УДК: 004.491

Александр В. Мельников[1], Николай С. Кобяков[2]
Воронежский институт Министерства внутренних дел Российской Федерации,
пр–кт Патриотов, 53, Воронеж, 394006, Россия
[1]*e-mail: meln78@mail.ru, https://orcid.org/0000-0001-5080-1162*
[2]*e-mail: kkobyakov1234@gmail.com, https://orcid.org/0000-0002-4950-7879*

ПОДХОД К ОЦЕНКЕ ОПАСНОСТИ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ ВРЕДОНОСНЫХ ПРОГРАММ НА АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

DOI: http://dx.doi.org/10.26583/bit.2023.3.03

Аннотация. Целью данной работы является разработка модели для определения значения и уровня опасности вредоносных программ. Актуальность работы подтверждается постоянным увеличением количества вредоносных программ и наносимым ущербом от их реализации, в том числе и на автоматизированные системы специального назначения. В статье рассматриваются три класса вредоносных программ: вредоносные утилиты, троянские программы, вирусы и черви. Рассчитаны весовые коэффициенты для классов вредоносных программ с помощью метода анализа иерархий. Разработан алгоритм для оценки опасности деструктивных воздействий на основе поведенческих паттернов вредоносны программ. Определены пары и тройки поведенческих паттернов, совместная реализация которых повышает опасность деструктивного воздействия вредоносных программ. Выполнена верификация модели для оценки опасности вредоносных программ, реализуемых в различных операционных системах. В ходе верификации модели вредоносным программам определены значения опасности и уровни опасности.

Ключевые слова: вредоносные программы, поведенческие паттерны вредоносных программ, троянские программы, вирусы и черви, вредоносные утилиты.

Для цитирования.: *МЕЛЬНИКОВ, Александр В.; КОБЯКОВ, Николай С. ПОДХОД К ОЦЕНКЕ ОПАСНОСТИ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ ВРЕДОНОСНЫХ ПРОГРАММ НА АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ. Безопасность информационных технологий, [S.l.], т. 30, № 3, с. 51–60, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1529. DOI: http://dx.doi.org/10.26583/bit.2023.3.03.*

Alexander V. Melnikov[1], Nikolai S. Kobyakov[2]
[1]*Voronezh Institute of the Ministry of the Interior of the Russian Federation,*
53 Patriots Ave., Voronezh, 394006, Russia
[1]*e-mail: meln78@mail.ru, https://orcid.org/0000-0001-5080-1162*
[2]*e-mail: kkobyakov1234@gmail.com, https://orcid.org/0000-0002-4950-7879*

Approach to assessing the danger of destructive effects of malware on special-purpose automated systems

DOI: http://dx.doi.org/10.26583/bit.2023.3.03

Abstract. The purpose of this study is to develop models for determining the values and severity levels of malware. The relevance of the study is confirmed by the constant increase in the number of malicious programs and the damage caused by their implementation, including on automated special-purpose systems. This paper discusses three classes of malware: malicious utilities, Trojans, viruses, and worms. Weight coefficients for malware classes are calculated using the hierarchy analysis method. An algorithm for assessing the danger of destructive effects based on the behavioral patterns of malicious programs has been developed. Pairs and triples of behavioral patterns have been identified, the joint implementation of which increases the risk of destructive effects of malware. The model was verified to assess the danger of malware implemented in various operating systems. During the verification of the model, malware has determined the hazard values and hazard levels.

Keywords: malware, classes of malware, behavioral patterns of malware, trojans, viruses and worms, malware utilities.
For citation: MELNIKOV, Alexander V.; KOBYAKOV, Nikolai S. Approach to assessing the danger of destructive effects of malware on special-purpose automated systems. IT Security (Russia), [S.l.], v. 30, no. 3, p. 51–60, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1529. DOI: http://dx.doi.org/10.26583/bit.2023.3.03.

Введение

Автоматизированные системы специального назначения (АССН) предназначены для нужд органов государственной власти, обороны страны, безопасности государства и обеспечения правопорядка [1]. Вопросу актуальности исследования деструктивных воздействий на автоматизированные системы посвящено множество работ [2–6]. Результаты данных работ описывают основные деструктивные воздействия, характерные для автоматизированных систем общего назначения. Исследования [7–9] посвящены описанию различных подходов к анализу деструктивных воздействий на АССН и объекты КИИ. Основными деструктивными воздействиями на автоматизированные системы специального назначения являются вредоносные программы. Оценка опасности вредоносных программ играет важную роль в процессе защиты информации, обрабатываемой в автоматизированных системах специального назначения. Оценивая опасность вредоносных программ, исходя из их поведенческих паттернов, можно определить какой комплекс организационно-технических мер необходимо предпринять для защиты информации от актуальных для конкретной автоматизированной системы специального назначения деструктивных воздействий.

