Информатика и вычислительная техника
Informatics and computer engineering

Научная статья
УДК 004.056
DOI: 10.14529/ctcr220401

МОДЕЛИ ДОСТОВЕРНОСТИ КОМПЛЕКСНОГО КОНТРОЛЯ СОСТОЯНИЙ В ПРОСТРАНСТВЕННО-РАСПРЕДЕЛЕННЫХ СИСТЕМАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.В. Ананьев[1], *sasha303_75@mail.ru*
С.А. Баркалов[2], *barkalov@vgasu.vrn.ru*
К.С. Иванников[3], *ivannikov_ks@radar-mms.com*
С.И. Моисеев[2], *mail@moiseevs.ru, https://orcid.org/0000-0002-6136-9763*
[1] *АО «Научно-производственное предприятие «Полет», Нижний Новгород, Россия*
[2] *Воронежский государственный технический университет, Воронеж, Россия*
[3] *АО «Научно-производственное предприятие «Радар ммс», Санкт-Петербург, Россия*

Аннотация. В работе рассматриваются широко применяемые на практике распределенные системы, предполагающие хранение, обработку критически важной для предприятий и учреждений информации на периферии, анализируется спектр уязвимостей по отношению к информационной безопасности (ИБ) предприятий, организаций, учебных заведений и т. д. В статье проведен подробный анализ применения математического аппарата теории массового обслуживания, используемого для исследований информационной безопасности распределенных систем. **Цели и задачи** поставлены по результатам проведенного анализа, который показал, что существующее соотношение «распределенная инфокоммуникационная система – угрозы ИБ» не в полной мере отражает свойство достоверности данных о состоянии ИБ для количества элементов (датчиков), участвующих в обеспечении ИБ для данной информационной системы, и количества каналов, по которым могут приходить угрозы для данной информационной системы. Таким образом, целью данной работы является разработка математической модели, основанной на марковских случайных процессах и теории массового обслуживания, которая позволяет в динамике вероятностными методами оценить актуальность информации о возможных угрозах в области информационной безопасности и принять упреждающие меры по их ликвидации. **Материалы и методы.** В основе исследований лежит идея, заключающаяся в том, что имеется некоторая информационная система, которая может подвергаться угрозам в области информационной безопасности, угрозы могут поступать по некоторым каналам. Для математического моделирования описанной ситуации введен ряд ограничений, с учетом которых показано, что достоверность данных об информационных угрозах может быть исследована на основе марковских случайных процессов. **Результаты.** С использованием модели достоверности комплексного контроля состояний в пространственно-распределенных системах ИБ получены: зависимости вероятности достоверности информации об угрозах от интенсивности их поступления при разном количестве источников угроз; зависимости вероятности достоверности информации от времени получения и обработки информации при разном количестве источников угроз; минимальные значения элементов, которые необходимы для обеспечения с вероятностью не менее заданной, достоверности информации при известном количестве источников угроз для разных значений интенсивности их поступления и другие. **Заключение.** Полученные зависимости имеют квазиленейный характер, что позволяет проводить приближенные, но достаточно точные расчеты при оценке указанных параметров, что позволит эффективно организовывать мероприятия по ИБ. Разработанная модель позволит проводить оперативное планирование стратегии защиты информационной системы от возможных угроз, а также осуществлять поддержку принятия решений по количеству элементов ИБ в меняющихся условиях противостояния внешним информационным воздействиям.

Ключевые слова: распределенная система, информационная безопасность, теория массового обслуживания, достоверность информации

Для цитирования: Модели достоверности комплексного контроля состояний в пространственно-распределенных системах информационной безопасности / А.В. Ананьев, С.А. Баркалов, К.С. Иванников, С.И. Моисеев // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». 2022. Т. 22, № 4. С. 5–15. DOI: 10.14529/ctcr220401

Original article
DOI: 10.14529/ctcr220401

RELIABILITY MODELS OF COMPLEX STATE CONTROL IN SPATIALLY DISTRIBUTED INFORMATION SECURITY SYSTEMS

A.V. Ananiev[1], *sasha303_75@mail.ru*
S.A. Barkalov[2], *barkalov@vgasu.vrn.ru*
K.S. Ivannikov[3], *ivannikov_ks@radar-mms.com*
S.I. Moiseev[2], *mail@moiseevs.ru, https://orcid.org/0000-0002-6136-9763*
[1] *JSC Research and Production Enterprise "Polet", Nizhny Novgorod, Russia*
[2] *Voronezh State Technical University, Voronezh, Russia*
[3] *JSC Research and Production Enterprise "Radar mms", St. Petersburg, Russia*

