УДК 681.3

Профессор Н.С. Родионова
(Воронеж. гос. ун-т. инж. технол) факультет экономики и управления. тел. (473) 255-38-82
E-mail: rodionovast@mail.ru
начальник кафедры С.В. Белокуров
(Воронеж, ВИ ФСИН России) кафедра математики и естественнонаучных дисциплин.
тел. (8473) 2606-820
E-mail: bsvlabs@mail.ru
профессор С.В. Скрыль
(Воронеж, ВИ ФСИН России) кафедра технических комплексов охраны и связи.
тел. (8473) 2606-818
E-mail: skril@mail.ru

Professor N.S. Rodionova
(Voronezh state university of engineering technology) faculty of economics and management.
phone (473) 255-38-82
E-mail: rodionovast@mail.ru
head of department S.V. Belokurov
(Voronezh, VI FPS) Department of mathematics and natural sciences. phone (8473) 2606-820
E-mail: bsvlabs@mail.ru
professor S.V. Skryl'
(Voronezh, VI FPS) Department of technical systems of protection and communication.
phone(8473) 2606-818
E-mail: skril@mail.ru

Показатели эффективности управления информационными процессами в интегрированных системах безопасности

Efficiency indicators information management in integrated security systems

Реферат. Внедрение информационных технологий для повышения эффективности охранной деятельности приводит к необходимости учета ряда негативных факторов, связанных с последствиями использования этих технологий, как ключевого элемента современных систем охраны. Одним из наиболее ощутимых факторов является подверженность информационных процессов в системах охраны угрозам безопасности. Это в значительной степени относится к интегрированным системам безопасности (ИСБ), являющимся системами охраны с наиболее высоким уровнем информатизации охранных функций. Значительный ущерб охраняемым объектам, которые они потенциально могут понести вследствие нарушения работоспособности ИСБ, ставит весьма актуальную проблему оценки факторов, снижающих эффективность функционирования ИСБ с целью обоснования путей и методов ее повышения. Исходя из специфики угроз искажения и блокирования информации в ИСБ, интерес представляют: объем неискаженной рабочей среды ИСБ, как характеристика целостности информации; время доступа к информации как характеристика ее доступности. Это в свою очередь приводит к необходимости использования этих параметров в качестве характеристик эффективности информационных процессов в ИСБ – полноты и своевременности обработки информации. В статье предлагаются показатели эффективности информационных процессов в интегрированных системах безопасности в условиях оптимального управления процедурами защиты информации от несанкционированного доступа. Набор рассмотренных показателей позволяет провести комплексный анализ защищенности интегрированных системах безопасности, а также выработать рекомендации по совершенствованию управления процедурами защиты информации в них.

Summary. Introduction of information technology to improve the efficiency of security activity leads to the need to consider a number of negative factors associated with in consequence of the use of these technologies as a key element of modern security systems. One of the most notable factor is the exposure to information processes in protection systems security threats. This largely relates to integrated security systems (ISS) is the system of protection with the highest level of informatization security functions. Significant damage to protected objects that they could potentially incur as a result of abnormal operation ISS, puts a very actual problem of assessing factors that reduce the efficiency of the ISS to justify the ways and methods to improve it. Because of the nature of threats and blocking distortion of information in the ISS of interest are: the volume undistorted ISF working environment, as a characteristic of data integrity; time access to information as a feature of its availability. This in turn leads to the need to use these parameters as the performance characteristics of information processes in the ISS - the completeness and timeliness of information processing. The article proposes performance indicators of information processes in integrated security systems in terms of optimal control procedures to protect information from unauthorized access. Set the considered parameters allows to conduct comprehensive security analysis of integrated security systems, and to provide recommendations to improve the management of information security procedures in them.

Ключевые слова: защита информации, управление, интегрированные системы безопасности.

Keywords: information security, management, integrated security systems.

Широкое внедрение информационных технологий для повышения эффективности охранной деятельности приводит к необходимости учета ряда негативных факторов, связанных с последствиями использования этих технологий, как ключевого элемента современных систем охраны [1]. Одним из наиболее ощутимых факторов является подверженность информационных процессов в системах охраны угрозам безопасности. Это в значительной степени относится к интегрированным системам безопасности (ИСБ), являющимся системами охраны с наиболее высоким уровнем информатизации охранных функций [2, 3].