В рамках данной работы рассматриваются три класса вредоносных программ:

1. Вредоносные утилиты – предназначены для автоматизации создания других вирусов, червей или троянских программ, организации DoS-атак на удаленные сервера, взлома других компьютеров[1].

2. Троянские программы – предназначены для осуществления несанкционированных пользователем действий, направленных на уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей[2].

3. Вирусы и черви – их отличительной особенностью является способность к саморазмножению в локальных или сетевых ресурсах компьютера[3].

Существует несколько подходов к оценке опасности деструктивных воздействий на автоматизированные системы специального назначения. В исследованиях [10–13] авторы при оценке опасности деструктивных воздействий и эффективности защиты от них опираются на методы моделирования процессов реализации угроз. «Лаборатория Касперского» проводит оценку опасности вредоносных программ, основываясь на правиле поглощения[4]. Согласно данному правилу класс вредоносной программы определяется самым опасным поведением, из реализуемых. В рамках проведенной работы предлагается определять класс вредоносной программы по самому опасному

[1]Вредоносные утилиты. URL: https://encyclopedia.kaspersky.ru/knowledge/malicious-tools/ (дата обращения: 15.04.2023).
[2]Троянские программы. URL: https://encyclopedia.kaspersky.ru/knowledge/trojans/ (дата обращения: 15.04.2023).
[3]Вирусы и черви. URL: https://encyclopedia.kaspersky.ru/knowledge/viruses-and-worms/ (дата обращения: 15.04.2023).
[4]Правило поглощения. URL: https://encyclopedia.kaspersky.ru/knowledge/rules-for-classifying/ (дата обращения 15.04.2023).

поведенческому паттерну, но для получения количественной оценки опасности необходимо учитывать и менее опасные паттерны.

Цель работы. Разработать модель для оценки опасности вредоносных программ.

Для достижения цели работы необходимо решить следующие задачи:

1. Определить весовые коэффициенты для каждого класса в модели оценки опасности вредоносных программ.
2. Определить поведенческие паттерны, совместная реализация которых, повышает опасность вредоносной программы.
3. Разработать алгоритм вычисления значения опасности вредоносных программ.
4. Провести верификацию разработанной модели.

1. Разработка модели для расчета опасности деструктивных воздействий

В ходе проведения вычислительного эксперимента, на основе численного метода предварительной экспертизы [14, 15], получены следующие результаты для вычисления опасности классов вредоносных программ:

$$J_{\text{ВУ}} = 10\,(0{,}258 * p1 + 0{,}181 * p2 + 0{,}121 * p3 + 0{,}121 * p4 + 0{,}077 * p5 + 0{,}077 * p6 + 0{,}077 * p7 + 0{,}027 * p8 + 0{,}027 * p9 + 0{,}019 * p10 + 0{,}015 * p11)/0{,}516 \quad (1)$$

$$J_{\text{ТП}} = 10\,(0{,}229 * p12 + 0{,}229 * p13 + 0{,}118 * p14 + 0{,}118 * p15 + 0{,}081 * p16 + 0{,}081 * p17 + 0{,}042 * p18 + 0{,}03 * p19 + 0{,}021 * p20 + 0{,}021 * p21 + 0{,}014 * p22 + 0{,}014 * p23)/0{,}458 \quad (2)$$

$$J_{\text{ВЧ}} = 10\,(0{,}534 * p24 + 0{,}354 * p25 + 0{,}067 * p26 + 0{,}069 * p27)/0{,}534 \quad (3)$$

В приведенных выше формулах используются следующие обозначения:

$J_{\text{ВУ}}$ – опасность вредоносных программ класса вредоносные утилиты;

$J_{\text{ТП}}$ – опасность вредоносных программ класса троянские программы;

$J_{\text{ВЧ}}$ – опасность вредоносных программ класса вирусы и черви;

$p_{1\text{-}27}$ – поведенческие паттерны вредоносных программ, табл. 1

Для определения весовых коэффициентов опасности классов вредоносных программ проведен опрос 10 специалистов в области защиты информации. Результаты опроса были обобщены, а также определены наиболее близкие значения к мнениям экспертов для матрицы парных сравнений, табл. 2.

