С.В. Скрыль, **Д.А. Голубков** **В.А. Половинкин**
доктор технических наук,
профессор

ПОКАЗАТЕЛИ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В ИНТЕГРИРОВАННЫХ СИСТЕМАХ БЕЗОПАСНОСТИ В УСЛОВИЯХ ОБЕСПЕЧЕНИЯ АНТИВИРУСНОЙ ЗАЩИТЫ

INFORMATION PROCESSES EFFICIENCY INDICATORS IN THE INTEGRATED SECURITY SYSTEMS UNDER ANTIVIRUS PROTECTION

Обосновывается вероятностный формат показателей эффективности информационных процессов в интегрированных системах безопасности (ИСБ) в условиях обеспечения антивирусной защиты. Приводятся математические зависимости для определения характеристик информационных процессов в ИСБ в условиях воздействия вредоносных программ и реализации процедур защиты информации от угроз ее искажения и блокирования компонентами антивирусной защиты.

The article explains the probabilistic format of efficiency indicators of information processes in the integrated security system (ISS) under antivirus protection. There are mathematical dependences to determine the characteristics of information processes in the ISS under the impact of malicious sofware and implementation procedures to protect information from threats of its distortion and blocking by antivirus protection components.

Характерным примером тенденции широкого внедрения информационных технологий как фактора повышения эффективности охранной деятельности служат интегрированные системы безопасности (ИСБ), являющихся системами охраны с наиболее высоким уровнем информатизации охранных функций. Вместе с тем, высокий уровень информатизации ИСБ приводит к необходимости учета ряда обстоятельств, связанных с негативными последствиями использования информационных технологий в качестве ключевой тенденции в концепции развития современных систем охраны. Одним из таких обстоятельств является подверженность процессов функционирования ИСБ угрозам информационной безопасности, приводящих к нарушению работоспособности ИСБ и, как следствие, значительному ущербу охраняемым объектам, которые они потенциально могут понести вследствие своей доступности для злоумышленников [1].

Потенциальной возможности несанкционированного воздействия на информацию в ИСБ способствуют два основных фактора: многообразие форм такого воздействия и рост профессионализма в использовании криминалом новейших достижений научно-технического прогресса в преступных целях. К таким достижениям следует отнести некоторые свойства информационных объектов, проявляемые ими в информационной среде, аналогичные свойствам объектов живой природы. Это позволило синтезировать совершенно новый тип компьютерных программ, известный как компьютерные вирусы. Такого рода программам присущи свойства репликативности, ассоциируемости и и полимофизма [2], т.е. те свойства, которые характерны их аналогам в живой природе — вирусам. Разрабатываемые с использованием вирусных механизмов

вредоносные программы представляют серьезную угрозу процессам функционирования в ИСБ, так как проявлением их воздействия в большинстве случаев является либо искажение информации, либо блокирование информационных процессов в этих системах. При этом оба эти последствия нарушения безопасности информации в ИСБ ведут к так называемым функциональным отказам данных систем, как систем, функционирующих по своему целевому назначению.

Это ставит весьма актуальную проблему разработки математических моделей для оценки эффективности механизмов антивирусной защиты в ИСБ и влияния их механизмов на эффективность информационных процессов в данных системах в условиях воздействия вредоносных программ.

Исходя из того, что характеристиками воздействия вредоносных программ на информацию ИСБ являются либо ее искажаемый объем, либо время блокирования информационных процессов в этих системах, определим аналогичные характеристики — объем рабочей среды, в которой реализуется программное обеспечение (ПО) ИСБ и время реализации процессов обработки информации в качестве базовых для оценки полноты и своевременности обработки информации как частных показателей эффективности информационных процессов в ИСБ [3].

