ИННОВАЦИОННЫЕ СИСТЕМЫ, ПРОЦЕССЫ И ОБОРУДОВАНИЕ

УДК 681.3

Декан факультета Н.С. Родионова
(Воронеж. гос. ун-т инж. технол.) факультет экономики и управления, тел. (473) 255 38 82
Начальник кафедры С.В. Белокуров
(Воронежский институт ФСИН России) кафедра математики и естественнонаучных дисциплин, тел. (473) 260 68 20
Профессор С.В. Скрыль
(Воронежский институт ФСИН России) кафедра технических комплексов охраны и связи, тел. (473) 260 68 18

Показатель своевременности обработки информации в условиях оптимизации управления механизмами антивирусной защиты

В статье приводится обоснование показателя своевременности обработки информации в инфокоммуникационных системах органов внутренних дел в условиях оптимизации механизмов антивирусной защиты. Реализация этого показателя дает возможность описывать механизмы реализации информационно-аналитического процесса и процесса антивирусной защиты от угроз нарушения доступности информации такими их характеристиками, через которые можно выразить все остальные параметры этих процессов.

The paper outlines the rationale index timeliness of information processing in information and communication systems of internal affairs while optimizing the mechanisms of anti-virus protection. Implementation of this parameter allows to describe the mechanisms for the implementation of information-analytical process and the anti-virus protection from threats to the availability of information such violations of their characteristics, through which we can express all the other parameters of these processes.

Ключевые слова: защита информации, управление, инфокоммуникационная система.

Решение задачи формирования оптимальных вариантов средств антивирусной защиты в информационно-аналитической инфраструктуре инфокоммуникационных системам органов внутренних дел (ИАИ ИКС ОВД) связано с оценкой соответствующих показателей. В основу синтеза таких показателей положен сформулированный в [2, 3] принцип однородности показателей своевременности обработки информации в ИАИ и эффективности антивирусной защиты от угроз нарушения доступности информации.

Реализация этого принципа дает возможность описывать механизмы реализации информационно-аналитического процесса и процесса антивирусной защиты от угроз нарушения доступности информации такими их характеристиками, через которые можно выразить все остальные параметры этих процессов.

Учитывая то обстоятельство, что информационно-аналитические процессы в ИАИ ИКС и процессы антивирусной защиты от угроз нарушения доступности информации относятся к информационным процессам, для определения соответствующих характеристик будем использовать ряд положений теоретических основ информатики [1].

Следует отметить, что качество информации и качество ее защиты как системные категории подчинены ряду закономерностей. Концентрировано эти закономерности изложены в целом ряде работ, среди которых следует выделить [1], в которой рассматриваются проблемы оценки качества одного из трех основных состояний защищенности информации - ее конфиденциальности.

Учитывая то обстоятельство, что к этим состояниям относится и доступность информации, изложенные в [2, 3] закономерности характерны и для исследуемых в данной работе вопросов.

В соответствии с [1] степень удовлетворения потребностей информационной деятельности в обеспечении защиты информации от нарушения ее доступности определяется качеством такой деятельности. В общем случае под качеством понимают совокупность свойств и характеристик продукции или услуги, которые придают изделию или услуге спо-собность соответствовать установленным или возможным требованиям. Данное понятие интуитивно легко воспринимается. Однако при приложении его к деятельности по защите информации от нарушения ее доступности становится очевидным, что отсутствуют как перечень семантически определенных свойств и характеристик, так и области допустимых их значений.

В связи с этим ограничимся пониманием следующих аспектов проблемы качества обеспечения защиты информации от нарушения ее доступности:

1. Качество обеспечения защиты информации от нарушения ее доступности есть обобщенная характеристика потребительских свойств данного вида деятельности. При этом потребительская стоимость доступной информации определяется исходя из реального ущерба пользователю от ее блокирования.

2. Требуемый и реально предоставляемый уровни качества обеспечения защиты информации от нарушения ее доступности определяются соответственно потребностями в защите информации и применяемыми технологиями противодействия ее блокированию.

3. Требуемый и предоставляемый уровни качества защиты информации от нарушения ее доступности есть функции времени.