Таблица 2. Матрица парных сравнений

Классы	Вирусы и черви	Троянские программы	Вредоносные утилиты
Вирусы и черви	1	4	7
Троянские программы	1/4	1	4
Вредоносные утилиты	1/7	1/4	1

В данной таблице представлены результаты опроса в формате матрицы парных сравнений. Из данной матрицы видно, что по мнению экспертов вредоносное ПО класса вирусы и черви опаснее, чем вредоносное ПО класса троянские программы в 4 раза, вредоносные утилиты в 7 раз, а троянские программы опаснее чем вредоносные утилиты в 4 раза.

Далее с использованием программного обеспечения Mathcad определены собственные векторы для классов вредоносных программ, рис. 1. В данной матрице представлены результаты вычислений собственных векторов для каждого класса

вредоносных программ: в первой строке для вирусов и червей, во второй для троянских программ, в третьей для вредоносных утилит.

$$\text{eigenvecs}(A) = \begin{pmatrix} 0.945 & 0.945 & 0.945 \\ 0.311 & -0.156 + 0.269i & -0.156 - 0.269i \\ 0.102 & -0.051 - 0.089i & -0.051 + 0.089i \end{pmatrix}$$

Рис. 1. Собственные векторы классов вредоносных программ
Fig. 1. Eigenvectors of malware classes

Таблица 1. Поведенческие паттерны

Поведенческий паттерн	Обозначение
Проникновение на компьютер-жертву	p1
Скрытие следов присутствия преступников в системе	p2
Внесение в список разрешенных посетителей системы новых пользователей	p3
Прекращение работы системы	p4
Проведение атак типа «Отказ в обслуживании»	p5
Сбор и анализ сетевых пакетов	p6
Подмена адреса отправителя письма по электронной почте	p7
Создание вредоносных программ	p8
Навязывание ложной информации (уведомление об опасности, нарушениях)	p9
Модификация вредоносных программ	p10
Распространение флуда (бесполезных сообщений по каналам электронной почты)	p11
Скрытое удаленное управление злоумышленником пораженным компьютером	p12
Ведение электронного шпионажа (вводимая с клавиатуры информация и др.)	p13
Несанкционированная пользователем модификация данных таким образом, чтобы сделать невозможной работу с ними	p14
Кража пользовательских аккаунтов (логин/пароль)	p15
Несанкционированная пользователем загрузка и установка вредоносных программ (без интернета)	p16
Несанкционированная пользователем загрузка и установка вредоносных программ (через интернет)	p17
Сбор адресов электронной почты	p18
Имитация работы средств антивирусной защиты	p19
Несанкционированный пользователем доступ к различным интернет-ресурсам	p20
Оповещение злоумышленника о том, что зараженный компьютер появился в сети	p21
«Архивная бомба»	p22
«Кликер»	p23
Несанкционированное пользователем саморазмножение в компьютерных сетях	p24
Несанкционированное пользователем саморазмножение в компьютерных сетях (необходим пользователь)	p25
Несанкционированное пользователем саморазмножение по локальным ресурсам компьютера	p26
Несанкционированное пользователем саморазмножение по каналам электронной почты	p27

Вектор коэффициентов относительной важности признаков (вектор приоритетов), предложенный в [16], имеет вид:

$$V = (V_1, V_2, V_3), \quad (4)$$

где $V_{1\text{-}3}$ – коэффициенты относительной важности классов вредоносных программ.

В [16] предложена нормировка элементов собственного вектора делением на сумму его элементов:

$$\hat{V} = (\widehat{V_1}, \widehat{V_2}, \widehat{V_3}), \quad (5)$$

где $\widehat{V_{1-3}}$ – нормированные весовые коэффициенты относительной важности классов вредоносных программ.

Нормирование обеспечивает соотношение $\sum Vi = 1$.

