3 – длина программного модуля защиты информации на интервале времени обработки и хранения документа в СОД.
Пусть: *N1 = N2 = N3 =10 000 бит*.
Пусть во всех случаях злоумышленникам предоставлена возможность «изучения» программы с использованием машинного языка [6].
Документы, подлежащие защите, поступают в СОД в электронном виде. Поступления документов описывается Пуассоновским законом с параметром
$\beta = 0{,}001$ [1/сек].
Документы пребывают в обработке (хранении) время, описываемое экспоненциальным распределением с параметром распределения
$\gamma = 0{,}001$ [1/сек].
Обработка документа приносит владельцу СОД доход в
C1 = 1 [единиц стоимости].
Ущерб от НСД к любому документу, оказавшемуся в СОД, оценивается в
C2 = 1000000 [единиц стоимости].
Злоумышленник заинтересован в НСД к каждому документу.
Пусть злоумышленник скооперировался с другими злоумышленниками и распределил работу таким образом, что модули с длинами *N1, N2, N3* «изучаются» параллельно и независимо.
В этом случае в соответствии с (2) среднее время изучения (расшифровки) каждого программного модуля составит:
$T \approx 3 * 10000^2 \approx 300000000$ *с*.

Оценка вероятности расшифровки программного модуля системы защиты информации между моментами поступления документов в СОД
Примем:
P1 – вероятность нерасшифровки текста программы модуля защиты информации на этапе отсутствия документа в СОД между соседними поступления документов в СОД (вероятность неблокирования системы защиты информации для данного этапа);
P2 – вероятность нерасшифровки текста программы модуля защиты информации на этапе приема (формирования) документа в СОД между соседними моментами поступления документов в СОД (вероятность неблокирования системы защиты информации для данного этапа);
P3 – вероятность нерасшифровки текста программы модуля защиты информации на этапе обработки и хранения документа в СОД между соседними моментами поступлениями документов в СОД (вероятность неблокирования системы защиты информации для данного этапа);
Поскольку предположен Пуассоновский закон поступления документов в СОД вероятность нерасшифровки программного модуля длиной *N1* системы защиты информации между моментами поступления документов в СОД оценивается согласно (3) как:

$$\mathrm{P1} = \mathrm{P2} = \mathrm{P3} = 1 - \frac{1/T}{\beta + 1/T} = \frac{0{,}001}{0{,}001 = 1/300000000} = 0{,}999997$$

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ВЗВИМОДЕЙСТВИЯ СОД, ДОКУМЕНТОВ, ПОСТУПАЮЩИХ В СОД, И ЗЛОУМЫШЛЕННИКА

Изучаемая система взаимодействия формально представляет собой систему обработки данных, на вход которой поступает информация – документы, подлежащие защите. В защищаемой системе реализована система защиты информации на основании технических средств защиты. Технические средства защиты обеспечивают защиту информации на всех этапах ее пребывания и обработки в защищаемой системе.

Таким образом, исследуемая система характеризуется:

- пуассоновским потоком событий, связанных с НСД, с параметром λ;
- пуассоновским потоком документов, подлежащих защите, с параметром β;
- экспоненциальным распределением времени обработки (пребывания) документов в защищаемой системе с параметром γ;
- в системе создана комплексная система защиты информации, которая обеспечивает:
  - защиту информации на интервале, когда ее нет в защищаемой системе, с вероятностью *P1 = 0,999997*;
  - защиту информации на интервале времени, когда сообщение поступило в защищаемую систему – на этапе предварительной обработки (аутентификации) поступившего сообщения – *P2 = 0,999997*;
  - защиту информации в ходе обработки поступившего сообщения (отработки документа) – *P3 = 0,999997*.

Замечание: С формализмами, связанными с пуассоновскими потоками информации на входе СОД и экспоненциальными распределениями времени пребывания информации в них, связаны наиважнейшие результаты исследований в области теории вычислительных систем, вычислительных сетей, теории телетрафика и иных областях техники. Поэтому применение данных формализмов вполне уместно.

Будем исходить из того, что «злоумышленнику» интересно каждое сообщение, поступившее в систему. Это делает возможным для рассматриваемой системы использование формализма о пуассоновском потоке событий, связанных с НСД, к сообщениям с параметром, численно равным параметру потока документов.

В нашем случае процесс функционирования защищаемой системы может быть представлен в виде графа переходов *рис. 1* и матрицей переходов *рис. 2*.

Рис. 1 Граф переходов

Здесь: *S1, S2, S3, S4, S5* – множество состояний:

S1 – сложное состояние, которое включает:

- отсутствие документов в системе;
- обнаружение факта НСД на этапе отсутствия документа в системе и мгновенное восстановление системы после обнаружения факта НСД.

S2 – сложное состояние, которое включает:

- поступление документа в систему;
- обнаружение факта НСД на этапе проверки сообщения и мгновенное восстановление системы после обнаружения факта НСД.

S3 – состояние необнаружения факта НСД, когда в системе нет документов;

S4 – состояние проверки системы при наличии факта НСД на этапе обработки поступившего сообщения.