Значительный ущерб охраняемым объектам, которые они потенциально могут понести вследствие нарушения работоспособности ИСБ, ставит весьма актуальную проблему оценки факторов, снижающих эффективность функционирования ИСБ с целью обоснования путей и методов ее повышения. Одними из наиболее значимых факторов являются угрозы безопасности информационным процессам в ИСБ. Исходя из специфики угроз искажения и блокирования информации в ИСБ, интерес представляют: объем неискаженной рабочей среды ИСБ [2], как характеристика целостности информации; время доступа к информации как характеристика ее доступности [2].

Это в свою очередь приводит к необходимости использования этих параметров в качестве характеристик эффективности информационных процессов в ИСБ – полноты и своевременности обработки информации.

Характеризуя полноту обработки информации в ИСБ, будем оперировать ее информационным объемом $V_{(o)}$ [3]. Информация в ИСБ считается обработанной в полном объеме, если величина $V_{(o)}$ будет превышать или быть равной некоторой величине $V_{(но)}$:

$$V_{(o)} \geq V_{(но)}. \qquad (1)$$

Величина $V_{(но)}$ является характеристикой того минимального объема обрабатываемой информации, при котором ИСБ еще выполняет свои функции, как система, функционирующая по своему целевому назначению, обеспечивается ее работоспособное состояние.

Входящая в неравенство (1) величина $V_{(o)}$ является случайной, что приводит к необходимости рассматривать его выполнение как случайное событие, которое, в соответствии с представленным в [2, 3] форматом, характеризуется вероятностью выполнения условий соответствия двух случайных величин.

Как правило, величина $V_{(но)}$ соответствует нормативно определенным требованиям и является детерминированной величиной.

Исходя из этого, можно сделать вывод о том, что вероятность выполнения (1) достаточно полно характеризует полноту обработки информации в ИСБ, что позволяет использовать данную вероятность в качестве соответствующего показателя:

$$C = P(V_{(o)} \geq V_{(но)}) = 1 - P(V_{(o)} < V_{(но)}). \qquad (2)$$

Аналогия представления (2) и функции распределения вероятностей из классической теории вероятностей [1] позволяет применить аппарат данной теории для формирования вероятностных математических моделей полноты обработки информации в ИСБ.

Для физической характеристики информационного объема $V_{(ои)}$ воспользуемся программной метрикой Холстеда [1]:

$$V_{(o)} = R \cdot \log_2 r + D \cdot \log_2 d,$$

где r и d – число операторов и операндов в программах обработки информации в ИСБ соответственно; R и D – число неповторяющихся операторов и операндов в программах обработки информации в ИСБ соответственно (словари операторов и операндов).

Характеризуя своевременность информации в ИСБ, будем оперировать временем $\tau_{(o)}$ [1] обработки информации в этих системах. Информация в ИСБ считается обработанной своевременно, если величина $\tau_{(o)}$ не будет превышать некоторой величины $\tau_{(но)}$:

$$\tau_{(o)} \leq \tau_{(но)}. \qquad (3)$$

Величина $\tau_{(но)}$ является характеристикой того максимального времени обработки информации в ИСБ, при котором ИСБ еще выполняет свои функции как система, функционирующая по своему целевому назначению, обеспечивается ее работоспособное состояние.

Входящая в неравенство (3) величина $\tau_{(o)}$ является случайной, что приводит к необходимости рассматривать его выполнение как случайное событие, которое аналогично (1) характеризуется вероятностью выполнения условий соответствия двух случайных величин. Как правило, величина $\tau_{(но)}$ соответствует нормативно определенным требованиям и является детерминированной величиной. Исходя из этого, можно сделать вывод о том, что вероятность выполнения (3) достаточно полно характеризует своевременность обработки информации в ИСБ, что позволяет использовать данную вероятность в качестве соответствующего показателя:

$$T = P(\tau_{(o)} \leq \tau_{(но)}) = 1 - P(\tau_{(но)} < \tau_{(o)}). \qquad (4)$$

Как и в случае (2) аналогия представления (4) и функции распределения вероятностей из классической теории вероятностей [1] позволяет применить аппарат данной теории для формирования вероятностных математических моделей своевременности обработки информации в ИСБ.