В данной работе нормированные весовые коэффициенты равны:

$$\hat{V} = (0{,}696; 0{,}229; 0{,}075). \quad (6)$$

Таким образом, модель для расчета оценки опасности вредоносных программ будет иметь следующий вид:

$$J_{\text{ВП}} = J_{\text{ВУ}} * 0{,}075 + J_{\text{ТП}} * 0{,}229 + J_{\text{ВЧ}} * 0{,}696. \quad (7)$$

2. Определение пар и троек поведенческих паттернов вредоносных программ

При выполнении верификации данной модели было определено, что значения опасности вредоносных программ не соответствовали их реальному деструктивному воздействию. Для получения более объективного значения были определены поведенческие паттерны, совместная реализация которых повышает деструктивное воздействия вредоносной программы. Примером таких поведенческих паттернов может служить пара «Скрытие следов присутствия преступника в системе (p2)» и «Ведение электронного шпионажа (p13)». Совместная реализация данных поведенческих паттернов позволяет злоумышленнику получить доступ к информации, обрабатываемой пользователем, а также долгое время оставаться незамеченным в системе, что влечет за собой более значительные последствия, как для конкретного пользователя, так и для всей автоматизированной системы. Кроме того, в ходе выполнения исследования, оказалось, что имеют место быть тройки поведенческих паттернов, повышающих деструктивное воздействие на автоматизированные системы. К примеру, поведенческие паттерны «Прекращение работы системы (p4)», «Несанкционированная пользователем модификация данных таким образом, чтобы сделать невозможной работу с ними (p14)» и «Несанкционированное пользователем саморазмножение в компьютерных сетях (p24)», реализуемые в одной вредоносной программе, обеспечивают выполнение комплекса действий, которые приводят к нарушению доступности одного рабочего места, а затем и всех ресурсов автоматизированных систем специального назначения. Всего было определено 38 пар и 5 групп по три поведенческих паттерна, совместная реализация которых приводит к повышению деструктивного воздействия вредоносных программ на автоматизированные системы специального назначения.

Для учета данного фактора решено увеличивать сумму значений опасности таких поведенческих паттернов в 2 раза (коэффициент z).

На основании вышеизложенного разработан алгоритм для оценки опасности вредоносных программ, приведенный на рис. 2.

