УДК 004.94
DOI 10.52575/2712-746X-2023-50-4-873-882

Модель оценки эффективности организационных мер для обеспечения информационной безопасности АССН при появлении неизвестной вредоносной программы

[1] Мельников А.В., [2] Сумин В.И., [1] Кобяков Н.С.
[1] Воронежский институт МВД России,
Россия, 394065, г. Воронеж, пр. Патриотов, д. 53
[2] Воронежский институт ФСИН России
Россия, 394072, г. Воронеж, ул. Иркутская, д. 1а
E-mail: meln78@mail.ru, viktorsumin51@yandex.ru, kkobyakov1234@gmail.com

Аннотация. В статье рассматриваются вопросы обеспечения информационной безопасности автоматизированных систем специального назначения при появлении неизвестных вредоносных программ. Обсуждаются вопросы реализации организационных мер обеспечения информационной безопасности, направленные на подготовку пользователей автоматизированных систем специального назначения. Для оценки эффективности принятых организационных мер сформирована модель на основе метода анализа иерархий. Исходя из численного эксперимента, рассчитан корректирующий коэффициент с использованием искусственной нейронной сети. Итоговая модель верифицирована на тестовом наборе данных и может применяться руководителями подразделений, обеспечивающих информационную безопасность для принятия управленческих решений.

Ключевые слова: метод анализа иерархий, искусственная нейронная сеть, цели обеспечения информационной безопасности

Для цитирования: Мельников А.В., Сумин В.И., Кобяков Н.С. 2023. Модель оценки эффективности организационных мер для обеспечения информационной безопасности АССН при появлении неизвестной вредоносной программы. Экономика. Информатика, 50(4): 873–882. DOI: 10.52575/2712-746X-2023-50-4-873-882

Model for Assessing the Effectiveness of Organizational Measures to Ensure Information Security of ASSN When an Unknown Malware Appears

[1] Alexander V. Melnikov, [2] Victor I. Sumin, [1] Nikolay S. Kobyakov
[1] Voronezh Institute of the Ministry of Internal Affairs of Russia
53 Patriots Ave., Voronezh, 394065, Russia
[2]VRI of the FPS of Russia
1a Irkutskaya St, Voronezh, 394072, Russia
E-mail: meln78@mail.ru, viktorsumin51@yandex.ru, kkobyakov1234@gmail.com

Abstract. The article discusses issues of ensuring information security of automated special-purpose systems in the event of the appearance of unknown malicious programs. Issues of implementing organizational measures to ensure information security aimed at training users of special-purpose automated systems are discussed. The goals for implementing organizational measures are identified as signs for forming a model. To assess the effectiveness of the organizational measures taken, a model was formed based on the hierarchy analysis method. The initial data for forming the model are the results of a survey of specialists in the field of information security. During the survey, experts assessed the effectiveness of the measures in accordance with a linguistic scale from 0 to 10. Based on a numerical

experiment, a correction factor is calculated using an artificial neural network. Fourteen examples are defined for training the artificial neural network. The final model was tested on a test data set and can be used by heads of information security departments to make management decisions.

Keywords: analytic hierarchy process, artificial neural network, information security objectives

For citation: Melnikov A.V., Sumin V.I., Kobyakov N.S. 2023. Model for Assessing the Effectiveness of Organizational Measures to Ensure Information Security of ASSN When an Unknown Malware Appears. Economics. Information technologies, 50(4): 873–882 (in Russian). DOI: 10.52575/2712-746X-2023-50-4-873-882

Введение

Обеспечение информационной безопасности становится все более актуальным в условиях появления большого количества автоматизированных систем [Sumin et al., 2021]. Автоматизированные системы специального назначения также получают все более широкое распространение, поскольку позволяют ускорить выполнение задач, возложенных на подразделение. Такое широкое распространение автоматизированных систем приводит к появлению новых и совершенствованию уже существующих методов по противодействию угроз злоумышленников. Одной из наиболее актуальных угроз информационной безопасности автоматизированных систем специального назначения является реализация деструктивных функций вредоносных программ. Меры по обеспечению информационной безопасности могут быть законодательные, организационные, технологические, морально-этические, физические и программно-аппаратные (технические). Несмотря на важность вышеперечисленных мер, должностным лицам, обеспечивающим информационную безопасность автоматизированных систем специального назначения, особое внимание следует уделять организационным мерам.