Характеризуя целостность информации в ИСБ, будем оперировать объемом $V_{(ни)}$ [1] неискаженной рабочей среды этих систем. Рабочая среда считается целостной, если величина $V_{(ни)}$ будет превышать или быть равной некоторой величине $V_{(мн)}$:

$$V_{(ни)} \geq V_{(мн)}. \quad (5)$$

Величина $V_{(мн)}$ является характеристикой того минимального объема неискаженной рабочей среды, при котором программы и данные, размещенные в ней, еще обеспечивают работоспособное состояние ИСБ.

В общем случае обе входящие в неравенство (5) величины являются случайными, что приводит к необходимости рассматривать его выполнение как случайное событие, которое аналогично (1) и (3) характеризуется вероятностью выполнения условий соответствия двух случайных величин.

Исходя из этого, можно сделать вывод о том, что вероятность выполнения (5) достаточно полно характеризует целостность информации в ИСБ, что позволяет использовать данную вероятность в качестве соответствующего показателя:

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

Аналогия представления (6) и функции распределения вероятностей из классической теории вероятностей [1] позволяет применить аппарат данной теории для формирования вероятностных математических моделей обеспечения целостности информации в ИСБ.

Для формализации физической характеристики объема $V_{(ни)}$ неискаженной рабочей среды определим величину ее адресного пространства:

$$V_{(рс)} = 2^n,$$

где: n – размерность условного адресного регистра, обеспечивающего адресацию рабочей среды ИСБ.

Тогда объем $V_{(ни)}$ неискаженной рабочей среды определим как:

$$V_{(ни)} = 2^n - V_{(и)},$$

где: $V_{(и)}$ – объем искаженной рабочей среды ИСБ.

Используя вероятностное представление $V_{(и)}$ как функции угроз искажения информации, представим выражение для его определения в виде:

$$V_{(и)} = 2^n \cdot P_{(и)},$$

где: $P_{(и)}$ – вероятность искажения информации в ИСБ (вероятность наступления последствий от воздействия угрозы искажения информации).

Откуда: $P_{(и)} = V_{(и)}/2^n$.

Тогда:

$$V_{(ни)} = 2^n (1 - P_{(и)}). \quad (7)$$

В этом случае показатель (6) целостности информации в ИСБ представим в виде:

$$I = P(2^n (1 - P_{(и)}) \geq V_{(мн)}) = 1 - P(2^n (1 - P_{(и)}) < V_{(мн)}). \quad (8)$$

Характеризуя доступность информации в ИСБ, будем оперировать временем $\tau_{(д)}$ [3] доступа к информации в этих системах. Информация в ИСБ считается доступной, если величина $\tau_{(д)}$ не будет превышать некоторой величины $\tau_{(дн)}$:

$$\tau_{(д)} \leq \tau_{(дн)}. \quad (9)$$

Величина $\tau_{(дн)}$ является характеристикой того максимального времени доступа к информации ИСБ, при котором еще обеспечивается работоспособное состояние ИСБ.

В общем случае обе входящие в неравенство (9) величины являются случайными, что приводит к необходимости рассматривать его выполнение как случайное событие, которое аналогично (1), (3) и (5) характеризуется вероятностью выполнения условий соответствия двух случайных величин.

Исходя из этого, можно сделать вывод о том, что вероятность выполнения (9) достаточно полно характеризует доступность информации в ИСБ, что позволяет использовать данную вероятность в качестве соответствующего показателя:

$$A = P(\tau_{(д)} \leq \tau_{(дн)}) = 1 - P(\tau_{(дн)} < \tau_{(д)}). \quad (10)$$

Как и в случае (4) аналогия представления (10) и функции распределения вероятностей из классической теории вероятностей [1] позволяет применить аппарат данной теории для формирования вероятностных математических моделей доступности информации в ИСБ. При обосновании показателя уровня угрозы нарушения целостности и доступности информации в ИСБ воспользуемся надежностной интерпретацией такого рода угроз как угроз нарушения работоспособности ИСБ.

