Список літератури

1. Гарасим Ю. Р. Поняття живучості системи захисту інформації захищених корпоративних мереж зв'язку / Ю. Р. Гарасим, В. Б. Дудикевич // Тези доповідей III міжнародної науково-практичної конференції «Інформаційна та економічна безпека (INFECO-2010)». – Харків, 2010. – Випуск 3 (84). – С. 107-109.
2. Dudykevych V. Survivable security Systems Analysis / V. Dudykevych, I. Garasym // Computer science and information technologies: Materials of the VIth International scientific and technical conference CSIT 2010. – Lviv : Publishing House Vezha&Co, 2010. – pp. 108-110.
3. Гарасим Ю. Розробка моделі оцінки живучості для систем захисту інформації / Ю. Гарасим // Комп'ютерні науки та інженерія: Матеріали IV Міжнародної конференції молодих вчених CSE-2010. – Львів : Видавництво Львівської політехніки, 2010. – С. 320-321.
4. Дудикевич В. Б. Моделі оцінки живучості систем захисту інформації / В. Б. Дудикевич, Ю. Р. Гарасим // «Обчислювальні методи і системи перетворення інформації»: зб. праць наук. техн. конф., Львів, 7-8 жовтня 2010 р. – Львів : ФМІ НАНУ, 2010. – С. 104-107.

В статті розроблено математичну модель оцінки живучості системи захисту інформації корпоративної мережі зв'язку за станом системи, що, на відміну від інших, дає можливість оцінити виживаність системи захисту при n-кратному впливі дестабілізуючих факторів та використовувати точкову, статичну модель системи без врахування стійкості елементів і вторинних наслідків після впливу дестабілізуючих факторів.

Ключові слова: оцінка живучості, живучість систем захисту інформації, корпоративні мережі зв'язку.

Рецензент:д.т.н., проф. Рибальський О.В.
Надійшла 16.11.2010

УДК 004.621.519 **Браиловский Н.Н., Орленко В.С., Хорошко В.А.** (ГУИКТ)

ФОРМИРОВАНИЕ КОМПЛЕКСНЫХ ПРОГРАММ ПО ЗАЩИТЕ ОБЪЕКТОВ ПРИ НАЛИЧИИ УГРОЗ И РИСКОВ

Введение

При разработке требований и системе защиты информации (СЗИ) следует учитывать возникновения угроз и рисков, анализировать их влияние и на этой основе предусматривать меры по их отражению.

При формировании требований с учетом угроз и рисков возникают следующие задачи:

– Определение количественных характеристик влияния угроз и рисков на эффективность СЗИ;

– Определение количественных показателей относительной эффективности СЗИ при наличии угроз и рисков;

– Распределения ресурсов между отражению угроз и рисков и системой, имеющими созидательную направленность.

Известные методы решения первой задачи предусматривает идентификацию рисков (количественный анализ) [1], а также оценивание вероятностей и размеров возможного ущерба (количественный анализ) [2]. Однако при этом задача оценки эффективности защиты с учетом рисков не решается и остается уделом лица, принимающего решения (ЛПР). Более того, определения ущерба в абсолютном измерении (в денежном выражении) часто невозможно для сложенных СЗИ.

Метод решения задачи относительной эффективности защиты при наличии угроз и рисков естественно разрабатывает на основе методов решения данной задачи без учета этих факторов. Наиболее распространение в настоящие время получили мультикритериальные

методы оценки [3,4]. Область их применения ограничивает, по крайней мере, двумя необходимыми условиями, которым должна удовлетворять конкретная задача.

Первое условие – наличие множества критериев, по каждому из которых можно оценить каждую альтернативу. Второе условие – способность ЛПР оценить тем или иным образом каждую альтернативу по каждому критерию, т.е. полностью разобраться в проблеме.