Условие полноты рабочей среды, реализующей ПО ИСБ, определим в виде неравенства

$$V_{(по)} \geq V_{(нпо)}, \qquad (1)$$

в котором $V_{(по)}$ — объем рабочей среды, реализующей ПО ИСБ, а $V_{(нпо)}$ — минимально необходимая величина объема $V_{(по)}$, необходимого ИСБ для выполнения своих функций как системы, функционирующей по своему целевому назначению. При этом величина $V_{(по)}$ носит случайный характер, а величина $V_{(нпо)}$, будучи характеристикой минимально необходимого объема рабочей среды, реализующей ПО ИСБ, при котором еще обеспечивается работоспособное состояние ИСБ, является детерминированной. Это позволяет в качестве показателя полноты рабочей среды ИСБ, реализующей ее ПО, рассматривать вероятность выполнения условия (1):

$$C_{(рс)} = P(V_{(по)} \geq V_{(нпо)}) = 1 - P(V_{(по)} < V_{(нпо)}). \qquad (2)$$

Аналогичным образом условие своевременности обработки информации в ИСБ определим в виде неравенства

$$\tau_{(об)} \leq \tau_{(ноб)}, \qquad (3)$$

в котором $\tau_{(об)}$ — время обработки информации за определенный временной интервал (цикл обработки), а $\tau_{(ноб)}$ — максимально допустимая величина времени $\tau_{(об)}$ выполнения функций ИСБ как системы, функционирующей по своему целевому назначению. При этом величина $\tau_{(об)}$ носит случайный характер, а величина $\tau_{(ноб)}$, будучи характеристикой максимально допустимого времени обработки информации, при котором еще обеспечивается работоспособное состояние ИСБ, является детерминированной. Это позволяет в качестве показателя своевременности обработки информации в ИСБ рассматривать вероятность выполнения условия (3):

$$T_{(об)} = P(\tau_{(об)} \leq \tau_{(ноб)}) = 1 - P(\tau_{(ноб)} < \tau_{(об)}). \qquad (4)$$

В качестве характеристики возможностей антивирусных средств по защите информации в ИСБ от искажения рассмотрим объем $V_{(нис)}$ неискаженной рабочей среды программных средств этих систем. Будем полагать, что антивирусные средства обеспечивают целостность рабочей среды при выполнении условия

$$V_{(нис)} \geq V_{(мц)}, \qquad (5)$$

где $V_{(мц)}$ — минимальный объем неискаженной рабочей среды, при котором она еще считается целостной, иными словами работа размещенных в таком объеме рабочей среды программ еще обеспечивает работоспособное состояние ИСБ.

Случайный характер величины $V_{(нис)}$ приводит к необходимости рассматривать

выполнение неравенства (5) как случайное событие, которое аналогично (1) и (3), характеризуется вероятностью выполнения соответствующих условий, что позволяет использовать вероятность выполнения условия (5) в качестве показателя возможностей антивирусных средств ИСБ по защите информации в этих системах от искажения:

$$I = P(V_{(нис)} \geq V_{(мj)}) = 1 - P(V_{(нис)} < V_{(мj)}). \quad (6)$$

В качестве характеристики возможностей антивирусных средств по защите информации в ИСБ от блокирования рассмотрим время $\tau_{(дос)}$ доступа к информации в этих системах. Будем полагать, что антивирусные средства обеспечивают доступность информации в ИСБ при выполнении условия

$$\tau_{(дос)} \leq \tau_{(мд)}, \quad (7)$$

где $\tau_{(мд)}$ — максимальное время доступа к информации ИСБ, при котором еще обеспечивается доступность информации в ИСБ и, следовательно, ее работоспособное состояние.

Случайный характер величины $\tau_{(мд)}$ приводит к необходимости рассматривать выполнение неравенства (7) как случайное событие, которое аналогично (1), (3) и (5), характеризуется вероятностью выполнения соответствующих условий, что позволяет использовать вероятность выполнения условия (7) в качестве показателя возможностей антивирусных средств ИСБ по защите информации в этих системах от блокирования:

$$A = P(\tau_{(дос)} \leq \tau_{(мд)}) = 1 - P(\tau_{(мд)} < \tau_{(дос)}). \quad (8)$$

При обосновании показателя уровня угрозы искажения или блокирования вредоносными программами информации в ИСБ воспользуемся приведенными в [4] результатами надежностной интерпретации угроз нарушения целостности и доступности информации в этих системах как угроз нарушения их работоспособности.