Это позволяет ввести следующие предположения о характере потока угроз:

- стационарность потока;
- его ординарность;
- отсутствие последействия в событиях, инициируемых этим потоком.

Обоснуем эти предположения. С целью

проверки предположения о стационарности потока воздействия угроз искажения информации и ее блокирования в ИСБ по аналогии с [1] предположим, что временной интервал $[t_{(н)}, t_{(о)}]$ от момента $t_{(н)}$ начала до момента $t_{(о)}$ окончания исследования процесса функционирования ИСБ значительно превосходит время $\tau_{(у)}$ существования угрозы, т.е. имеет место неравенство:

$$t_{(о)} - t_{(н)} >> \tau_{(у)}. \qquad (11)$$

С учетом этого, а также того, что период $T_{(у)}$ воздействия угроз искажения информации и ее блокирования в ИСБ как временной интервал между двумя последовательными воздействиями и требуемый период $T_{(т)}$ реакции на подобные воздействия соизмеримы с длиной $\Delta\tau = t_{(о)} - t_{(н)}$ временного интервала $[t_{(н)}, t_{(о)}]$, можно утверждать о стационарности процесса воздействия угроз рассматриваемого типа.

При обосновании предположения об ординарности потока воздействия угроз искажения информации и ее блокирования в ИСБ воспользуемся практикой расследования противоправных действий в информационной сфере. Результаты показывают, что комплексное применение таких разнородных по способу реализации атак, как "ложный объект РВС" и "отказ в обслуживании" [2] при реализации злоумышленниками своих противоправных действий - явление крайне редкое [3]. Это подтверждает представление возможности представления процессов воздействия угроз искажения информации и ее блокирования в ИСБ как ординарных процессов.

Для предположения об отсутствии последействия в событиях, инициируемых потоком воздействия угроз искажения информации и ее блокирования в ИСБ воспользуемся тем обстоятельством, что при реализации такого рода угроз злоумышленник может реализовать такие сложные по способу реализации атаки, как "ложный объект вычислительной сети" и "отказ в обслуживании" лишь однократно, так как повторить подобного рода действия в условиях ИСБ маловероятно.

Это позволяет вероятность воздействия угроз искажения информации в ИСБ представить в виде:

$$P_{(и)} = 1 - e^{-\frac{k_{(ло)}}{\Delta\tau}\cdot\left(t_{(о)} - t_{(н)}\right)}, \qquad (12)$$

где $k_{(ло)}$ – среднее число атак типа "ложный объект вычислительной сети" на временном интервале $[t_{(н)}, t_{(о)}]$ функционирования ИСБ.

Аналогичным образом вероятность воздействия угроз блокирования информации в ИСБ представляется в виде:

$$P_{(б)} = 1 - e^{-\frac{k_{(оо)}}{\Delta\tau}\cdot\left(t_{(о)} - t_{(н)}\right)}, \qquad (13)$$

где k – среднее число атак типа "отказ в обслуживании" на временном интервале $[t_{(н)}, t_{(о)}]$ функционирования ИСБ.

С целью аналитического представления показателя эффективности информационных процессов в ИСБ в условиях реализации механизмов защиты информации от несанкционированного доступа (НСД) рассмотрим вероятностную интерпретацию группы событий [3], связанных с реализацией информационных процессов в ИСБ, реализацией угроз искажения информации и ее блокирования в этих системах и мер обеспечения защиты от НСД.

Для этого определим следующие события: событие 1 – «Информационный процесс в ИСБ в условиях отсутствия угроз искажения информации и ее блокирования» и событие 2 – «Информационный процесс в ИСБ в условиях воздействия угроз искажения информации и ее блокирования». В свою очередь событие 2 составляют два события: событие 21 – «Меры защиты информации от НСД обеспечивают целостность и доступность информации» и событие 22 – «Меры защиты информации от НСД не обеспечивают целостность и доступность информации».