Первое условие в большинстве случаев формирования сложны СЗИ не выполняется из-за существенного различия природы подсистем защиты, входящих в них. Выполнения второго условия проблематично, когда выбор наилучшей альтернативы из нескольких десятков или ранжирования такого количества альтернатив требует учета их оценок по нескольким десяткам взаимосвязанных критериев. Такая ситуация имеет место при принятии решения по формированию сложных комплексных целевых программ государственного масштаба, программ построения СЗИ крупных банков, корпораций и государственных предприятий.

Поэтому методы поддержки принятия решений при формировании комплексных целевых программ по защите информации (ЗИ) в условиях угроз и рисков будем разрабатывать путем модификации методов целевого оценивания альтернатив [5]. При поддержке решений по разработке таких программ по ЗИ относительная эффективность защиты должна оцениваться как функция времени, заданная на интервале проектирования [6]. Поэтому возможность учета фактора времени при оценке программ по ЗИ принципиальная для решения задач поддержки решения такого рода.

Основная идея предлагаемого подхода к анализу влияния угроз и рисков при выполнении программы по ЗИ (ПЗИ) состоит в том, что события, вызывающие угрозу или риск, рассматривается как составная часть СЗИ, т.е. влияние внешней среды. Поэтому такие модели угроз и рисков включается в иерархию целей ПЗИ [6], устанавливаются их связи с другими системами и целями ПЗИ. Таким образом, каждая из моделей угроз и рисков имеет хотя бы одну цель или программу, на рассмотрение которой (степень выполнения которого) он оказывает непосредственное влияние. Следуя [6], назовем такие цели (программы) непосредственными над целями модели угрозы или риска. При этом влияния угроз и/или риска, как и других ПЗИ, оценивается !? влияния на рассмотрения главной цели программы. Эффективность ПЗИ оценивается при условии наличия угроз и рисков с учетом их вероятных характеристик. Такой подход дает возможность распределять ресурсы на отражение угроз и рисков на ровне с распределением ресурсов на программы, составляющие сущность ПЗИ.

Цель работы

Для реализации предлагаемого подхода необходимо решать ряд задач. Первая связана с разработкой математических моделей угроз и рисков позволяющих , включать события, которые вызывают угрозу и/или риск, в иерархию целей ПЗИ. Сущность второй задачи состоит в разработке количественного оценивания угрозы и/или риска.

Основная часть

Угрозы разделяются на внешние и внутренние, которые действуют на СЗИ [7].

Анализ формирования угроз позволяет выявить некоторые свойства, характеризующие это понятие. Во-первых, следует отметить, что угроза – это следствие события, заключающегося в возникновении ситуации, влияющей на выполнения ПЗИ. Однако угрозы как результат деятельности определенных групп людей в отличие от риска, который в основном – следствие случайного события. Во-вторых, интенсивность воздействия угрозы на выполнения ПЗИ – случайная, изменяющаяся во времени.

Общим для понятий «угроза» и «риска» является влияния внешней среды на выполнения ПЗИ и то, что они – следствия ее воздействия на выполнения ПЗИ.

Анализ содержания угроз позволяет сформировать понятия «угроза».

Определение 1. Угроза есть влияющее на эффективность ПЗИ состояние среды, в которой выполняется комплексная целевая программа.

Кроме того, можно сделать вывод о существовании средств отражающих угрозы, которые влияют на уровень ее опасности.

Из этого следует возможность построения модели угрозы, которая представляет собой некоторою ПЗИ, причем существует хотя бы одна программа, или цель, уровень достижения, которых зависит от уровня выполнения модели угроз (МУ). Кроме того, МУ может иметь в качестве подпрограмм другие программы, влияющие на ее эффективность, с.е. меры парирования угрозы.

Таким образом, модель угрозы имеет все свойства ПЗИ с некоторыми особенностями, рассматриваемыми в дальнейшем.