Abstract. The paper considers distributed systems widely used in practice, which involve the storage and processing of information critical for enterprises and institutions on the periphery, analyzes the range of vulnerabilities in relation to information security (IS) of enterprises, organizations, educational institutions, etc. The article provides a detailed analysis of the application of the mathematical apparatus of the theory of queuing used to study the information security of distributed systems. **The goals and objectives** were set based on the results of the analysis, which showed that the existing ratio "distributed infocommunication system – IS threats" does not fully reflect the property of reliability of data on the state of IS for the number of elements (sensors) involved in providing IS for this information system and the number of channels through which threats to this information system can come. Thus, the purpose of this work is to develop a mathematical model based on Markov random processes and queuing theory, which allows using probabilistic methods to evaluate the relevance of information about possible threats in the field of information security in dynamics and take preventive measures to eliminate them. **Materials and methods.** The research is based on the idea that there is some information system that can be exposed to threats in the field of information security, threats can come through some channels. For mathematical modeling of the described situation, a number of restrictions are introduced, taking into account which it is shown that the reliability of data on information threats can be investigated on the basis of Markov random processes. **Results.** Using the model of reliability of complex monitoring of states in spatially distributed IS systems, the following were obtained: dependences of the probability of reliability of information about threats on the intensity of their arrival with a different number of threat sources; dependence of the probability of reliability of information on the time of receipt and processing of information with a different number of sources of threats; the minimum values of the elements, which are necessary to ensure the reliability of information with a probability not less than a given one, with a known number of threat sources for different values of the intensity of their arrival, and others. **Conclusion.** The dependences obtained are quasi-linear in nature, which makes it possible to carry out approximate, but sufficiently accurate calculations when evaluating these parameters, which will make it possible to effectively organize information security measures. The developed model will allow for operational planning of an information system protection strategy against possible threats, as well as support for decision-making on the number of information security elements in changing conditions of confronting external information influences.

Keywords: distributed system, Information Security, queuing theory, reliability of information

For citation: Ananiev A.V., Barkalov S.A., Ivannikov K.S., Moiseev S.I. Reliability models of complex state control in spatially distributed information security systems. *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics*. 2022;22(4):5–15. (In Russ.) DOI: 10.14529/ctcr220401

Введение

Современный уровень инфокоммуникационных технологий, обеспечивающих высокоскоростную передачу по линиям связи при возможности доступа к системе через вычислительные системы, в том числе персональные, позволяет воплощать в реальность высокоэффективные распределенные системы. Основным признаком распределенных систем является отсутствие локального сосредоточения компонентов в одном физическом местоположении. Дополнительным стимулом к развитию таких распределенных систем служат эпидемиологическая обстановка, привя-

занность узких специалистов к местам постоянного проживания, локализация производственной базы, использование облачных сервисов и т. д.

В то же время на практике распределенные системы, предполагающие хранение, обработку критически важной для предприятий и учреждений информации на периферии, открывают целый спектр уязвимостей по отношению к информационной безопасности (ИБ) предприятий, организаций, учебных заведений и т. д. [1]. В связи с этим одновременно со стремительной информатизацией общества, промышленности и экономики на первое место выходят проблемы информационной безопасности в распределенных системах самого различного назначения [2–4], которые могут свести «на нет» любые перспективные проекты и функционирующие системы практически в любой отрасли народного хозяйства.

В интересах получения качественных, научно обоснованных, а самое главное, ***своевременных*** организационных и технических решений по обеспечению безопасности информации в распределенных системах широкое применение находит математический аппарат теории массового обслуживания (ТМО), обзор которых проведен далее по тексту. В работах [5, 6] с использованием ТМО решаются задачи построения моделей мониторинга систем обработки данных по показателям информационной безопасности. Получены соотношения для наиболее важных характеристик указанных систем, в частности, вероятности числа не выявленных вызовов в моменты окончания обслуживания. В работе [7] исследуется технология «Умный дом», а именно проводится сравнение обработчиков данных по показателю среднего времени обработки запросов в зависимости от объема базы знаний экспертной системы. По результатам исследований получены функциональные зависимости количества запросов в очереди и времени ожидания очереди от общего количества запросов за некоторый интервал времени. В работе [8] исследуются вопросы временных затрат на время подготовки системы информационной безопасности к функционированию, включающему аутентификацию пользователя, установление соединения с базой данных, дешифрование данных, кэширование при запросах к базе данных, загрузку виртуальных машин и т. д.

Наиболее близкими по смыслу и содержанию к исследованию авторов являются работы, в которых при анализе угроз с использованием СМО определяется их актуальность, в том числе учитываются разнородные угрозы [9, 10]. В некоторых работах осуществлена привязка к реальным протоколам, например, протоколу установления сессий (Session Initiation Protocol, SIP) между двумя пользователями с одним межсетевым экраном по пути следования сигнальных сообщений [11]. В ряде исследований эффект от действий злоумышленника представлен в виде снижения интенсивности обработки заявок пользователей и повышения интенсивности обработки заявок на нарушение доступа [8, 12].

Цели и задачи

Одновременно анализируя использование теории СМО в сфере ИБ и существующее соотношение «распределенная инфокоммуникационная система – угрозы ИБ», можно сделать вывод о том, что остается не в полной мере исследованным свойство достоверности данных о состоянии ИБ для определенного количества элементов (датчиков) N, участвующих в обеспечении ИБ для данной информационной системы, а также для количества каналов M, по которым могут приходить угрозы для данной информационной системы. В свою очередь ***достоверность*** данных о ИБ инфокоммуникационной системы в первую очередь определяется устареванием информации о типах, видах и направлениях существующих информационных угроз.

Ввиду вышесказанного в данной работе предлагается математическая модель оценки эффективности проведения мероприятий по ликвидации информационных угроз для некоторой организации. В основе модели ставится цель в получении и передаче информации о возможных информационных угрозах на самых различных уровнях в условиях длительного времени. Под информационными угрозами следует понимать как отдельные частные кибератаки, приходящие от отдельных источников, так и любые долгосрочные проекты, связанные с уменьшением информационной безопасности.