С учетом рассмотренных событий представим рассмотренные выше характеристики информационных процессов в ИСБ в условиях реализации механизмов защиты информации от НСД информационным объемом $V_{(о)}$ обрабатываемой информации в ИСБ и временем $\tau_{(о)}$ ее обработки информации в этих системах. На основе этих событий запишем выражения для характеристик информационных процессов в ИСБ. Выражение для среднего значения объема обрабатываемой информации в ИСБ в этих условиях имеет вид:

$$\overline{V}_{(о)} = \overline{V}_{(оп)} + P_{(и)}\cdot\left(1 - I\right)\cdot\overline{V}_{(и)}, \qquad (14)$$

где $\overline{V}_{(оп)}$ – среднее значение потенциального объема обрабатываемой в ИСБ информации (в отсутствии угроз ее искажения и мер защиты от НСД); $\overline{V}_{(и)}$ – среднее значение случайной величины $V_{(и)}$ объема искажаемой в ИСБ информации (интерпретируется как мера ущерба

информационному процессу в ИСБ в единицах объема информации).

Выражение для среднего значения времени Δt реализации информационного процесса имеет вид:

$$\Delta\bar{t} = \Delta\bar{t}_{(оп)} + P_{(б)} \cdot (1 - A) \cdot \overline{\Delta}\,\tau_{(б)}, \quad (15)$$

где $\Delta\bar{t}_{(оп)}$ – среднее значение потенциального времени реализации информационного процесса в ИСБ (в отсутствии угроз ее блокирования и мер защиты от НСД); $\overline{\Delta}\,\tau_{(б)}$ – среднее значение случайной величины времени нахождения ИСБ в состоянии блокирования информации (интерпретируется как мера ущерба информационному процессу в ИСБ в единицах времени обработки информации).

С учетом специфики обеспечения защиты информации от НСД в ИСБ представим формально процесс защиты последовательностью процедур:

- закрытие от загрузки ОС через внешний накопитель (процедура 1);
- обеспечение санкционированного доступа (процедура 2);
- контрольная аутентификация пользователей, допущенных к информации ИСБ (процедура 3);
- разграничение доступа (процедура 4);
- поддержание целостности рабочей среды (процедура 5);
- администрирование работы механизмов защиты информации от НСД (МЗИ НСД) (процедура 6);
- управление контролем доступа пользователей к информации в ИСБ (процедура 7).

С учетом этого обстоятельства показатель (8) целостности информации в ИСБ представим в виде:

$$I = P(2^n (1 - P_{(и)}) \geq V_{(мн)}) =$$
$$= 1 - P(2^n (1 - P_{(и)}) < V_{(мн)}) =$$
$$= 1 - P((2^{n1} \circ 2^{n2} \circ 2^{n3} \circ 2^{n4} \circ 2^{n5} \circ 2^{n6} \circ 2^{n7}) \circ$$
$$\circ (1 - P_{(и)}) < V_{(мн)}), \quad (16)$$

где 2^{n1}, 2^{n2}, 2^{n3}, 2^{n4}, 2^{n5}, 2^{n6} и 2^{n7} – случайные величины адресных пространств, целостность которых обеспечивается реализацией процедур 1-7 защиты информации от НСД в ИСБ, соответственно; $\circ$ – знак композиции случайных величин

Вероятность (16) является наиболее полной характеристикой функциональных возможностей по защите целостности информации в ИСБ.

Аналогичным образом показатель (10) доступности информации в ИСБ запишем в виде:

$$A = P(\tau_{(д)} \leq \tau_{(дн)}) = 1 - P(\tau_{(дн)} < \tau_{(д)}) =$$
$$= 1 - P(\tau_{(дн)} < \tau_{(д1)} \circ \tau_{(д2)} \circ \tau_{(д3)} \circ \tau_{(д4)} \circ$$
$$\circ \tau_{(д5)} \circ \tau_{(д6)} \circ \tau_{(д7)}), \quad (17)$$

где $\tau_{(д1)}$, $\tau_{(д2)}$, $\tau_{(д3)}$, $\tau_{(д4)}$, $\tau_{(д5)}$, $\tau_{(д6)}$ и $\tau_{(д7)}$ – случайные величины времен доступа к информации в ИСБ, обеспечиваемых реализацией процедур 1-7 защиты информации от НСД в ИСБ, соответственно.