Поставим в соответствие угрозе z_i некоторое число $0 \le D \le 1$, называемое степенью реализации угрозы, причем $D_i = \tau$ при полном отсутствии влияния угрозы и $D = 1$ при максимально возможном ее проявлении. Кроме того, будем характеризировать угрозу z_i вероятностью $p(t)$ вероятности ее реализации в момент времени t. Эту величину должны определить эксперты с помощью групповых методов экспертного оценивания [8].

Определения 2. Частный коэффициент W_{ij} влияния (ЧКВ) угрозы z_i на достижения ее непосредственной подцели g_j (степень выполнения программ p_j) есть прирост степени достижения подцелей g_j(степень выполнения программ p_j), полученный вследствие полной реализации угроз z_i.

В дальнейшем, если это не вызывает разночтений, будем употреблять термин подцели для обеспечения как цели, на степень достижения которой непосредственно влияет модель угрозы, так и программы, на степень выполнения которой влияет эта угроза.

Для более адекватного описания задач поддержки решений относительно комплексного целевого планирования с учетом угроз и рисков целесообразно учитывать изменения во времени их влияний. Поэтому в дальнейшем будем говорить о мгновенных значениях в момент времени t коэффициента влияния $W_{ihk}(t)$ угрозы z_i на достижение ее непосредственной подцели g_h, которое определяется из выражения

$$W_{ih}(t) = \begin{cases} 0, если\ t < \tau_{ih} \\ y(w_{ih}, t)\ иначе \end{cases}, \qquad (1)$$

где W_{ih} - стационарное значение коэффициента влияния (СКВ) угрозы z_i на непосредственную подцель g_h, τ_{ih}- экспертная оценка задержки влияния угрозы z_i подцель g_h; y – полиномиальная функция, которая описывает изменения коэффициента влияния во времени.

Поскольку достоверная информация относительно точности экспертных оценок коэффициентов полинома $y(w_{ih}, t)$ отсутствует, полином в (1) $y(-w_{ih}, t) = w_{ih}$, т.е. будем учитывать только задержку влияния угрозы на ее непосредственную подцель. Эту величину должны определять эксперты.

Стационарные значения коэффициентов влияния $w_{ih} \in w_h, i = (1, n_h)$ непосредственных подцелей подцели g_h, среди которых могут быть угрозы, удовлетворяет условию $\sum_{i=1}^{n_h} |W_{ih}| = 1$.

В общем случае угроз z_i есть менее родственная подцель нескольких подцелей $g_1, g_2, \ldots, g_h, \ldots, g_\tau$, причем любая подцель g_h имеет некоторое множество $G_h = \{G_{hk}\}$ альтернативных подмножеств совместимых подцелей, $G_{hk} \cap G_{hl} \neq \emptyset, k \neq l$. Поэтому возможен случай, когда $g_i \in G_{hk}, g_i \in G_{hl}, k \neq l$, и одна и та же угроза z_i будет иметь разные стационарные значения W_{ihk}, W_{ihl} коэффициента влияния на одну и ту же ее непосредственную подцель g_h, которые вычислены для разных альтернативных подмножеств G_{hk}, G_{hl} совместных подцелей.

Если достижение подцели g_i содействует достижению ее непосредственной подцели g_h, то ее СКВ $W_{ihk} > 0, иначе\ W_{ihk} < 0$. Из содержания понятия угроз следует, что частичные коэффициенты влияния программ, которые являются моделями соответствующих угроз, отрицательны. Заметим, что к началу процесса определения СКВ подцелей иерархий должна быть преобразования таким образом, чтобы СКВ всех подцелей были положительными. Это достигается заменой подцелей, которые отрицательно влияют на соответствующие подцели, подцелями, которых являются их логическими инверсиями.

Первой характеристикой, которая определяет тип угрозы, есть способ выражения условий и последствий ее реализации. Если условия реализации угрозы можно выразить результатом измерения некоторой одной конкретной величины – ресурса , то такая угроза называется количественной по входу, иначе – качественной.