Таким образом, целью данной работы является разработка математической модели, основанной на марковских случайных процессах и теории массового обслуживания, которая позволяет в динамике вероятностными методами оценить актуальность информации о возмож-

ных угрозах в области информационной безопасности и принять упреждающие меры по их ликвидации.

Для достижения цели необходимо решить следующие задачи:

1) разработать математическую модель, позволяющую оценить вероятность того, что информация о возможных информационных угрозах актуальна, или провести оценку доли актуальной информации о возможных информационных угрозах;

2) получить численное решение для основных параметров, характеризующих степень актуальности информации об информационных угрозах;

3) проанализировать полученные решения, дать рекомендации по эффективной организации мероприятий, связанной с ликвидацией угроз в области информационной безопасности.

Математическая постановка задачи

В ее основе будет лежать идея, заключающаяся в том, что имеется некоторая информационная система, которая может подвергаться угрозам в области информационной безопасности, угрозы могут поступать по M каналам. Данная система имеет защиту от возможных угроз, которая содержит N элементов. При обнаружении угрозы по какому-либо каналу каждый элемент ИБ собирает информацию об угрозе и в течении какого-то времени обрабатывает ее, вследствие чего принимается решение о ликвидации угрозы. Для математического моделирования описанной ситуации введем следующие допущения.

1. Источник информационной угрозы заранее не известен, и процесс обнаружения угрозы каналом ИБ является случайным. При этом поток событий, заключающихся в обнаружении угрозы с получением и обработкой информации о нем, рационально считать потоком Пуассона [13, 14].

2. Учитывая динамичность внешних воздействий на информационную систему, рационально предположить, что информация, полученная о каждой обнаруженной угрозе, остается актуальной лишь некоторое время, после чего она устаревает и необходимо вновь получать актуальную информацию об источнике угрозы. Учитывая пуассоновский поток обнаружения информационных угроз, можно предположить, что поток событий, заключающихся в потерях актуальности информации об угрозе, также будет являться потоком Пуассона.

3. Процесс обеспечения ИБ информационной системы длится достаточно длительное время для того, чтобы случайный процесс, его описывающий, перешел в стационарный режим.

С учетом подобных допущений можно моделировать достоверность данных об информационных угрозах на основе марковских случайных процессов [13, 15].

Введем следующие обозначения:

N – количество элементов (датчиков), участвующих в обеспечении ИБ для данной информационной системы;

M – количество каналов, по которым могут приходить угрозы для данной информационной системы;

λ – интенсивность обнаружения, получения и успешной обработки информации об одной угрозе, интенсивность получения информации об угрозах для информационной системы согласно теореме о сложении потоков событий [15] будет равна $N\lambda$;

$T_{\text{а}}$ – среднее время сохранения актуальности информации об обнаруженной угрозе, если каналы, по которым возможно ее поступление, разные, то это средневзвешенное время, рассчитанное на основе времени актуальности информации, для каждого канала пропорционально их количеству;

$T_{\text{п}}$ – среднее время обработки информации об угрозе до момента ее ликвидации.

На основании двух последних параметров можно определить интенсивность потери актуальной информации для одного канала:

$$\mu = \frac{1}{T_{\text{а}} - T_{\text{п}}}.$$

Указанные параметры служат исходными данными для построения модели достоверности комплексного контроля состояний в пространственно-распределенных системах ИБ.

Модели достоверности комплексного контроля состояний в пространственно-распределенных системах ИБ

Перейдем к модели, основанной на случайных марковских процессах. Введем следующие состояния: S_k – состояние, когда имеется актуальная информация о k каналах, $k = 0, 1, \ldots, M$. Тогда процесс получения и устаревания информации для этих каналов можно смоделировать марковским процессом гибели и размножения [15], граф состояний которого приведен на рис. 1.

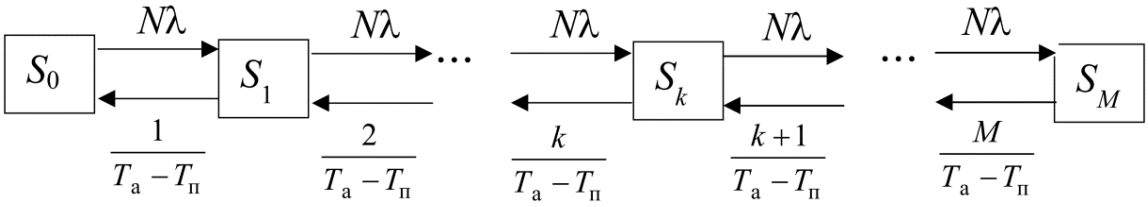

Рис. 1. Граф состояний процесса получения и устаревания информации
Fig. 1. Graph of the states of the process of obtaining and obsolescence of information

Определим вероятности состояний P_k, имеющие смысл вероятности того, что в произвольный момент времени имеется актуальная информация о k каналах, из которых возможны угрозы, $k = 0, 1, \ldots, M$. Для этого находим вероятность отсутствия информации для всех каналов:

$$P_0 = \left[\sum_{m=0}^{M} \frac{\left(N\lambda(T_а - T_п)\right)^m}{m!} \right]^{-1}, \tag{1}$$

а затем вероятности всех оставшихся состояний:

$$P_k = \frac{\left[N\lambda(T_а - T_п)\right]^k}{k!} P_0 = \frac{\left[N\lambda(T_а - T_п)\right]^k}{k! \cdot \sum_{m=0}^{M} \frac{\left(N\lambda(T_а - T_п)\right)^m}{m!}}, \; k = 0, 1, \ldots, M. \tag{2}$$