Это позволяет вероятность воздействия угроз искажения информации в ИСБ представить как вероятность атаки типа «ложный объект вычислительной сети» [5]:

$$P_{(ло)} = 1 - e^{-\lambda_{(ло)} \cdot (t_{(ок)} - t_{(нач)})}, \quad (9)$$

где $\lambda_{(ло)}$ — интенсивность атак рассматриваемого типа на временном интервале от момента начала $t_{(нач)}$ до момента окончания $t_{(ок)}$ функционирования ИСБ.

Вероятность воздействия угроз блокирования информации в ИСБ, представляемая как вероятность атаки типа «отказ в обслуживании» [5], запишется в виде

$$P_{(оо)} = 1 - e^{-\lambda_{(оо)} \cdot (t_{(ок)} - t_{(нач)})}, \quad (10)$$

где $\lambda_{(оо)}$ — среднее число атак рассматриваемого типа на временном интервале [$t_{(нач)}$, $t_{(ок)}$] функционирования ИСБ.

Следует отметить, что объектами воздействия вредоносных программ в ИСБ могут быть и компоненты антивирусной защиты, реализуемые в общей с программным обеспечением этих систем рабочей среде. При этом компоненты антивирусной защиты, как и компоненты ПО, могут быть подвержены искажению, а их работа — блокированию.

С учетом специфики обеспечения антивирусной защиты в ИСБ функции защиты информации реализуются рядом программных компонентов, процедурно объединяемых в две группы: компоненты обнаружения вредоносных программ и компоненты их подавления.

С учетом этого обстоятельства объем $V_{(аз)}$ компонент антивирусной защиты в ИСБ будет равен:

$$V_{(аз)} = v_{(азо)} \circ v_{(азп)}, \quad (11)$$

где $v_{(азо)}$ и $v_{(азп)}$ — объем компонент обнаружения вредоносных программ и компонентов их подавления, соответственно; $\circ$ — знак композиции случайных величин.

Определим показатель полноты обеспечения защиты информации в ИСБ от искажения соответствующими компонентами антивирусной защиты как

$$C_{(аз)} = P(V_{(аз)} \geq V_{(мj)}) = 1 - P(V_{(аз)} < V_{(мj)}) = 1 - P(v_{(азо)} \circ v_{(азп)} < V_{(мj)}). \quad (12)$$

Аналогичным образом определим показатель своевременности реагирования на угрозы искажения информации в ИСБ соответствующими компонентами антивирусной защиты. При этом временная характеристика компонент антивирусной защиты — время $\tau_{(аз)}$ реализации ими своих функций — определяется как

$$\tau_{(аз)} = \tau_{(аво)} \circ \tau_{(азп)}, \qquad (13)$$

где $\tau_{(азо)}$ и $\tau_{(азп)}$ — время реализации компонентами обнаружения вредоносных программ и компонентами их подавления своих функций, соответственно.

Тогда выражение для показателя своевременности реагирования на угрозы искажения информации в ИСБ соответствующими компонентами антивирусной защиты представляется в виде

$$T_{(ази)} = P(\tau_{(аз)} \le \tau_{(си)}) = 1 - P(\tau_{(си)} < \tau_{(аз)}), \qquad (14)$$

где $\tau_{(си)}$ — время существования угрозы искажения информации в ИСБ воздействием вредоносных программ.