Поскольку влияния МУ на достижение их непосредственных подцелей отрицательно, то для наихудшего случая степень их выполнения при отсутствии компенсирующих влияний принимается равной 1. При этом ресурс определяется как количественное выражение условий компенсации угрозы, которая приводит к тому, что степень выполнения МУ будет, равняется нулю. Так, ресурс программы, которая является модельно угрозы.

Если значения ресурса количественной по входу угрозы известно, то будем называть ее количественной по входу определенной. Значения ресурса такой угрозы однозначно определяется экспертами при построений иерархий целей. Если же значений ее ресурса достоверно неизвестно, то такую угрозу будем называть количественной по входу неопределенной. Для таких угроз определяются согласованные обобщенные экспертные оценки величины ресурса. Метод их определения приведен в [1].

Так как МУ всегда является непосредственной подцелью какой-нибудь цели или программы, он характеризуется результатом его выполнения. Если результат полного выполнения угрозы можно выразить эффектом, т.е. результатом измерения некоторой одной величины, то угроза называется количественной по входу, в противном случае – качественной по входу. Так эффект от выполнения МУ равняется экспертной оценке этих убытков в денежном измерении.

Определения 3. Непосредственные подцели g_i и g_j, в том числе и угрозы некоторой подцели g_s, называются совместимыми, если достижение одной не исключает возможности, или целесообразности достижения другой, и несовместимыми в противном случае.

Понятно, что при определении степени достижения подцели должны учитываться эффекты от достижения только множеств ее совместимых целей. Так как угроза действует независимо от исполнителей СЗИ, следует считать ее совместной с каждой из подцелей. Поэтому МУ входит в каждое подмножество совместимых подцелей той подцели, на достижение которой непосредственно влияет угроза.

Мгновенное значение $D_h(t)$ степени реализации угрозы z_h в момент времени t определятся таким образом.

$$D_h(t) = \begin{cases} 0, если \sup\limits_k \sum_i W_{ihk}(t) D_i(t) < T_h; \\ T_h, если \sup\limits_k \sum_i W_{ihk}(t) D_i(t) = T_h; \\ f\left\{\sup\limits_k \sum_i W_{ihk}(t) D_i(t)\right\}, если\ T_h < \sup\limits_k \sum_i W_{ihk}(t) D_i(t) \\ < 1 - \sum_q \left| W^{(-)}_{ghk}(t) \right| \\ 1, если \left[1 - \sum_q \left| W^{(-)}_{ghk}(t) \right|\right] \le \sup\limits_k \sum_i W_{ihk}(t) D_i(t) \le 1 \end{cases};$$

где T_h- порог угрозы z_h; $f\left[\sup\limits_k \sum_i W_{ihk}(t) D_i(t)\right]$ – функция степени реализации угрозы z_k, k – номер подмножества G_{hk} совместимых непосредственных подцелей угрозы, g_h; i – номер подцелей $g_i \in G_{hk}$. $W_{ihk}(t)$ – мгновенное значение в момент времени t частного коэффициента подцелей $g_i \in G_{hk}$ на достижение угрозы z_h, вычисленное при условии, что подцель g_i рассматривается как элемент подмножеств G_{hk} совместимых непосредственных подцелей угрозы z_h. $D_i(t)$ - мгновенное значения степени достижения подцели g_i в момент времени t, $W^{(-)}_{ghk}(t)$ - мгновенное значение в момент времени t частичного коэффициента влияния подцели $g_q \in G_{hk}$, отрицательно влияющей на z_h.

Важные частные случаи угроз – квазилинейная и пороговая угрозы.