При дифференциации процесса защиты информации от НСД в ИСБ можно выделить два частных процесса:

1) процесс автоматизированного контроля доступа пользователей к информации в ИСБ, включающий процедуры:

- обеспечения санкционированного доступа (процедура 2);
- контрольной аутентификации пользователей, допущенных к информации ИСБ (процедура 3);
- разграничения доступа (процедура 4);
- управления контролем доступа пользователей к информации в ИСБ (процедура 7).

2) процесс контроля основных МЗИ, включающий процедуры:

- закрытие от загрузки ОС через внешний накопитель (процедура 1);
- поддержание целостности рабочей среды (процедура 5);
- администрирование работы МЗИ НСД (процедура 6).

Это, в свою очередь, позволяет показатель (16) целостности информации в ИСБ представить в виде:

$$I = P(2^n (1 - P_{(и)}) \geq V_{(мн)}) =$$
$$= 1 - P(2^n (1 - P_{(и)}) < V_{(мн)}) =$$
$$= 1 - P((2^{n(кд)} \circ 2^{n(км)}) \cdot (1 - P_{(и)}) < V_{(мн)}), \quad (18)$$

где $2^{n(кд)}$ – случайная величина адресного пространства, целостность которого обеспечивается реализацией процесса автоматизированного контроля доступа пользователей к информации в ИСБ; $2^{n(км)}$ – случайная величина адресного пространства, целостность которого обеспечивается реализацией процесса основных МЗИ в ИСБ.

Аналогичным образом показатель (17) доступности информации в ИСБ представляется в виде:

$$A = P(\tau_{(д)} \leq \tau_{(дн)}) = 1 - P(\tau_{(дн)} < \tau_{(д)}) =$$
$$= 1 - P(\tau_{(дн)} < \tau_{(д(кд))} \circ \tau_{(д(кн))}), \quad (17)$$

где $\tau_{(д(кд))}$ – случайная величина времени доступа к информации в ИСБ, обеспечиваемая реализацией процесса автоматизированного контроля доступа пользователей к информации в ИСБ;

$\tau_{(д(кд))}$ – случайная величина времени доступа к информации в ИСБ, обеспечиваемая реализацией процесса контроля основных МЗИ в ИСБ.

Таким образом, в статье предлагаются показатели эффективности информационных процессов в интегрированных системах безопасности в условиях оптимального управления процедурами защиты информации от несанкционированного доступа. Набор рассмотренных показателей позволяет провести комплексный анализ защищенности интегрированных системах безопасности, а также выработать рекомендации по совершенствованию управления процедурами защиты информации в них.

ЛИТЕРАТУРА

1 Минаев В.А., Скрыль С.В. Основы информационной безопасности: учебник для высших учебных заведений МВД России. Воронеж: Воронежский институт МВД России, 2001. 464 с.

2 Белокров С.В., Скрыль С.В., Джоган В.К. и др. Методы и средства анализа эффективности систем информационной безопасности при их разработке: монографии. Воронеж: Воронежский институт МВД России, 2012. 83 с.

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

REFERENCES

1 Minaev V.A., Skryl’ S.V. Osnovy informatsionnoi bezopasnosti [Basics of information security]. Voronezh, Voronezhskii institute MVD, 2001. 464 p.

2 Belokurov S.V., Skryl’ S.V., Dzhogan V.K. et al. Metody i sredstva analiza effektivnosti system informatsionnoi bezopasnosti pri ikh razrabotke [Methods and tools for the analysis of the effectiveness of information security in their development]. Voronezh, Voronezhskii institute MVD, 2012. 83 p.

3 Belokurov S.V., Skryl’ S.V., Dzhogan V.K. et al. Model ii algorimy avtomatizirovannogo kontroliaeffektivnosti system zashchity informatsii v avtomatizirovannykh sistemakh [Models and algorithms for the automated control of the effectiveness of information security systems in automated systems : monograph]. Voronezh, Voronezhskii institute MVD, 2012. 116 p.