В этом случае показатель эффективности реализации антивирусными средствами функций защиты информации в ИСБ от искажения как комплексный показатель, отражающий полноту и своевременность реализации соответствующими компонентами антивирусной защиты этих функций, запишется в виде

$$E_{(зи)} = C_{(аз)} \cdot T_{(ази)} = (1 - P(v_{(азо)} \circ v_{(азп)} < V_{(мj)})) \cdot (1 - P(\tau_{(си)} < \tau_{(азо)} \circ \tau_{(азп)})). \qquad (15)$$

Аналогичным образом определим показатель эффективности реализации антивирусными средствами функций защиты информации в ИСБ от блокирования.

С учетом того, что антивирусными средствами осуществляется обнаружение и подавление всех типов вредоносных программ, функционально ориентированных как на искажение информации, так и на ее блокирование, показатель $C_{(аз)}$ полноты обеспечения защиты информации в ИСБ от искажения и от блокирования будет один и тот же.

Показатель же своевременности реагирования на угрозы блокирования информации в ИСБ представляется в виде

$$T_{(азб)} = P(\tau_{(аз)} \le \tau_{(сб)}) = 1 - P(\tau_{(сб)} < \tau_{(аз)}), \qquad (16)$$

где $\tau_{(сб)}$ — время существования угрозы блокирования информации в ИСБ воздействием вредоносных программ.

В этом случае показатель эффективности реализации антивирусными средствами функций защиты информации в ИСБ от блокирования как комплексный показатель, отражающий полноту и своевременность реализации соответствующими компонентами антивирусной защиты этих функций, запишется в виде

$$E_{(зб)} = C_{(аз)} \cdot T_{(азб)} = (1 - P(v_{(азо)} \circ v_{(азп)} < V_{(мj)})) \cdot (1 - P(\tau_{(сб)} < \tau_{(аво)} \circ \tau_{(азп)})). \qquad (17)$$

С целью аналитического представления показателя эффективности информационных процессов в ИСБ в условиях антивирусной защиты рассмотрим вероятностную интерпретацию группы событий, соответствующих реализации информационных процессов в ИСБ, воздействию вредоносных программ, искажающим или блокирующим информацию в этих системах, и процессов обеспечения защиты информации от угроз ее искажения или блокирования.

Представим выражение для среднего значения суммарного объема $V_{(рс)}$ рабочей среды ИСБ с учетом указанных событий:

$$\overline{V}_{(рс)} = \overline{V}_{(по)} + \overline{V}_{(аз)} + P_{(ло)} \cdot (1 - I) \cdot \overline{V}_{(и)}, \qquad (18)$$

где $\overline{V}_{(по)}$ и $\overline{V}_{(аз)}$ — средние значения случайных величин $V_{(по)}$ и $V_{(по)}$, соответственно;

$\overline{V}_{(и)}$ — среднее значение случайной величины объема искажаемой рабочей среды ИСБ (рассматривается как величина ущерба информационному процессу в ИСБ, наносимого данной системе за счет угроз искажения информации).

Выражение для среднего значения суммарного времени $\tau_{(с)}$ обработки информа-

ции, с учетом указанных событий имеет вид

$$\bar{\tau}_{(c)} = \bar{\tau}_{(об)} + \bar{\tau}_{(аз)} + P_{(оо)} \cdot (1 - A) \cdot \bar{\tau}_{(б)}, \qquad (19)$$

где $\bar{\tau}_{(об)}$ и $\bar{\tau}_{(аз)}$ — средние значения случайных величин $\tau_{(об)}$ и $\tau_{(аз)}$, соответственно;

$\bar{\tau}_{(б)}$ — среднее значение случайной величины времени нарушения доступности информации в ИСБ (рассматривается как величина ущерба информационному процессу в ИСБ, наносимого данной системе за счет угроз искажения информации).