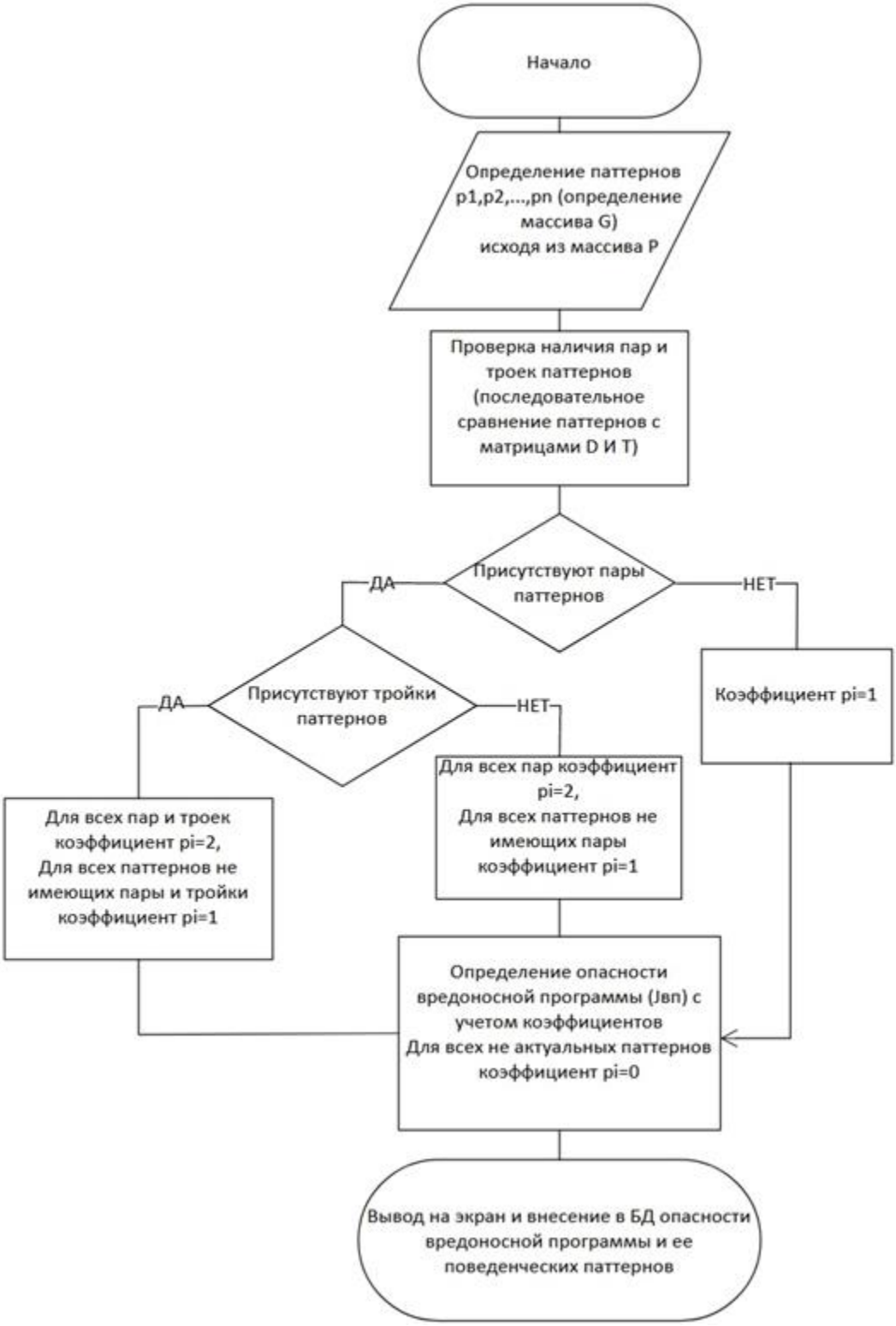

Рис. 2. Алгоритм вычисления значения опасности вредоносных программ
Fig. 2. Algorithm for Calculating the Malware Danger Value

Массив P представляет собой множество поведенческих паттернов вредоносных программ всех классов:

$$P = (p_1; p_2; \dots; p_{27}). \quad (8)$$

Далее, необходимо определить множество G, которое включает поведенческие паттерны, реализуемые конкретной вредоносной программой:

$$G = (p_1; p_2; \dots; p_n). \quad (9)$$

В матрице D представлены пары поведенческих паттернов, совместная реализация которых повысит деструктивность вредоносной программы, и, следовательно, ее опасность:

$$D = \begin{pmatrix} p_1 & p_{12} \\ p_1 & p_{13} \\ \dots & \dots \\ p_{20} & p_{23} \end{pmatrix}. \quad (10)$$

Матрица T включает тройки поведенческих паттернов:

$$T = \begin{pmatrix} p_1 & p_{13} & p_{15} \\ p_3 & p_{12} & p_{13} \\ p_4 & p_{14} & p_{24} \\ p_7 & p_{18} & p_{27} \\ p_{12} & p_{13} & p_{15} \end{pmatrix}. \quad (11)$$

Данный алгоритм реализован в программе для ЭВМ [17].

3. Верификация модели

Результаты верификации модели с учетом поведенческих паттернов, совместная реализация которых повышает опасность вредоносной программы, представлены в табл. 3.

Таблица 3. Верификация модели

Вредоносная программа	Реализуемые поведенческие паттерны	Опасность	Уровень опасности
Trojan.Siggen20.2910	p2,p4,p14,p26	3.54	Низкий
DDoS.Kardraw.13	p1,p2,p5	0,75	Низкий
BackDoor.ProRat.	p2,p5,p13,p14	4,348	Средний
Win32.HLLW.Autoruner1.50680	p2,p17,p20,p26	1,646	Низкий
Win32.HLLM.Julio.203	p11,p15,p18,p20,p27	2,333	Низкий
VirusConstructor.Binder.5	p2,p8,p10	0,658	Низкий
Petya	p1,p4,p9,p14,p17,p19,p24	10	Критический
Trojan.MulDrop.53.origin	p2, p17, p20, p27	1,359	Низкий
Trojan.KeyLogger.10096	p2, p13, p26	3,689	Низкий
Tool.Flooder.81	p7, p11, p18, p27	1,858	Низкий
Win32.HLLO.Siggen.8	p17, p20, p23, p26	3,54	Низкий
Trojan.Fakealert.30341	p1,p2,p20	0,731	Низкий
Linux.Aliande.1	p1,p6,p15	2,154	Низкий
Linux.Siggen.236	p1,p3,p13	3,392	Низкий
Linux.DDoS.89	p5,p6,p12,p20	1,538	Низкий
Linux.Siggen.366	p1,p2,p6,p20	0,855	Низкий
Linux.Siggen.941	p14,p20	0,695	Низкий
Linux.UbntFM.2	p1,p3,p6,p16,p17,p24	10	Критический
Linux.Themoon.2	p1,p6,p17,p20	0,967	Низкий
Linux.Sshdkit.6	p1,p2,p15	2,149	Низкий

В табл. 3 поведенческие паттерны троек выделены синим, а пар красным цветом. В случае, если опасность после учета фактора становится больше максимального значения 10, то опасность оценивается по максимальному значению. Для расчета опасности вредоносных программ использовались формулы (1), (2), (3), (7).