4. Общая тенденция изменений требуемого и предоставляемого качества защиты информации от нарушения ее доступности заключается в одновременном росте пользовательских требований и снижении существующего качества обеспечения защиты.

Из последнего утверждения следует, что уровни требуемого и реально предоставляемого качества не совпадают. Обозначим соответственно: Q(т)(t) - требуемый и Q(c)(t) - предоставляемый (существующий) уровни качества. Тогда в любой i -й момент времени может существовать одно из следующих отношений:

1. Качество обеспечения защиты информации от нарушения ее доступности не ниже требуемого:

$$Q_{(c)}(t_i) \geq Q_{(m)}(t_i) \qquad (1)$$

2. Качество обеспечения защиты информации от нарушения ее доступности ниже требуемого:

$$Q_{(c)}(t_i) < Q_{(m)}(t_i) \qquad (2)$$

Графическое представление динамики требуемого и предоставляемого качества показано на рисунке 1.

Приведенное на рисунке 1 графическое представление динамики требуемого и предоставляемого качества обеспечения защиты информации от нарушения ее доступности формально определяется выражениями:

$$Q_{(m)}(t_2) > Q_{(m)}(t_1) \qquad (3)$$

и

$$Q_{(c)}(t_2) < Q_{(c)}(t_1) \qquad (4)$$

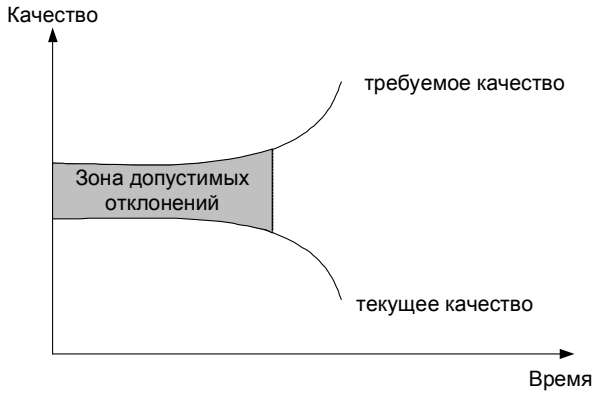

Рисунок 1 - Тенденция изменения требуемого и предоставляемого качества обеспечения защиты информации от нарушения ее доступности

На отдельных и относительно коротких временных интервалах могут существовать частные варианты отношений качества:

1. Пользовательские требования не меняются, а качество обеспечения защиты информации от нарушения ее доступности снижается:

$$Q_{(m)} = \text{const};\ Q_{(c)}(t_1) > Q_{(c)}(t_2) \qquad (5)$$

2. Рост пользовательских требований к обеспечению защиты информации от нарушения ее доступности при неизменном качестве:

$$Q_{(c)} = \text{const};\ Q_{(m)}(t_2) > Q_{(m)}(t_1) \qquad (6)$$

На рисунок 1 показана некоторая зона допустимых несоответствий ΔQ. Несоответствие между фактическим и требуемым состояниями на величину большую зоны допустимых несоответствий порождает необходимость деятельности (управления) по поддержанию каче-

ства обеспечения защиты информации от нарушения ее доступности в зоне допустимых значений.

В случае, описываемом выражением (5), управление состоит в реконструкции организационно-технической инфраструктуры механизмов защиты.

Цель реконструкции - поддержание качества обеспечения защиты информации от нарушения ее доступности в заданных пределах (рациональность). Формально цели реконструкции можно представить выражением:

$$Q_{(o)}(t_{(\partial)}) - Q_{(c)}(t_{(n)}) \leq \Delta Q, \qquad (7)$$

где $Q_{(c)}(t_{(\partial)})$ и $Q_{(c)}(t_{(n)})$ – соответственно качество обеспечения защиты информации от нарушения ее доступности до и после реконструкции механизмов защиты.

В случае, когда пользовательские требования не меняются, а качество обеспечения защиты информации от нарушения ее доступности снижается, управление состоит в реконструкции организационно-технической инфраструктуры информационной системы. Цель реконструкции - поддержание качества обеспечения защиты информации от нарушения ее конфиденциальности в заданных пределах (рациональность).