Степень D_j выполнения квазилинейного МУ z_j определяется выражением

$$D_j = \begin{cases} \sup\limits_h \sum\limits_s W_{shj} D_{shj}, если \sup\limits_h \sum\limits_s W_{shj} D_{shj} \le 1; \\ 1, если \sup\limits_h \sum\limits_s W_{shj} D_{shj} > 1; \end{cases}$$

где h- номер подмножества G_{hj} совместных непосредственных подцелей МУ z_j; S – номер подцели $g_{shj} \in G_{hj}$; W_{shj} - частный коэффициент влияния подцели $g_{shj} \in G_{hj}$ на достижения угрозы z_j.

Выражения для вычисления степени D_j достижения пороговой угрозы z_i имеет вид:

$$D_i = \begin{cases} 1, если \sup\limits_h \sum\limits_s W_{shj} D_{shj} \ge \left| 1 - \sum\limits_{j \in J_i^-} W_j \right|; \\ 0\ иначе; \end{cases}$$

где J_i^- - множество номеров подцелей угрозы z_i с отрицательным влиянием.

Понятие риск характеризуется неопределенностью, связанной с возможностью возникновения в ходе реализации программ на защите неблагоприятных ситуаций и последствий [9].

Иначе говоря, риск есть следствия случайного события, заключающеюся в возникновении ситуации, влияющей на выполнения СЗИ. В более общей трактовые это события – следствие воздействия на выполнения СЗИ.

Таким образом, под риском будем понимать следствие случайного события, вызванного внешними относительно СЗИ факторами, которое состоит в возникновении ситуации влияющей на выполнения ЗИ.

Поскольку риск есть следствие случайного события, которое толи состоится, толи нет, то в зависимости от того, является разработчик СЗИ оптимистом или пессимистом, сущность события, которое вызывает риск, можно сформулировать в одном случае так, что его возникновение вызовет отрицательное влияния на выполнения ЗИ, или так, что оно будет иметь положительное влияние.

В зависимости от природы событий, которые вызывает риск, различают : технично-технологические, финансовые, социальные, политические, экологические риском участников программы (исполнителей создания СЗИ), риски обстоятельств непреодолимой силы (форс-мажор), специфические риски [9]. При этом одно и то же событие может вызвать риски, которые имеют совсем разные последствия для выполнения разных операций по защите.

Примером может быть такое влияния окружающей среды, как резкие колебания температуры h. Случайное событие $h > h_{min}$ вызовет отказ или изменение параметров аппаратуры при пониженной температуре, что позволит несанкционированно получить информацию при $h > h_{max}$ имеет место риск отказа или изменение параметров аппаратуры при перегреве, что также позволит злоумышленнику проникнуть на охраняемый объект, при $h_{min} \le h \le h_{max}$ имеет место нормальные условия. Таким образом, рассмотренные случайные события образуют полную группу, поэтому они, как вызванные ими риски, полярно не совместимы.

Пример свидетельствуют о том, что риски должны оцениваться, исходя из системного подхода, с учетом целы защиты, самой СЗИ и ее структуры.

Сформулируем некоторые понятия.

Определение 4. Фактором риска ϕ для СЗИ Р называется случайный процесс ξ_ϕ такой, что $\exists p_i \in P\left[v(p_i)\xi_\phi(\check{t}) \neq v(p_i)\Gamma\xi_\phi\right]$,где $v(p_i)\xi_\phi(t) \neq v(p_i)\Gamma\xi_\phi$ - относительная эффективность программы $p_i \in P$ с учетом фактора риска $\xi_\phi(t)$ и без учета его соответственно.

Определение 5. Индикатором риска ϕ фиктивная цель g_ϕ, единой подцелью которой есть фактор риска ϕ.

Возвращаясь к рассмотренному примеру, заметим, что фактор риска изменения температурных характеристик окружающей среды, есть подцель для таких индикаторов риска $g_{\phi 1}$ – изменения характеристик СЗИ при пониженной температуре; $g_{\phi 2}$ – изменения характеристик СЗИ при повышенной температуре. Подцели $g_{\phi 1}$, $g_{\phi 2}$ - индикаторы риска, полностью описываются функциями степени достижения цели. В общем случае мгновенное значение $D_h(t)$ степени достижения непосредственной подцели g_h в момент времени t определяются выражением (2).