В предположении о независимости показателей (2) — полноты рабочей среды ИСБ, реализующей ее ПО, и (3) — своевременности обработки информации в этой системе, а также в соответствии с интерпретацией параметров этих показателей выражениями (18) и (19) показатель E эффективности информационных процессов в системах рассматриваемого класса в условиях антивирусной защиты определяется в соответствии с выражением

$$E = C_{(рс)} \cdot T_{(об)} = (1 - P(V_{(рс)} < V_{(нпо)})) \cdot (1 - P(\tau_{(нобр)} < \tau_{(с)})). \qquad (20)$$

Вероятностный формат рассмотренных показателей и его сходство с представлением функции распределения вероятностей позволяет применить методы теории вероятностей [6] для исследования информационных процессов в ИСБ в условиях антивирусной защиты.

С учетом выполняемых в ИСБ процедур обработки информации величину объема $V_{(по)}$, необходимого ИСБ для выполнения своих функций, представим в виде

$$V_{(по)} = v_{(ар)} \circ v_{(дозз)} \circ v_{(дтс)} \circ v_{(дио)} \circ v_{(тс)}, \qquad (21)$$

где $v_{(ар)}$ — объем рабочей среды, реализующей программные компоненты администрирования работы ЛВС ИСБ; $v_{(дозз)}$ — объем рабочей среды, реализующей программные компоненты ведения банка данных охраняемых зон; $v_{(дтс)}$ — объем рабочей среды, реализующей программные компоненты ведения банка данных тревожных ситуаций; $v_{(дио)}$ — объем рабочей среды, реализующей программные компоненты ведения банка данных используемого оборудования; $v_{(тс)}$ — объем рабочей среды, реализующей программные компоненты обработки информации по текущему состоянию охраняемого объекта.

Величину времени $\tau_{(об)}$ времени обработки информации в ИСБ представим в виде

$$\tau_{(об)} = \tau_{(ар)} \circ \tau_{(дозз)} \circ \tau_{(дтс)} \circ \tau_{(дио)} \circ \tau_{(тс)}, \qquad (22)$$

где $\tau_{(ар)}$ — время реализации программными компонентами администрирования работы ЛВС ИСБ своих функций; $\tau_{(дозз)}$ — время реализации программными компонентами ведения банка данных охраняемых зон своих функций; $\tau_{(дтс)}$ — время реализации программными компонентами ведения банка данных тревожных ситуаций своих функций; $\tau_{(дио)}$ — время реализации программными компонентами ведения банка данных используемого оборудования своих функций; $\tau_{(тс)}$ — время реализации программными компонентами обработки информации по текущему состоянию охраняемого объекта своих функций.

Исходя из (21) и (22), а также положений центральной предельной теоремы теории вероятностей [6], можно считать, что величины $V_{(по)}$ и $\tau_{(об)}$ распределены по нормальному закону.

При определении среднего значения случайной величины объема $V_{(аз)}$ компонент антивирусной защиты в ИСБ, воспользуемся представлением выражения (11) как функции от вероятностных характеристик величин $v_{(аво)}$ и $v_{(авп)}$ объемов компонент обнаружения вредоносных программ и компонент их подавления, соответственно [7]:

$$\bar{V}_{(аз)} = \int_{v_{(азо)\min}}^{\infty} y \int_{v_{(азп)\min}}^{\infty} f^{(v)}_{(азо)}(y - z) \cdot f^{(v)}_{(азп)}(z)\, dz\, dy, \qquad (23)$$

где $f^{(v)}_{(азо)}$ и $f^{(v)}_{(азп)}$ — плотности распределений случайных величин $v_{(аво)}$ и $v_{(авп)}$, соответственно, а $v_{(азо)\min}$ и $v_{(азп)\min}$ — их минимальные значения.