S5 – состояние необнаружения факта НСД по окончании обработки поступившего документа.

$$\begin{vmatrix} P_{11} & P_{12} & P_{13} & 0 & 0 \\ P_{21} & P_{22} & 0 & P_{24} & 0 \\ 0 & P_{32} & 0 & P_{34} & 0 \\ P_{41} & 0 & 0 & 0 & P_{45} \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

Примем допущение о том, что процесс переходов является марковским, тогда рассматриваемый процесс переходов представляется матрицей переходов *рис. 2*.

$$\boldsymbol{P} =$$

Рис. 2. Матрица переходов

На *рис. 2* $P_{11} = \lambda * P1/(\lambda + \beta)$; $P_{12} = \beta/(\lambda + \beta)$; $P_{13} = \lambda*(1-P1)/(\lambda + \beta)$;
$P_{21} = \gamma/(\lambda + \gamma)$; $P_{22} = P2*\lambda/(\lambda + \gamma)$; $P_{24} = (1-P2)*\lambda/(\lambda + \gamma)$;
$P_{32} = P2$; $P_{34} = 1- P2$;
$P_{41} = P3$; $P_{45} = 1- P3$.

При этом среднее время одиночного пребывания системы в каждом из невозвратных состояний составит (*рис. 3*).

$$M = \begin{vmatrix} \frac{1}{\lambda+\beta} & \frac{1}{\lambda+(1-P2)\times\gamma} & \frac{1}{\beta} & \frac{1}{\gamma} \end{vmatrix}$$

Рис. 3

Оценка среднего времени безопасного функционирования защищаемой системы

Оценка среднего времени безопасного функционирования защищаемой системы заключается в вычислении среднего времени пребывания процесса во множестве невозвратных состояний, матрицы *рис. 1*. Для чего получим матрицу ***Q*** путем вычеркивания 5-й строки и 5-го столбца матрицы ***P***.

$$\boldsymbol{Q} = \begin{vmatrix} P_{11} & P_{12} & P_{13} & 0 \\ P_{21} & P_{22} & 0 & P_{24} \\ 0 & P_{32} & 0 & P_{34} \\ P_{41} & 0 & 0 & 0 \end{vmatrix}$$

Рис. 4.

Среднее время безопасного функционирования рассматриваемой системы – среднее время пребывания процесса во множестве невозвратных состояний вычисляется по формуле (6).
Пусть:
1) Процесс начался из начального состояния *S1*. Этому соответствует вектор-строка $P(0)=(1,0,0,0)$.
2) M – Матрица средних времен однократного пребывания рассматриваемого процесса в каждом из состояний множества состояний (изображена на *рис. 3*).
Матрица $(I - Q)$ будет иметь вид:

$$\boldsymbol{(I - Q)} = \begin{vmatrix} (1-P_{11}) & P_{12} & P_{13} & 0 \\ P_{21} & (1-P_{22}) & 0 & P_{24} \\ 0 & P_{32} & 0 & P_{34} \\ P_{41} & 0 & 0 & 0 \end{vmatrix}$$

Рис. 5

Матрица $(I - Q)^{-1}$ получается в соответствии с выражением матричного преобразования:

$$(I - Q)^{-1} = \frac{1}{A} \begin{vmatrix} A_{11} & A_{21} & A_{31} & A_{41} \\ A_{12} & A_{22} & A_{32} & A_{42} \\ A_{13} & A_{23} & A_{33} & A_{43} \\ A_{14} & A_{24} & A_{34} & A_{44} \end{vmatrix}$$

где: A – определитель матрицы (*рис. 3*);
A_{ij} – алгебраические дополнения соответствующих элементов матрицы (*рис. 5*).
Откуда матрица N^* будет иметь вид:

$$N^* = \frac{1}{A} \begin{vmatrix} A_{11}*m_1 & A_{21}*m_1 & A_{31}*m_1 & A_{41}*m_1 \\ A_{12}*m_2 & A_{22}*m_2 & A_{32}*m_2 & A_{42}*m_2 \\ A_{13}*m_3 & A_{23}*m_3 & A_{33}*m_3 & A_{43}*m_3 \\ A_{14}*m_4 & A_{24}*m_4 & A_{34}*m_4 & A_{44}*m_4 \end{vmatrix}$$

Поскольку для выбранного начального состояния существенными являются численные значения $A, A_{11}, A_{21}, A_{31}, A_{41}$ определим их.
$A = (1 - P_{22})(1 - P_{11} - P_{41}\ P_{34}\ P_{13}) - P_{21}\ (P_{12} + P_{13}\ P_{32}) - P_{41}\ P_{24}\ (P_{12} + P_{13}\ P_{32})$.
$A_{11} = 1 - P_{22}$
$A_{21} = P_{12} + P_{13}\ P_{32}$
$A_{31} = P_{13}\ (1 - P_{22})$
$A_{41} = (1 - P_{22})P_{13}\ P_{34} + P_{24}\ (P_{12} + P_{13}P_{32})$