Заключение

Для оценки опасности деструктивных воздействий, актуальных для автоматизированных систем специального назначения, разработана модель. В ходе исследований и моделирования решены следующие задачи:

1. Определены весовые коэффициенты для классов в модели оценки опасности вредоносных программ (0, 075 для вредоносных утилит; 0,229 для троянских программ; 0, 696 для вирусов и червей).
2. Определены поведенческие паттерны, совместная реализация которых, увеличивает опасность вредоносных программ (38 пар и 5 групп по три поведенческих паттерна).
3. Написана программа для ЭВМ на основе разработанного алгоритма.
4. Выполнена верификация разработанной модели на примере двадцати вредоносных программ.

СПИСОК ЛИТЕРАТУРЫ:

1. Горяинов Р.И., Левко И.В., Шуваев Н.А. Метод распределения информационных потоков в автоматизированных системах специального назначения. Известия Тульского государственного университета. Технические науки. 2022, № 10, с. 18–22. – EDN CRJCTI.
2. Громов Ю.Ю., Карасев П.И., Губсков Ю.А., Котюкова В.О. Оценка эффективности систем защиты информации и анализ рисков информационной безопасности в организации. Информация и безопасность. 2022, т. 25, № 2, с. 187–192. DOI: http://dx.doi.org/10.36622/VSTU.2022.25.2.003. – EDN EDRNYF.
3. Gromov Y., Minin Y., Eliseev A., Abdulkarem Habib Alrammahi A. and Abbac Sari F. Building an External Classifier of Negative Impacts in Assessing Survivability and Ensuring the Security of Information Systems. 2nd International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA), Lipetsk, Russia. 2020, p. 636–641. DOI: http://dx.doi.org/10.1109/SUMMA50634.2020.9280776. – EDN IBBYMN.
4. Криулин А.А., Нефедов В.С., Потерпеев Г.Ю., Якунин В.И. Подход к анализу вредоносного программного обеспечения с использованием мультиклассовой классификации. Труды Военно-космической академии имени А.Ф. Можайского. 2021, № 679, с. 128–136. – EDN NFIURE.
5. Горячев Сергей Н.; Кобяков Николай С. Оценка состояния защищенности информационных систем от вредоносных программ. Безопасность информационных технологий, [S.l.]. 2022, т. 29, № 1, с. 44–56. DOI: http://dx.doi.org/10.26583/bit.2022.1.05. – EDN FPSNRR.
6. Кобяков Н.С., Мельников А.В., Горячев С.Н. О некоторых вопросах оценки опасности деструктивного воздействия вредоносных программ на автоматизированные системы. Вестник Пермского университета. Математика. Механика. Информатика. 2023, № 1(60), с. 77–83. – EDN OWXAHO.
7. Кочнев С.В., Лапсарь А.П., Барабошкина А.В. Синтез структуры объектов критической информационной инфраструктуры производственных процессов на основе марковских моделей. Прикаспийский журнал: управление и высокие технологии. 2022, № 1(57), с. 93–105. DOI: http://dx.doi.org/10.54398/2074-1707_2022_1_93. – EDN QFRGKT.
8. Анисимов В.Г., Анисимов Е.Г., Сауренко Т.Н., Зотова Е.А. Модели прогнозирования опасности деструктивных воздействий на информационные процессы в системах управления // Информационно-управляющие системы. 2019, № 5, с. 18–23. DOI: http://dx.doi.org/10.31799/1684-8853-2019-5-18-23. – EDN SEDJSI.
9. Жарова О.Ю. Разработка критериев оценки внешнего воздействия деструктивных потоков данных на технологическую сеть промышленного предприятия. Известия высших учебных заведений. Поволжский регион. Технические науки. 2020, № 3(55), с. 4–16. DOI: http://dx.doi.org/10.21685/2072-3059-2020-3-1. – EDN JCVEFV.