Аналогичным образом при определении среднего значения случайной величины времени $\tau_{(аз)}$ реализации компонентами антивирусной защиты своих функций, воспользуемся представлением выражения (13) как функции от вероятностных характеристик величин времен $\tau_{(азо)}$ и $\tau_{(азп)}$ реализации компонентами обнаружения вредоносных программ и компонентами их подавления своих функций, соответственно:

$$\overline{\tau}_{(аз)} = \int_{\tau_{(азо)\min}}^{\infty} y \int_{\tau_{(азп)\min}}^{\infty} f^{(\tau)}_{(азо)}(y-z)\cdot f^{(\tau)}_{(азп)}(z)\,dz\,dy, \qquad (24)$$

где $f^{(\tau)}_{(азо)}$ и $f^{(\tau)}_{(азп)}$ — плотности распределений случайных величин $\tau_{(азо)}$ и $\tau_{(авп)}$, соответственно, а $\tau_{(аво)\min}$ и $\tau_{(азп)\min}$ — их минимальные значения.

Частные случаи построения математических моделей на основе выражений (23) и (24) для равномерного, экспоненциального и нормального законов распределения случайных величин приводятся в [7].

С целью аналитического представления показателя полноты $C_{(аз)}$ обеспечения защиты информации в ИСБ от искажения соответствующими компонентами антивирусной защиты поставим в соответствие минимальному объему $V_{(мj)}$ неискаженной рабочей среды, при котором она еще считается целостной, предельное значение времени $\tau_{(мj)}$ реализации программ, размещенных в пределах данного:

$$V_{(мj)} = \varphi(\tau_{(мj)}), \qquad (25)$$

где $\varphi(*)$ — оператор линейного преобразования.

Опишем формально процесс реализации функций антивирусной защиты от угроз искажения и блокирования информации в ИСБ как элементарный поток событий.

При этом такой поток формально рассматривается как реакция на воздействие вредоносных программ. С учетом обоснованных в [4] ограничений на формальное представление угроз нарушения целостности и доступности информации в ИСБ предположим, что случайные величины $\tau_{(мj)}$, $\tau_{(си)}$ и $\tau_{(сб)}$ аппроксимируются экспоненциальными законами распределения.

С учетом этого выражения (12), (14) и (16) для показателей полноты обеспечения антивирусными средствами функций защиты информации в ИСБ и своевременности реагирования на угрозы искажения и блокирования информации в ИСБ, соответственно, представляются в виде

$$C_{(аз)} = 1 - \exp\left(-\frac{\overline{V}_{(аз)} - V_{(мщ)\min}}{\overline{V}_{(мщ)}}\right), \qquad (26)$$

где $\overline{V}_{(мщ)}$ — среднее значение случайной величины $V_{(мj)}$;

$V_{(мj)\min}$ — минимальное значение случайной величины $V_{(мj)}$;

$\overline{V}_{(аз)}$ — среднее значение случайной величины $V_{(аз)}$;

$$T_{(ази)} = \exp\left(-\frac{\overline{\tau}_{(аз)} - \tau_{(си)\min}}{\overline{\tau}_{(си)}}\right), \qquad (27)$$

где $\overline{\tau}_{(си)}$ — среднее значение случайной величины $\tau_{(си)}$;

$\tau_{(си)\min}$ — минимальное значение случайной величины $\tau_{(си)}$;

$\overline{\tau}_{(аз)}$ — среднее значение случайной величины $\tau_{(аз)}$;

$$T_{(азб)} = \exp\left(-\frac{\overline{\tau}_{(аз)} - \tau_{(сб)\min}}{\overline{\tau}_{(сб)}}\right), \qquad (28)$$

где $\overline{\tau}_{(сб)}$ и $\tau_{(сб)\min}$ — среднее и минимальное значения случайной величины $\tau_{(сб)}$, соответственно.