При задании функции степени достижение цели – индикатора риска нудно учитывать такие особенности:

1. Поскольку пороги целей удовлетворяют условию [5,6]: $0 \le T_h \le 1$, то значения случайного процесса $\xi_\phi(t)$, задающею фактор риска ϕ, должно также удовлетворять условию $0 \le \xi_\phi(t), \le 1$;

2. Если $\left[\partial D\left(g_{\phi i}\right)/\partial\xi_{\phi}(t)\right] < 0$ (как это имеет место для примера риска при пониженной температуре окружающей среды), а в качестве фактора риска для цели $g_{\phi 1}$, являющейся индикатором этого риска, надо брать $\left[1-\xi_{\phi}(t)\right]$, вместо $\xi_{\phi}(t)$.

Таким образом, модели рисков, которые обусловлены уровнем h температуры окружающий среды следующие:

– Факторы риска $\xi_{\phi}^{(1)}(t) = h(t)/h_{max}$;

$\xi_{\phi}^{(2)}(t) = h(t)/h_{max}$;

– Индикатор риска пониженная температура – цель $g_{\phi 1}$ с порогом $T_{g_{\phi 1}} = h_{max}/h_{min}$; подцель – фактор риска $\xi_{\phi}^{(2)}(t)$ с частным коэффициентом влияния равным 1;

– Индикатор риска повышенная температура – цель $g_{\phi 2}$ с порогом $T_{g_{\phi 2}} = 1$; подцель – фактор риска $\xi_{\phi}^{(2)}(t)$ с частным коэффициентом влияния равным 1;

Для более детального описания рисков, которые связаны с фактором риска температурных колебаний окружающей внешней среды можно ввести несколько индикаторов риска, причем для любой из этих сформированных целей соответствует свое значения порога.

Выводы

Предложенный подход к поддержке принятия решений при формировании комплексных целевых программ с учетом угроз и рисков. Под угрозой понимается влияющее на эффективность программ реализации защиты объектов. Риск определен как следствие случайного события, вызванного влияния внешних относительно СЗИ факторов, который состоит в возникновении ситуации, влияющей на выполнения СЗИ своих функциональных обязанностей. Предположены модели угроз и риска. Моделью угрозы выступает программа, включаемая в иерархию целей комплексной программы, которая описывается степенью и вероятностью реализации. Модель риска состоит из двух компонентов: фактора риска, описываемого случайным процессом, некоторой фиктивной цели, называемой индикатором риска, единственной подцелью которой есть фактор риска. Эти компоненты включаются в граф, описывающий иерархию целей комплексной программы, и используются для определения относительной эффективности ее программ с учетом угроз и рисков.

Литература

1. Капустян М.В. – Качественная оптимизация информационных структур корпоративных сетей / Капустян М.В., Кудинов В.А., Пархуць Л.Т., Хорошко В.А.//Вісник ДУІКТ, т.5, №3, 2007-с.290-300.

2. Капустян М.В. – Кількісна оптимізація інформаційних структур корпоративних мереж/ Капустян М.В., Кудинов В.А., Пархуць Л.Т., Хорошко В.А.// Компютерні технології друкарства. Збір.наук.праць.- Львів, №16, 2006 – с.24-34.

3. Герасимов Б.М. – Системы поддержки принятия решений: проектирование применение, оценка эффективности/ Герасимов Б.М., Субач И.Ю. – Севастополь: Из центр СНИЯЭиП, 2004-с.318

4. Тарасов В.А. – Интеллектуальные системы поддержки принятия решений / Герасимов Б.М., Тарасов В.А., Левин И.А., Корнейчук В.А. – К.: МАКНС,2007-с.336.

5. Тоценко В.Г. – Согласование и агрегация оценок экспертов с учетом их компетенции при групповом оценивании альтернатив для поддержки принятия решений / Тоценко В.Г. //Проблемы управления и информатики, №4, 2002-с.128-141.