10. Язов Ю.К., Соловьев С.В., Тарелкин М.А. Логико-лингвистическое моделирование угроз безопасности информации в информационных системах. Вопросы кибербезопасности. 2022, № 4(50), с. 13–25. DOI: http://dx.doi.org/10.21681/2311-3456-2022-4-13-25. – EDN XEEFHI.
11. Язов Ю.К., Соловьев С.В. Моделирование значимых объектов критической информационной инфраструктуры в интересах исследования защищенности применяемых в них информационных технологий. Безопасные информационные технологии: Сборник трудов Одиннадцатой международной научно-технической конференции, Москва, 06–07 апреля 2021 года. М.: Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет). 2021, с. 363–369. – EDN LSOBLP.
12. Язов Ю.К., Соловьев С.В. Методология оценки эффективности защиты информации в информационных системах от несанкционированного доступа. Санкт-Петербург: Издательство «Наукоемкие технологии», 2023. – 258 с. ISBN 978-5-907618-36-7. – EDN WVCHKW.
13. Машкина Ирина В.; Гарипов Ильдар Р. Разработка EPC-моделей угроз нарушения информационной безопасности автоматизированной системы управления технологическими процессами. Безопасность информационных технологий, [S.l.]. 2019, Т. 26, № 4, с. 6–20. DOI: http://dx.doi.org/10.26583/bit.2019.4.01. – EDN KYEBPF.
14. Мельников А.В., Четверикова А.И. Модели принятия решений при оперативном управлении силами и средствами органов внутренних дел. Вестник Воронежского института МВД России. 2023, № 1, с. 40–47. – EDN SGKDBS.
15. Мельников А.В. Метод оценки степени обфускации программы для ЭВМ на основе кластерно-иерархического подхода. Общество и экономическая мысль в XXI В.: пути развития и инновации: Материалы X Международной научно-практической конференции (посвященной 115-летию Университета), Воронеж, 21 апреля 2022 года. Воронеж: Издательско-полиграфический центр «Научная книга». 2022, с. 460–463. – EDN SFHOJQ.
16. Мельников А.В. Кластерно-иерархические методы экспертизы технических и экономических объектов: автореф. дисс. … докт. техн. наук: 05.13.18. Воронеж, 2014. – 32 с.
17. Кобяков Н.С., Мельников А.В., Поляков К.А., Плюхин А.Ю. Расчет опасности вредоносных программ. Свидетельство о государственной регистрации программы для ЭВМ RU № 2023662134. Заявка № 2023660462 от 23.05.2023, опубл. 06.06.2023. – EDN CBJXFU.

REFERENCES:

[1] Goryainov R.I., Levko I.V., Shuvaev N.A Analysis of methods of flow distribution in information systems for special purposes. Izvestiya of Tula State University. Technical Sciences. 2022, no. 10, p. 18–22. DOI: http://dx.doi.org/10.24412/2071-6168-2022-10-18-22 (in Russian). – EDN CRJCTI.
[2] Gromov Yu.Yu., Karasev P.I., Gubskov Yu.A., Kotyukova V.O. Evaluation of the effectiveness of information security systems and analysis of information security risks in the organization. Information and Security. 2022, v. 25, no. 2, p. 187–192. DOI: http://dx.doi.org/10.36622/VSTU.2022.25.2.003 (in Russian). – EDN EDRNYF.
[3] Gromov Y., Minin Y., Eliseev A., Alrammahi A.A.H. and Sari F.A. Building an External Classifier of Negative Impacts in Assessing Survivability and Ensuring the Security of Information Systems. 2nd International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA), Lipetsk, Russia. 2020, p. 636–641. DOI: http://dx.doi.org/10.1109/SUMMA50634.2020.9280776 (in Russian). – EDN IBBYMN.
[4] Kriulin A.A., Nefedov V.S., Poterpeev G.Yu., Yakunin V.I. Approach to analysis of malicious software using multiclass classification. Proceedings of the A.F. Mozhaisky Military-Space Academy. 2021, no. 679, p. 128–136 (in Russian). – EDN NFIURE.
[5] Goryachev Sergey N.; Kobyakov Nikolai S. Assessment of the state of protection of information systems against malware. IT Security (Russia), [S.l.], v. 29, no. 1, p. 44–56, 2022. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2022.1.05 (in Russian). – EDN FPSNRR.
[6] Kobyakov N.S., Melnikov A.V., Goryachev S.N. About some consequences of destructive influence software virus for automatic systems. Perm University Herald. Mathematics. Mechanics. Informatics. 2023, no. 1(60), p. 77–83. DOI: http://dx.doi.org/10.17072/1993-0550-2023-1-77-83 (in Russian). – EDN OWXAHO.
[7] Kochnev S.V., Lapsar A.P., Baraboshkina A.V. Designing the markov models-based structure for critical information infrastructure objects of production processes. Caspian Journal: Management and High Technologies. 2022, no. 1(57), p. 93–105. DOI: http://dx.doi.org/10.54398/2074-1707_2022_1_93 (in Russian). – EDN QFRGKT.
[8] Anisimo V.G., Anisimov E.G., Saurenko T.N., Zotova E.A. Models of forecasting destructive influence risks for information processes in management systems. Information and Control Systems. 2019, 5, p. 18–23. DOI: https://doi.org/10.31799/1684-8853-2019-5-18-23. – EDN SEDJSI.