Исходя из изложенного, а также учитывая (26), (27) и (28), выражение (20) для показателя эффективности информационных процессов в ИСБ в условиях антивирусной защиты представим в виде

$$E = C_{(рс)} \cdot T_{(об)} = \left[1 - \left(\Phi^*\left(\frac{\overline{V}_{(рс)} - \overline{V}_{(ппо)}}{\sigma^{(V)}_{(рс)}}\right) + \Phi^*\left(\frac{\overline{V}_{(рс)}}{\sigma^{(V)}_{(рс)}}\right)\right)\right] \cdot \left[\Phi^*\left(\frac{\overline{\tau}_{(азб)} - \overline{\tau}_{с}}{\sigma^{(\tau)}_{(с)}}\right) + \Phi^*\left(\frac{\overline{\tau}_{(ф)}}{\sigma^{(\tau)}_{(с)}}\right)\right], \qquad (29)$$

где $\Phi^*(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} dt$ — **интеграл вероятностей** [6], **в котором** $t = \frac{u - \overline{u}}{\sigma_u}$;

$$\overline{V}_{(рс)} = \overline{V}_{(ппо)} - P_{(ло)} \cdot \left(1 - \left(1 - \exp\left(-\frac{\overline{V}_{(аз)} - V_{(мщ)\min}}{\overline{V}_{(мщ)}}\right)\right) \cdot \exp\left(-\frac{\overline{\tau}_{(аз)} - \tau_{(сиг)\min}}{\overline{\tau}_{(сиг)}}\right)\right) \cdot \overline{V}_{(и)}; \qquad (30)$$

$$\begin{aligned} \overline{\tau}_{(с)} = {} & \overline{\tau}_{(об)} + \int_{\tau_{(п)1\min}}^{\infty} y \int_{\tau_{(п)2\min}}^{\infty} f^{(\tau)}_{(азо)}(y - z) f^{(\tau)}_{(азп)}(z) dz\, dy + \\ & + P_{(оо)} \cdot \left(1 - \left(1 - \exp\left(-\frac{\overline{V}_{(аз)} - V_{(мщ)\min}}{\overline{V}_{(мщ)}}\right)\right) \cdot \exp\left(-\frac{\overline{\tau}_{(аз)} - \tau_{(сб)\min}}{\overline{\tau}_{(сб)}}\right)\right) \cdot \overline{\tau}_{(б)}; \end{aligned} \qquad (31)$$

$\sigma^{(V)}_{(рс)}$ и $\sigma^{(\tau)}_{(с)}$ — среднеквадратичное отклонение случайных величин $V_{(рс)}$ и $\tau_{(с)}$, соответственно.

Выражения (29), (30) и (31) следует рассматривать как аналитические модели для оценки эффективности информационных процессов в ИСБ в условиях воздействия вредоносных программ и реализации процедур защиты информации от угроз ее искажения и блокирования компонентами антивирусной защиты.

ЛИТЕРАТУРА

1. Зарубин В.С., Гурченко С.В., Фамильнов А.Р. Классификация информационных угроз интегрированных систем безопасности // Информация и безопасность: региональный научно-технический журнал. — Воронеж, 2009. — Т. 12. — Ч.3. — С. 425 — 428.

2. Чагина Л.В., Скрыль К.С., Сушков П.Ф. Вирусологическая типизация вредоносных программ // Наука производству. — 2005. — Вып. 6 (86). — С. 12—17.

3. Информатика: учебник для высших учебных заведений МВД России. — Т. 1. Информатика: Концептуальные основы / В.А. Минаев [и др.]. — М.: Маросейка, 2008. — 464 с.

4. О некоторых допущениях в математической интерпретации угроз нарушения целостности и доступности информации в компьютерных системах / В.С. Зарубин [и др.]// Информация и безопасность: региональный научно-технический журнал. — Воронеж, 2009. — Т. 12. — Ч.4. — С. 625 — 626.

5. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet — М.: ДМК, 2002. — 400 с.

6. Вентцель Е.С. Теория вероятностей: учебник. — 11-е изд. — М.: КноРус, 2010. — 664 с.

7. Оценка защищенности информационных процессов в территориальных ОВД: модели исследования: монография / под ред. С.В. Скрыля. — Воронеж: Воронежский институт МВД России, 2009. — 217 с.