Как было сказано ранее, будем считать информацию достоверной, если информация о всех M каналах поступления угроз является актуальной. Вероятность этого равна

$$P_M = \frac{\left[N\lambda(T_a - T_n)\right]^M}{M! \cdot \sum_{m=0}^{M} \frac{\left(N\lambda(T_a - T_n)\right)^m}{m!}}. \tag{3}$$

Проанализируем полученные вероятности получения достоверной информации в зависимости от интенсивности обнаружения, получения и обработки достоверной информации об угрозах. Это связано с тем, что вероятность получения достоверной информации P_M можно интерпретировать как некоторый показатель полной информационной защищенности: чем выше вероятность обнаружения и обработки актуальной информации о всех возможных угрозах, тем выше значения критерия защищенности информационной системы. С другой стороны, интенсивность обнаружения, получения и успешной обработки информации об угрозах одним элементом ИБ λ может служить показателем своевременности получения информации об угрозах: скорость обнаружения угроз по всем возможным каналам напрямую влияет на поддержание имеющейся информации на актуальном уровне и обеспечение ИБ.

На рис. 2 представлены графики зависимости вероятности достоверности информации об угрозах P_M от интенсивности λ.

Как видим из рис. 2, достоверность информации сильно зависит от скорости (интенсивности) обнаружения информационных угроз, а также от количества необходимых для полного контроля ситуации при принятии решений числа элементов системы ИБ.

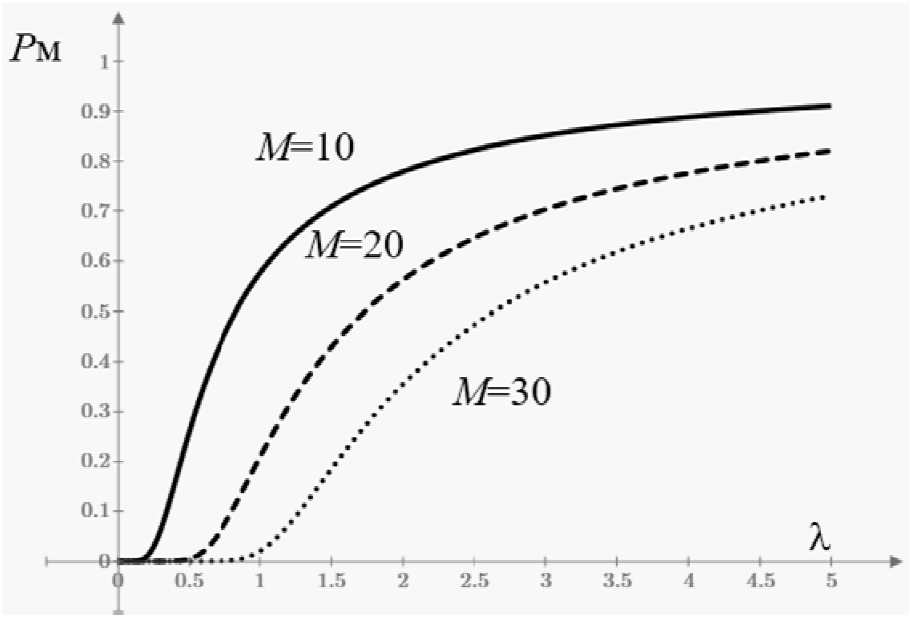

Рис. 2. Зависимость вероятности достоверности информации об угрозах от интенсивности λ при разном количестве источников угроз (N = 12, $T_а$ = 2 ч, $T_п$ = 10 мин)
Fig. 2. Dependence of the probability of reliability of information about threats on the intensity λ for a different number of sources of threats (N = 12, $T_а$ = 2 h, $T_п$ = 10 min)

Второй составляющей служит время обработки полученной информации до момента принятия решений на ликвидацию угрозы $T_п$. Не меньшую роль играет время актуальности информации $T_а$, но этот параметр является экзогенным и им управлять невозможно. Приведем зависимость вероятности достоверности информации от времени передачи информации $T_п$ и от количества источников информационных угроз, который приведен на рис. 3.