[9] Zharova O.Yu. The development of criteria for assessing the external impact of destructive data flows on the technological network of an industrial enterprise. Proceedings of Higher Educational Institutions. Volga Region. Technical Sciences. 2020, no. 3(55), p. 4–16. DOI: https://doi.org/10.21685/2072-3059-2020-3-1 (in Russian). – EDN JCVEFV.
[10] Yazov Yu.K., Solovyev S.V., Tarelkin M.A. 2022, no. 4(50), p. 13–25. DOI: https://doi.org/10.21681/2311-3456-2022-4-13-25 (in Russian). – EDN XEEFHI.
[11] Yazov Yu.K., Solovyev S.V. Simulation of significant objects of critical information infrastructure in the interest of investigating the security of information technologies used therein. Safe information technologies: Proceedings of the Eleventh International Scientific and Technical Conference, Moscow, April 06-07, 2021. M.: Bauman Moscow State Technical University (National Research University) (Moscow). 2021, p. 363–369 (in Russian). – EDN LSOBLP.
[12] Yazov Yu.K., Solovyev S.V. Methodology for evaluating the effectiveness of protecting information in information systems from unauthorized access. St. Petersburg: "Nauchnoemkie tekhnologii" Publishers, 2023. – 258 p. - ISBN 978-5-907618-36-7 (in Russian). – EDN WVCHKW.
[13] Mashkina Irina V.; Garipov Ildar R. Development of EPC-Models of threats to information security of the automated process control system. IT Security (Russia), [S.l.], v. 26, no. 4, p. 6–20, 2019. ISSN 2074-7136. DOI: https://doi.org/10.26583/bit.2019.4.01 (in Russian). – EDN KYEBPF.
[14] Melnikov A.V., Chetverikova A.I. Models of decision-making in the operational management of the forces and facilities of the internal affairs bodies. Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. 2023, no. 1, p. 40–47 (in Russian). – EDN: SGKDBS.
[15] Melnikov A.V. Method for evaluating the degree of obfuscation of a computer program based on a cluster-hierarchical approach. Society and Economic Thought in the XXI Century: Development Paths and Innovations: Proceedings of the Tenth International Scientific and Practical Conference (Dedicated to the 115th Anniversary of the University), Voronezh, April 21, 2022. Voronezh: Publishing and Polygraphic Center "Scientific Book". 2022, p. 460–463 (in Russian). – EDN SFHOJQ.
[16] Melnikov A.V. Cluster-hierarchical methods of expert review of technical and economic objects: author's abstract. diss.... Dr. Techn. Sciences: 05.13.18. Voronezh, 2014. – 32 p. (in Russian).
[17] Kobyakov N.S, Mel'nikov A.V., Polyakov K.A., Plyuhin A.YU. Raschet opasnosti vredonosnyh program. Svidetel'stvo o gosudarstvennoj registracii programmy dlya EVM RU № 2023662134. Zayavl.№ 2023660462, 23.05.2023 : opubl. 06.06.2023 (in Russian). – EDN CBJXFU.

Поступила в редакцию – 18 апреля 2023 г. Окончательный вариант – 22 августа 2023 г.
Received – April 18, 2023. The final version – August 22, 2023.