При изменениях внешней или внутренней ситуации, определяющих рост пользовательских требований к качеству обеспечения защиты информации от нарушения ее доступности, возникает необходимость совершенствования последнего. Под совершенствованием защиты информации от нарушения ее доступности будем понимать управленческую деятельность по приведению ее на новый уровень качества.

Будем полагать, что в целом качество обеспечения защиты информации от нарушения ее доступности определяется технологией защиты. Технология защиты информации, в свою очередь, является результатом развития информационных технологий, нормативной базы и предшествующего объема организационно-технических работ в данной сфере.

Перечисленные факторы являются стохастическими и слабо коррелированны. Тем не менее, они системно взаимосвязаны в части влияния на качество обеспечения защиты информации. В частности, такие компоненты технологии защиты информации как техническая и нормативная база, являются зависимыми от структурных решений. Поэтому можно полагать, что качество обеспечения защиты информации от нарушения ее доступности есть функция состояния системы защиты информации (СЗИ).

Обоснованный выбор требуемого уровня качества обработки информации в процессе информационно-аналитической деятельности является крайне сложной проблемой, поэтому целесообразно исходить из посылки, что качество любой деятельности может быть адекватно оценено качеством ее результата.

Результатом обработки информации в ИАИ ИКС органа внутренних дел является своевременное обеспечение данными сотрудников соответствующих его подразделений. Из этого следует, что для оперирования понятием качества обработки информации необходимо обладать, во-первых, определенным набором свойств и характеристик самой информации и, во-вторых, уметь их оценивать.

Следует отметить, что, несмотря на многообразие проявляемых в процессе обработки информации ее свойств, сложность, размеры и организационную природу информационно-аналитических процессов в ИАИ ИКС, широкий диапазон и динамику пользовательских требований, имеется возможность существенно сузить значительное и варьируемое количество различных, слабо связанных или несвязанных между собой показателей, характеризующих [2, 3]:

- объективное качество процесса обработки информации в ИАИ, являющееся инвариантом для условий ее функционирования, архитектуры и реализуемых информационных технологий;

- субъективное качество процесса обработки информации в ИАИ - способность результатов обработки отвечать определенным требованиям.

В соответствии с обоснованным в п. 1.2 положением о временных параметрах процесса обработки информации в ИАИ ИКС как наиболее целесообразной формы описания функциональных возможностей этих систем, объективное качество процесса обработки информации в ИАИ будем характеризовать временем $\tau_{(об)}$ реализации процедур обработки информации, под которым будем понимать временной интервал с момента начала реализации информационно-аналитического процесса в ИАИ до момента его завершения [1].

Аналогичным образом объективное качество процесса защиты информации от угроз нарушения ее доступности в ИАИ будем характеризовать временем $\tau_{(з)}$ реализации процедур защиты информации от такого рода угроз, под которым будем понимать временной интервал с момента начала реализации процедур защиты до момента их завершения [1].

Исходя из этих же положений, к субъ-

ективным показателям качества обработки информации в ИАИ ИКС в условиях обеспечения ее защиты от угроз нарушения доступности относятся [1]:

- своевременность $\varepsilon_{(c)}$ обработки информации, характеризующая время, в течение которого информация имеет полезность для решения предметных задач;

- доступность $\varepsilon_{(\partial)}$ информации для обработки, характеризующая способность обеспечивать свободный доступ к ней по мере возникновения необходимости.

По сути, как своевременность обработки информации, так и доступность информации для обработки являются нормированными показателями допустимого времени реализации информационно-аналитического процесса и процесса защиты информации от воздействия угроз нарушения доступности и информации в ИАИ, соответственно.

Формальными условиями своевременности обработки информации в ИАИ ИКС являются следующие:

$$\varepsilon_{(c)} = 1 \text{ при } \tau_{(об)} \le \tau_{(m)} \qquad (8)$$

и

$$\varepsilon_{(c)} = 0 \text{ при } \tau_{(об)} > \tau_{(m)}, \qquad (9)$$

где $\tau_{(m)}$ – требуемое время удовлетворения пользовательских потребностей.