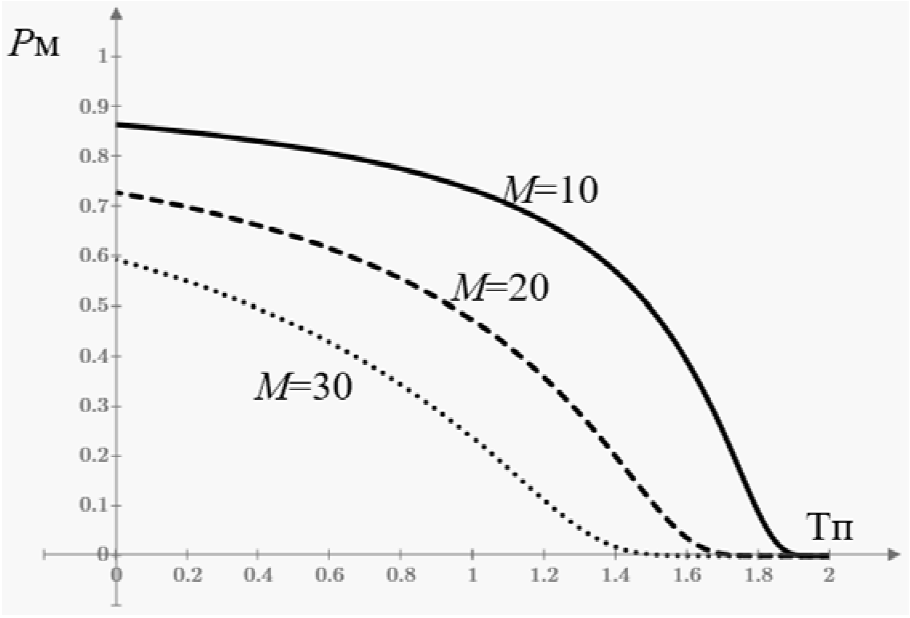

Рис. 3. Зависимость вероятности достоверности информации от времени получения и обработки информации $T_п$ (ч) при разном количестве источников угроз (λ = 3, N = 12, $T_а$ = 2 ч)
Fig. 3. Dependence of the probability of information reliability on the time of receipt and processing of information $T_п$ (h) with a different number of threat sources (λ = 3, N = 12, $T_а$ = 2 h)

Закономерно достоверность информации падает при росте времени получения и обработки информации и количества источников информационных угроз.

На основании модели (3) можно рассчитать минимальное количество элементов защиты информационной системы от возможных угроз $N_{кр}$, которое необходимо использовать для того, чтобы с вероятностью не менее $P_{кр}$ поддерживать в актуальном состоянии информацию о M источниках угроз. Для этих целей необходимо решать трансцендентное уравнение относительно параметра $N_{кр}$ вида

$$\frac{\left[\lambda(T_{а}-T_{п})\text{floor}(N_{кр})\right]^{M}}{M!\cdot\sum_{m=0}^{M}\frac{\left(\lambda(T_{а}-T_{п})\text{floor}(N_{кр})\right)^{m}}{m!}}=P_{кр}, \tag{4}$$

где функция floor(x) округляет аргумент до ближайшего меньшего целого.

Результаты решения (4) позволят планировать количество элементов системы ИБ, которое необходимо использовать для получения достоверной информации для заданного числа источников информационных угроз так, чтобы имелась актуальная информация о всех возможных угрозах с заданной вероятностью. Зависимость минимального количества элементов ИБ N, которое необходимо для обеспечения с вероятностью не менее $P_{кр} = 0{,}9$ достоверности информации при M источниках угроз при разных интенсивностях получения новой информации λ о них, представлена на рис. 4.

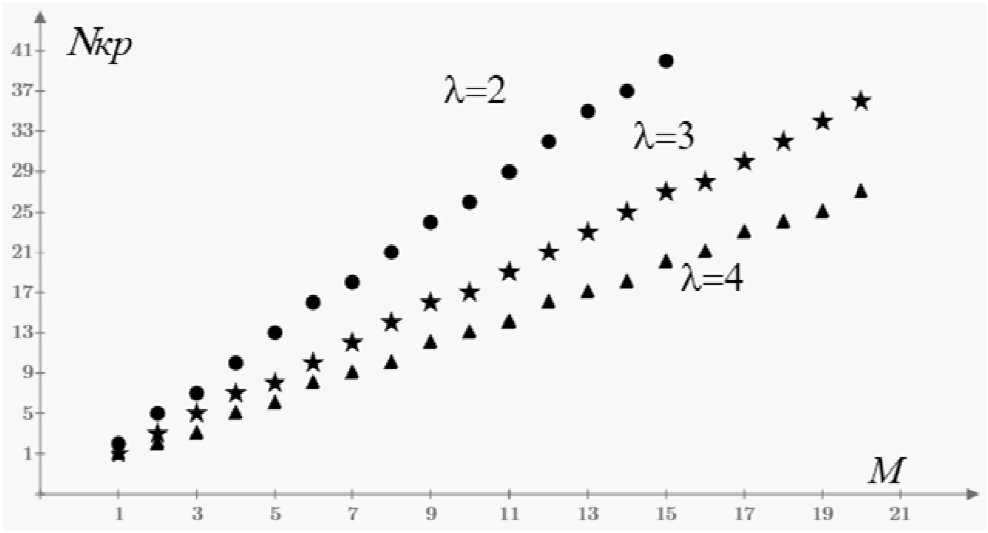

Рис. 4. Минимальное количество элементов ИБ N, которое необходимо для обеспечения с вероятностью не менее $P_{кр}$ = 0,9 достоверности информации при M источниках угроз при разных интенсивностях λ (N = 12, $T_{а}$ = 2 ч, $T_{п}$ = 10 мин)

Fig. 4. The minimum number of IS elements N, which is necessary to ensure, with a probability of at least $P_{кр}$ = 0.9, the reliability of information with M sources of threats at different intensities λ (N = 12, $T_{а}$ = 2 h, $T_{п}$ = 10 min)

Как видно из рис. 4, зависимость $N(M)$ практически линейная, что позволит получать аналитические зависимости методами регрессионного анализа.