6. Грачева М.В. – Анализ проектных рисков/ Грачева М.В.-К.: ЗАО Финстатинформ, 1999-с.216.

7. Макаров И.М. – Теория выбора и принятия решений/ Макаров И.М., Виноградская Т.М., Рубчинский А.А., Соколов В.Б.-М.: Наука, 1982-с.328.

8. Емельянов С.В. - Многокритериальные методы принятия решений / Емельянов С.В., Ларичев О.И.-М.: Знания, 1985-с.31.

9. Корнійчук М.Т. – Ризик і безпека: кореляція категорій/ Корнійчук М.Т., Хорошко В.О., Дирнов В.М. // Захист інформації, Спец.випуск, 2008-с.15-21.

Разработаны математические модели угроз и рисков позволяющие , включать события, которые вызывают угрозу или риск, в иерархию целей программ по защите информации. Разработан способ количественного оценивания угрозы и риска.

Ключевые слова: система защиты информации, количественные показатели относительной эффективности система защиты информации, модели угроз и рисков, порог угрозы, фактор риска, индикатор риска.

Рецензент:д.т.н., проф. Козловський В.В.
Надійшла 10.10.2010

УДК 004:004.65

д.т.н., проф. **Лєнков С.В.** (ВІКНУ)
к.т.н., доц. **Пампуха І.В.** (ВІКНУ)
Джулій А.В. (УЕП, м.Хмельницький)

УЗАГАЛЬНЕННЯ ЗАДАЧІ НА ВИПАДОК СИСТЕМИ ЗАХИСТУ ІЗ КІНЦЕВИМ ЧИСЛОМ ДІАЛОГОВИХ КАНАЛІВ СПІЛКУВАННЯ З КОРИСТУВАЧАМИ

Вступ

Інформаційна безпека є складовою частиною інформаційних технологій - області, що розвивається надзвичайно високими темпами. Розробка сучасної системи інформаційної безпеки вимагає, з одного боку, відстеження швидких змін в інформаційних технологіях і погрозах, що з'являються, а з іншого боку - обліку реальних характеристик апаратного й програмного забезпечення корпоративних мереж і систем. Процедура придбання пристроїв інформаційної безпеки не складна. Істотно більш складним є рішення проблем, як захищати і які засоби безпеки застосовувати. Це рішення охоплює й керування інформаційною безпекою, включаючи планування, розробку політики безпеки й проектування необхідних процедур безпеки[1].

Постановка й проведення дослідження можливостей програмно – апаратних засобів захисту електронних джерел інформації являє собою актуальну дослідницьку задачу і має за мету розробку математичної моделі функціонування системи захисту на розглянутому проміжку часу тривалістю t.

Постановка задачі. Марківський процес, описаний у [2,3], у якому діюча система захисту (СЗ) послідовно накопичує у вершинах S_{2k} графа станів, кількість пропущених нелегальних користувачів визначимо як процес *одноканального діалогового спілкування*. У цьому процесі безпосередньо «робочими» вершинами служать вершини S_{2k+1} графа, k=0,1,2,... ... Саме в цих вершинах відбувається контрольний діалог програмно - апаратної структури СЗ із користувачами, що входять у контакт із інформаційною системою.

За своїм інтелектно-конструкторським рішенням схема побудови діалогу всередині кожної вершини S_{2k+1} залишається незмінною протягом усього процесу, що відбувається. У цьому значенні вершини S_{2k+1} графа нерозрізнені: у будь-який момент t (у будь-яку добу) це одна і та ж одноканальна типова СМО, яка характеризується своїми параметрами, дисципліною черги й основними показниками функціонування. Зокрема, це може бути одноканальна система з відмовами (рис. 1-а), або одноканальна СМО з обмеженим числом місць у черзі (рис. 1-б).