Будем полагать, что условие (8) является обязательным требованием к реализации процедур информационно-аналитического процесса. В противном случае (условие (9)) реализация информационно-аналитического процесса в ИАИ теряет смысл.

Аналогичным образом формальными условиями доступности информации ИАИ ИКС для обработки являются следующие:

$$\varepsilon_{(\partial)} = 1 \text{ при } \tau_{(з)} \le \tau_{(\partial)} \qquad (10)$$

и

$$\varepsilon_{(\partial)} = 0 \text{ при } \tau_{(з)} > \tau_{(\partial)}, \qquad (11)$$

где $\tau_{(\partial)}$ – допустимое время обеспечения доступа к информации в ИАИ.

Как и в случае условия (8), условие (10) является обязательным требованием к реализации процедур защиты информации в ИАИ ИКС от угроз нарушения ее доступности. В противном случае (условие (11)) реализация процедур защиты теряет смысл.

Представление показателей своевременности обработки информации в ИАИ ИКС и ее доступности в виде (8) и (9) соответственно, позволяет дать их количественное представление. Следует отметить, что как при реализации технологий обработки информации, так и при реализации технологий ее защиты это обстоятельство является определяющим.

Анализируя условия (8) и (9) применительно к исследуемым в работе вопросам становится очевидным следующее:

1) требуемое время удовлетворения пользовательских потребностей $\tau_{(m)}$ представляет собой нормативное время обработки информации в ИАИ ИКС ОВД, а допустимое время обеспечения доступа к информации в ИАИ $\tau_{(\partial)}$ определяется характером воздействия вредоносной программы;

2) условия (8) и (9) являются обязательными требованиями к реализации процедур обработки и защиты информации в ИАИ ИКС от нарушения ее доступности;

3) показатели своевременности обработки информации в ИАИ ИКС и ее доступности носят вероятностный характер [2, 3]:

$$0 \le \varepsilon_{(c)} \le 1;\ 0 \le \varepsilon_{(\partial)} \le 1 \qquad (12)$$

С целью определения формы показателя своевременности обработки информации в ИАИ ИКС, по аналогии с [1], условимся использовать время $\tau_{(об)}$ реализации цикла обработки информации и его требуемое значение $\tau_{(m)}$. При этом под временем $\tau_{(об)}$ реализации цикла обработки информации в ИАИ ИКС будем понимать время реализации схемы обработки информации, циркулирующей в ИАИ с момента получения данных или команд на обработку до момента выдачи обработанных данных.

Информационно-аналитический процесс в ИАИ ИКС считается реализованным своевременно, если время $\tau_{(об)}$ не превышает $\tau_{(m)}$, т.е. при выполнении неравенства:

$$\tau_{(об)} \le \tau_{(m)}. \qquad (13)$$

Исходя из того, что входящие в данное неравенство величины являются случайными, а его выполнение является случайным событием, условие (13) опишем соответствующей вероятностью.

Данная вероятность представляет собой среднее количество своевременно реализованных запросов на обработку информации в ИАИ ИКС относительно их общего числа на i-ом, i=1, 2, …, I временном интервале $\Delta t_i = [t_{(н)i},\ t_{(к)i}]$ функционирования ИАИ:

$$\varepsilon_{(c)i} = P_i(\tau_{(об)i} \le \tau_{(m)i}) = \frac{1}{J_i}\sum_{j=1}^{J_i}\delta_{i,j}, \qquad (14)$$

где $\delta_{i,j} = \begin{cases} 1, & \text{если } \tau_{(об)i,j} \le \tau_{(m)i,j} \\ 0, & \text{в противном случае} \end{cases}$; $\tau_{(об)i,j}$ - время реализации j-го запроса на временном интервале $[t_{(н)i}, t_{(к)i}]$; $\tau_{(m)i,j}$ - требуемое время реализации j-го запроса на рассматриваемом временном интервале; J_i - количество запросов на обработку информации в ИАИ

ИКС на временном интервале $[t_{(н)i}, t_{(к)i}]$.