Рассмотрим теперь обратную задачу: определим минимальную интенсивность обнаружения, получения и успешной обработки информации об одной угрозе одним элементом ИБ $\lambda_{кр}$, которые напрямую определяют своевременность мероприятий по ликвидации информационных угроз, от минимальной вероятности поддерживания актуальной информации о возможных угрозах и, как следствие, достоверности информации $P_{кр}$. Для решения этой задачи также необходимо решать уравнение относительно параметра $\lambda_{кр}$ вида

$$\frac{\left[N\lambda_{кр}(T_{а}-T_{п})\right]^{M}}{M!\cdot\sum_{m=0}^{M}\frac{\left(N\lambda_{кр}(T_{а}-T_{п})\right)^{m}}{m!}}=P_{кр}. \tag{5}$$

На рис. 5 приведены зависимости минимальной интенсивности обнаружения, получения и успешной обработки информации об угрозе одним элементом ИБ $\lambda_{кр}$, которые обеспечивают достоверность информации с вероятностью $P_{кр}$ от значения этой вероятности.

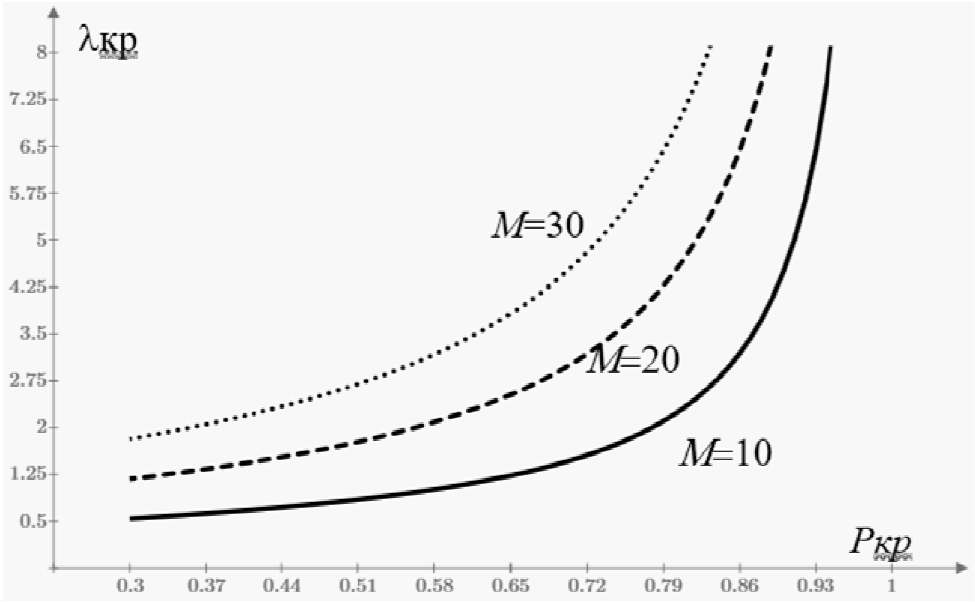

Рис. 5. Зависимости минимальной интенсивности обнаружения, получения и успешной обработки информации об угрозе одним элементом ИБ $\lambda_{кр}$ от вероятности $P_{кр}$ (N = 12, $T_а$ = 2 ч, $T_п$ = 10 мин)
Fig. 5. Dependences of the minimum intensity of detection, receipt and successful processing of information about the threat by one IS element $\lambda_{кр}$ on the probability $P_{кр}$ (N = 12, $T_а$ = 2 h, $T_п$ = 10 min)

Для полного описания картины взаимоотношений между своевременностью и достоверностью получаемой информации об угрозах приведем зависимость между своевременностью получения и обработки информации, выраженной в единицах времени, которая имеет смысл среднего времени, необходимого на получении новой информации об информационной угрозе $T_{кр}$, которая связана с интенсивностью получения этой информации формулой $T_{кр} = 1/\lambda_{кр}$, от вероятности $P_{кр}$ обеспечения необходимой достоверности. Эта зависимость приведена на рис. 6.

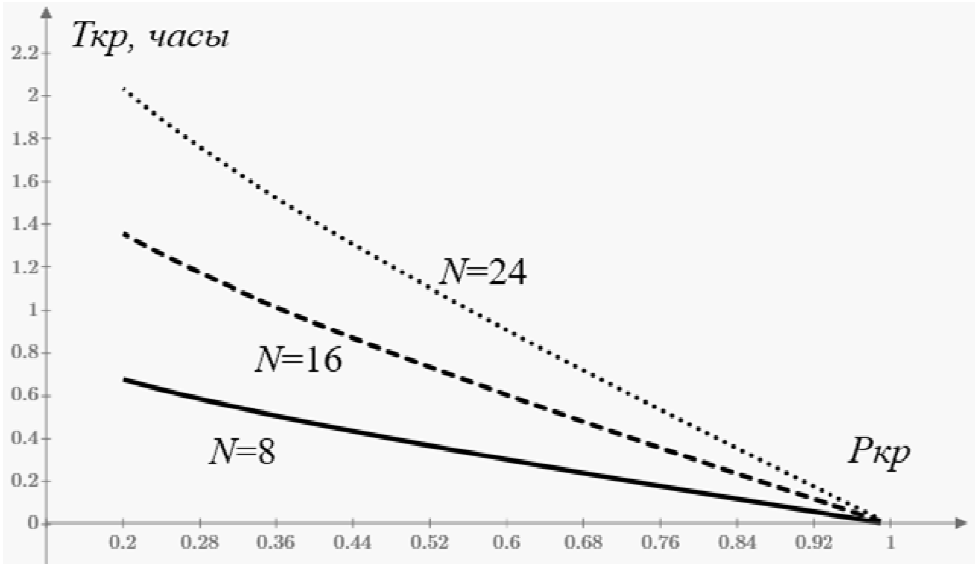

Рис. 6. Зависимости минимального времени на получение актуальной информации одним элементом ИБ $T_{кр}$ от вероятности $P_{кр}$ обеспечения необходимой достоверности (M = 20, $T_а$ = 2 ч, $T_п$ = 10 мин)
Fig. 6. Dependences of the minimum time for obtaining up-to-date information by one IS element $T_{кр}$ on the probability $P_{кр}$ of providing the necessary reliability (M = 20, $T_а$ = 2 h, $T_п$ = 10 min)

Из рис. 6 видно, что данная зависимость является близкой к линейной и на практике ее можно получать методами регрессионного анализа.