Откуда среднее время безопасного функционирования рассматриваемой системы составит:

$$t = \frac{\mathrm{m1}}{\mathrm{A}}(A_{11} + A_{21} + A_{31} + A_{41}) = 1{,}40932\ e{+}7\ лет.$$

Оценка интервала времени, на котором вероятность исключения НСД защищаемой информации не ниже заданной величины
Полагая, что доведение сообщения не по адресу (нормируемая величина для систем обмена данными) можно рассматривать как своего рода НСД, и эта величина для системы Autodin (единая автоматизированная системы связи США, предназначена для передачи различных видов информации: речевой, цифровой и видео [5]) она равна 0,0000001. Возьмем эту величину как нормативную для нашего случая. Тогда среднее значение интервала времени, на котором обеспечивается вероятность исключения НСД – $P_{нсд}$ с численным значением не менее 0,9999999 в соответствии с (2) составит (в годах):

$$T0 = \frac{t(1 - P_{НСД})}{P_{НСД}} = \frac{1{,}40932e + 7 \times 0{,}0000001}{0{,}999999} = 1{,}4 лет$$

Из полученного следует, что для обеспечения защиты информации от НСД с уровнем защищенности 0,9999999 в условиях возможного злоумышленного изучения технического средства защиты и в дальнейшем модификации технического средства, установленного в СОД, необходимо проведение регламентных работ над средствами защиты информации через 1,4 лет. Понятно, что регламентные работы должны обеспечить необходимую глубину проверок исправности (отсутствия модификации) технического средства защиты информации.

Оценка дохода от использования системы защиты информации

Ранее было принято, что обработка документа в СОД приносит доход в 1 единиц ценности, а НСД – ущерб в 1000000 единиц ценности. Тогда в соответствии с выражением (9) доход составит:

$$Д = C1 * P_{нсд} – C2*(1 – P_{нсд}) = 1 \times 0,9999999 – 1000000 \times 0,0000001 = 0,899999 \text{ ед.}$$

Поскольку численное значение $Д>0$, – техническое средство защиты информации приносит доход.

ВЫВОДЫ

Для исследуемой СОД, которая характеризуется:

- наличием комплексной системы защиты информации на основе технического средства с длинами программ контроля в период отсутствия защищаемой информации в СОД, в период поступления документа в СОД и в период обработки (хранения) документа в СОД – 10 000 бит;
- потоком документов электронной формы, подлежащих защите с параметром $\beta = 0,001$ [1/сек];
- временем пребывания документа в СОД с параметром $\gamma = 0,001$ [1/сек];
- заинтересованностью злоумышленника в доступе к каждому поступившему документу;
- доходом владельца СОД в 1 единицу ценности и штрафными санкциями в случае НСД к каждому документу в 1000000 единиц ценности;
- требованием – вероятность исключения НСД = 0,9999999,

получены оценки:

- среднее время безопасной обработки документов, подлежащих защите в СОД, – 1,40932 e + 7 лет;
- среднее время функционирования СОД с вероятностью исключения НСД к документам, подлежащим защите, равной 0,9999999 – 1,4 лет;
- доход, приведенный к каждому обработанному документу, – 0,899999 единиц ценности;
- сделан вывод о рентабельности использования технического средства защиты информации, а также о необходимости проведения регламентных работ для технических средств защиты через 1,4 лет.

ЗАКЛЮЧЕНИЕ

Данная статья может быть полезной как разработчикам систем защиты информации, так и преподавателям высших учебных заведений, где преподается курс безопасности информации, поскольку предлагаемая методика позволяет:

- обосновать ряд нормативных положений руководящих документов Гостехкомиссии России;
- сравнивать технические средства защиты информации от НСД, реализованные программными, программно-аппаратными средствами;
- формировать системный подход при решении задачи организации эксплуатации технических средств защиты информации и иных задач.

Использование достаточно простого математического аппарата, несомненно, является достоинством предлагаемой методики.

Полагаю, что читателям журнала будет интересно самостоятельно сравнить, что значит дать возможность злоумышленнику изучать текст программы защиты информации на машинном языке или предоставить возможность изучения текста программы на языке ассемблера или ином алгоритмическом языке. Думается, что выводы подтвердят, что создатели системы защиты информации «АККОРД» [8], делая упор на аппаратные средства защиты, стоят на правильном пути.

Литература

1. В.А. Герасименко. Защита информации в автоматизированных системах обработки данных. В двух книгах. М. Энергоатомиздат. 1994.
2. Дж. Клир. Системология. Автоматизация решения системных задач. М. Радио и связь. 1990.
3. В.В. Дружинин и др. Системотехника. М. Радио и связь. 1985.
4. Ю.П. Журавлев и др. Надежность и контроль ЭВМ. М. Советское радио. 1978.
5. И.А. Мизин и др. Передача информации в сетях с коммутацией сообщений. М. Связь. 1977.
6. Холстед М.Х. Начала науки о программах. М. Финансы и статистика. 1981.
7. В.Ф. Матвеев и др. Системы массового обслуживания. Издательство Московского университета. 1984.
8. В.А. Конявский. Управление защитой информации на базе СЗИ НСД «АККОРД». М. Радио и связь. 1999.