Принимая во внимание многоэтапность информационно-аналитического процесса в ИАИ ИКС ОВД, время $\tau_{(об)}$ можно представить как комбинацию семи случайных величин:

- времени $\tau_{(1)}$ реализации процедуры приема входных потоков информации;
- времени $\tau_{(2)}$ реализации процедуры обработки информации в реальном масштабе времени;
- времени $\tau_{(3)}$ реализации процедуры базовой обработки информации;
- времени $\tau_{(4)}$ реализации процедуры аналитической обработки информации;
- времени $\tau_{(5)}$ реализации процедуры ведения баз регламентных данных;
- времени $\tau_{(6)}$ реализации процедуры функциональной обработки информации;
- времени $\tau_{(7)}$ реализации процедуры обработки выходных данных.

В этом случае время реализации процедур информационно-аналитического процесса в ИАИ ИКС ОВД можно записать в виде:

$$\tau_{(об)} = \tau_{(1)} \circ \tau_{(2)} \circ \tau_{(3)} \circ \tau_{(4)} \circ \tau_{(5)} \circ \tau_{(6)} \circ \tau_{(7)}, \qquad (15)$$

где $\circ$ - знак композиции случайных величин.

Требуемое время $\tau_{(m)}$ реализации процедур информационно-аналитического процесса в ИАИ ИКС ОВД, несмотря на нормативные рамки в общем случае носит ситуативный характер.

С учетом изложенного можно сделать вывод о том, что вероятность $P(\tau_{(об)} \leq \tau_{(m)})$ является достаточно полной характеристикой своевременной реализации процедур информационно-аналитического процесса в ИАИ ИКС ОВД, что является основанием целесообразности использования ее в качестве соответствующего показателя:

$$\varepsilon_{(c)} = P(\tau_{(об)} \leq \tau_{(m)}) \qquad (16)$$

Из (16) очевидна функциональная зависимость показателя своевременности обработки информации в ИАИ ИКС от характеристик ее временного ресурса.

Таким образом, в статье приводится обоснование показателя своевременности обработки информации в инфокоммуникационных системах органов внутренних дел в условиях оптимизации механизмов антивирусной защиты.

Реализация этого показателя дает возможность описывать механизмы реализации информационно-аналитического процесса и процесса антивирусной защиты от угроз нарушения доступности информации такими их характеристиками, через которые можно выразить все остальные параметры этих процессов.

ЛИТЕРАТУРА

1 Основы информационной безопасности [Текст]: учебник для высших учебных заведений МВД России / под ред. В.А. Минаева, С.В. Скрыля. - Воронеж: Воронежский институт МВД России, 2001. – 464 с.

2 Белокуров, С.В. Методы и средства анализа эффективности систем информационной безопасности при их разработке [Текст]: монография / С.В. Белокуров, С.В. Скрыль, В.К. Джоган и др. – Воронеж: Воронежский институт МВД России, 2012. – 83 с.

3 Белокуров, С.В. Модели и алгоритмы автоматизированного контроля эффективности систем защиты информации в автоматизированных системах [Текст]: монография / С.В. Белокуров, С.В. Скрыль, В.К. Джоган и др. – Воронеж: Воронежский институт МВД России, 2012. – 116 с.

REFERENCES

1 Fundamentals of information security [Text]: textbook for universities MIA Russia / ed. by V.A. Minayev, S.V. Skril. – Voronezh: Voronezh Institute of MIA of Russia, 2001. - 464 p.

2 Belokurov, S.V. Methods and tools for analysis of the effectiveness of information security systems in their design [Text]: monograph / S.V. Belokurov, S.V. Skril, V.K. Joghan et al. – Voronezh: Voronezh Institute of MIA of Russia, 2012. - 83 p.

3 Belokurov, S.V. Models and algorithms for the automated control of the effectiveness of information security systems in automated systems [Text]: monograph / S.V. Belokurov, S.V. Skril, V.K. Joghan et al. – Voronezh: Voronezh Institute of MIA of Russia, 2012. - 116 p.