Заключение

Полученные зависимости также имеют квазилинейный характер, что позволит проводить приближенные, но достаточно точные расчеты при оценке указанных параметров.

Таким образом, представленная модель позволит проводить оперативное планирование стратегии защиты информационной системы от возможных угроз [16], а также осуществлять поддержку принятия решений по количеству элементов ИБ в меняющихся условиях противостояния внешним информационным воздействиям.

Список литературы

1. Андреев Н.О. Современные проблемы безопасности корпоративных сетей // Прикладная информатика. 2008. № 1 (13). С. 25–31.

2. Вотинов, М.В. Обеспечение систем автоматического управления современными информационными средствами удаленного доступа и мобильного контроля. Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». 2017. Т. 17, № 2. С. 141–148. DOI: 10.14529/ctcr170213

3. Сергеева Т.А., Хазимов М.В. Информационная безопасность при обмене технологической информацией для осуществления функций телеуправления в энергетике // Электроэнергетика глазами молодежи – 2017: материалы VIII Междунар. науч.-техн. конф. 2017. С. 292–295.

4. Лукашев В.М. Защита конечных ресурсов КИС с использованием интеллектуальных систем безопасности // Защита информации. Инсайд. 2006. № 2 (8). С. 27–29.

5. Моделирование процесса мониторинга систем информационной безопасности на основе систем массового обслуживания / Г.А. Попов, С.Ж. Симаворян, А.Р. Симонян, Е.И. Улитина // Информатика и ее применения. 2020. Т. 14, № 1. С. 71–79. DOI: 10.14357/19922264200110

6. Красножон Ю.Г. Математическая модель как средство оптимизации системы автоматизации процесса управления инцидентами информационной безопасности // Безопасность информационных технологий. 2018. Т. 25, № 1. С. 99–107.

7. Еременко В.Т., Лякишев А.А. Оптимизация процессов информационного обмена в системе безопасности и мониторинга АСУЗ на примере технологии «Умный дом» // Вестник БГТУ имени В. Г. Шухова. 2017. № 7. С. 146–151. DOI: 10.12737/article_5940f01a8d60b0.87715921

8. Модель оценивания оперативности облачных вычислений с учетом виртуализации и обеспечения информационной безопасности / С.Е. Ададуров, С.В. Калиниченко, В.А. Лохвицкий и др. // Известия Тульского государственного университета. Технические науки. 2017. № 9-1. С. 233–245.

9. Щеглов К.А., Щеглов А.Ю. Интерпретация и моделирование угрозы атаки на информационную систему. Часть 1. Моделирование угрозы уязвимости и интерпретация угрозы атаки // Информационные технологии. 2015. Т. 21, № 12. С. 930–940.

10. Распределенная информационно-диагностическая система управления технологическим процессом / С.А. Манцеров, К.В. Ильичев, А.М. Бремзен, В.О. Балашов // Международный студенческий научный вестник. 2017. № 6. С. 92.

11. Самуйлов К.Е., Ботвинко А.Ю., Зарипова Э.Р. Оценка времени установления сессии между пользователями при наличии межсетевого экрана // Вестник Российского университета дружбы народов. Серия: Математика, информатика, физика. 2016. № 1. С. 59–66.

12. Подход к анализу состояния информационной безопасности беспроводной сети / Н.А. Бажаев, А.Е. Давыдов, И.Е. Кривцова и др. // Прикладная информатика. 2016. Т. 11, № 6 (66). С. 121–128.

13. Алексеев О.Г., Анисимов В.Г., Анисимов Е.Г. Марковские модели боя. М.: МО СССР, 1985. 85 с.

14. Козлитин С.Н., Козирацкий Ю.Л., Будников С.А. Моделирование совместного применения средств радиоэлектронной борьбы и огневого поражения в интересах повышения эффективности борьбы за превосходство в управлении // Системы управления, связи и безопасности. 2020;(1):49–73. DOI: 10.24411/2410-9916-2020-00001

15. Вентцель Е.С. Овчаров Л.А. Теория случайных процессов и ее инженерные приложения. М.: Высш. шк., 1998. 354 с.

16. Надеждин Е.Н., Роганов А.А. Параметрический синтез системы активного мониторинга корпоративной вычислительной сети // Современные наукоемкие технологии. 2020. № 10. С. 67–61. DOI: 10.17513/snt.38255

References

1. Andreev N.O. [Modern problems of security of corporate networks]. Journal of Applied Informatics. 2008;1(13):25–31. (In Russ.)

2. Votinov M.V. The Equipment of Automatic Systems with Modern Remote Access and Mobile Control. *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics*. 2017;17(2):141–148. (In Russ.) DOI: 10.14529/ctcr170213

3. Sergeeva T.A., Khazimov M.V. [Information security in the exchange of technological information for the implementation of telecontrol functions in the energy sector]. In: Power industry through the eyes of youth – 2017. Proceedings of the VIII International Scientific and Technical Conference. 2017. P. 292–295. (In Russ.)

4. Lukashev V.M. [Protection of the end resources of the KIS using intelligent security systems]. *Zaŝita informacii. Inside*. 2006;2(8):27–29. (In Russ.)

5. Popov G.A., Simavoryan S.Zh., Simonyan A.R., Ulitina E.I. Modeling of monitoring of information security process on the basis of queuing systems. *Informatics and Applications*. 2020;14(1):71–79. (In Russ.) DOI: 10.14357/19922264200110

6. Krasnozhon Yu.G. Mathematical model as means of optimization of the automation system of the process of incidents of information security management. *Bezopasnost' Informatsionnykh Tekhnologiy*. 2018;25(1):99–107. (In Russ.)

7. Eremenko V.T., Lyakishev A.A. [Optimization of information exchange processes in the system of security and monitoring of the BMS on the example of the technology "Smart House"]. *Bulletin of BSTU named after V.G. Shukhov*. 2017;(7):146–151. (In Russ.) DOI: 10.12737/article_5940f01a8d60b0.87715921

8. Adadurov S.E., Kalinichenko S.V., Lokhvitsky V.A., Khomonenko A.D., Yakovlev V.V. Model for estimation of the operativity of cloud computing with the account of virtualization and security. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskiye nauki = Izvestiya Tula State University. Technical science*. 2017;9-1:233–245. (In Russ.)

9. Shcheglov K.A., Shcheglov A.Yu. Informational system attack threat modeling and interpretation. Part 1. Vulnerability threat modeling and attack threat interpretation. *Information technologies = Informacionnye tehnologii*. 2015;21(12):930–940. (In Russ.)

10. Mantserov S.A., Il'ichev K.V., Bremzen A.M., Balashov V.O. Distributed information-diagnostic process control system. *International Student Scientific Bulletin*. 2017;(6):92. (In Russ.)

11. Samouylov K.E., Botvinko A.Yu., Zaripova E.R. Session setup time estimation in the network with a firewall. *Bulletin of Peoples' friendship university of Russia. Series: Mathematics. Information scinces. Physics*. 2016;(1):59–66. (In Russ.)

12. Bazhaev N.A., Davydov A.E., Krivtsova I.E., Lebedev I.S., Salakhutdinova K.I. The approach to the analysis of the information security wireless network status. *Journal of Applied Informatics*. 2016;11(6(66)):121–128. (In Russ.)

13. Alekseev O. G., Anisimov V. G., Anisimov E. G. *Markovskiye modeli boya* [Markov models of combat]. Moscow: Ministry of defense of the USSR; 1985. 85 p. (In Russ.)

14. Kozlitin S.N., Koziratsky Yu.L., Budnikov S.A. Electronic warfare and fire damage means joint use modeling for improving a superiority of control struggle efficiency. *Systems of Control, Communication and Security*. 2020;(1):49–73. (In Russ.) DOI: 10.24411/2410-9916-2020-00001

15. Wentzel E.S. Ovcharov L.A. *Teoriya sluchaynykh protsessov i yeye inzhenernyye prilozheniya* [Theory of random processes and its engineering applications]. Moscow: Vysshaya shkola, 1998. 354 p. (In Russ.)

16. Nadezhdin E.N., Roganov A.A. Parametric synthesis of the active corporate computer network monitoring. *Modern high technologies*. 2020;(10):67–61. (In Russ.) DOI: 10.17513/snt.38255

Информация об авторах

Ананьев Александр Владиславович, д-р техн. наук, старший научный сотрудник, АО «Научно-производственное предприятие «Полет», Нижний Новгород, Россия; sasha303_75@mail.ru.

Баркалов Сергей Алексеевич, д-р техн. наук, проф., заведующий кафедрой управления, Воронежский государственный технический университет, Воронеж, Россия; barkalov@vgasu.vrn.ru.

Иванников Кирилл Сергеевич, директор научно-производственного комплекса «Специальное программное обеспечение», АО «Научно-производственное предприятие «Радар ммс», Санкт-Петербург, Россия; ivannikov_ks@radar-mms.com.

Моисеев Сергей Игоревич, канд. физ.-мат. наук, доц., доц. кафедры управления, Воронежский государственный технический университет, Воронеж, Россия; mail@moiseevs.ru.

Information about the authors

Alexander V. Ananiev, Dr. Sci. (Eng.), Senior Researcher, JSC Research and Production Enterprise “Polet”, Nizhny Novgorod, Russia; sasha303_75@mail.ru.

Sergey A. Barkalov, Dr. Sci. (Eng.), Prof., Head of the Department of Management, Voronezh State Technical University, Voronezh, Russia; barkalov@vgasu.vrn.ru.

Kirill S. Ivannikov, Director of the Research and Production Complex “Special Software”, JSC Research and Production Enterprise “Radar mms”, St. Petersburg, Russia; ivannikov_ks@ radar-mms.com.

Sergey I. Moiseev, Cand. Sci. (Phys. and Math.), Ass. Prof., Ass. Prof. of the Department of Management, Voronezh State Technical University, Voronezh, Russia; mail@moiseevs.ru.

Статья поступила в редакцию 15.09.2022
The article was submitted 15.09.2022