В настоящее время отсутствуют подходы, предназначенные для численной оценки эффективности применения организационных мер обеспечения информационной безопасности автоматизированных систем специального назначения. Оценка эффективности принятых организационных мер позволит определить их необходимый набор для обеспечения информационной безопасности в зависимости от опасности вредоносной программы.

Объекты и методы исследования

Цель работы: разработка модели оценки эффективности принятых организационных мер по подготовке пользователей автоматизированных систем специального назначения для обеспечения информационной безопасности в условиях возможной реализации деструктивных функций неизвестных вредоносных программ.

Постановка задачи. Для достижения цели работы необходимо решить следующие задачи:

1. Определить цели реализации организационных мер по подготовке пользователей АССН для обеспечения информационной безопасности.
2. Определить перечень организационных мер по подготовке пользователей АССН для обеспечения информационной безопасности.
3. Сформировать модель для оценки эффективности принятых организационных мер.
4. Выполнить верификацию разработанной модели.

Результаты и их обсуждение

Автоматизированные системы специального назначения становятся все более распространены и необходимы для оперативного решения задач [Сумин, 2023; Сумин, Громов, Тютюнник, 2023; Сумин и др., 2023]. Вопросы деструктивных воздействий вредо-

носных программ широко исследуются во многих современных исследованиях [Наличев и др., 2021; Середкин, 2022]. Авторы приходят к единому мнению о том, что обеспечение информационной безопасности является одним из наиболее актуальных направлений деятельности государства. Особенно актуален вопрос обеспечения информационной безопасности автоматизированных систем от неизвестных вредоносных программ для силовых ведомств.

Исходя из опыта обеспечения информационной безопасности автоматизированных систем специального назначения и результатов научных исследований, определены цели реализации организационных мер по подготовке пользователей для обеспечения информационной безопасности в условиях возможной реализации деструктивных функций неизвестных вредоносных программ [Язов, Соловьев, 2018; Жиляков и др., 2021; Горячев, Кобяков, 2022; Жиляков, Лубков, Болгова, 2022; Мельников, Кобяков, Жилин, 2023]:

1. Недопущение создания угроз реализации деструктивных функций вредоносных программ при эксплуатации автоматизированных систем специального назначения. Достижение цели подразумевает четкое знание каждым пользователем автоматизированной системы специального назначения актуальных угроз деструктивных функций вредоносных программ и действий по недопущению их реализации (e_1).

2. Умение пользователей эксплуатировать автоматизированную систему специального назначения в новых условиях. В результате достижения цели пользователи смогут эксплуатировать автоматизированную систему специального назначения и выполнять свои служебные обязанности в полном объеме, несмотря на ограничения (e_2).

3. Знание и понимание алгоритма действий в случае обнаружения признаков реализации деструктивных функций вредоносных программ на автоматизированном рабочем месте пользователя. Достижение цели обеспечит своевременную реакцию пользователей на заражение автоматизированного рабочего места вредоносной программой и реализацию действий по недопущению ее дальнейшего распространения по сети или другим рабочим местам (e_3).

4. Понимание ответственности за нарушение новых требований по обеспечению безопасности информации, обрабатываемой в автоматизированной системе специального назначения. В результате достижения цели пользователи будут осознавать в полном объеме ответственность за реализацию угроз информационной безопасности вследствие их действий или бездействий (e_4).

5. Осведомленность пользователей о появлении неизвестной вредоносной программы. Достижение данной цели обеспечит информированность пользователей о том, что появилась неизвестная вредоносная программа и описание ее функций (e_5).

Достижение всех целей часто не целесообразно по следующим причинам:

1. Специалистов в области обеспечения информационной безопасности намного меньше, чем пользователей автоматизированных систем специального назначения, их привлечение к проведению занятий может привести к недостаточному вниманию на непосредственно обеспечение безопасности информации.

2. Отрыв пользователей автоматизированных систем специального назначения от исполнения своих должностных обязанностей на продолжительное время.

3. Создание и ведение дополнительных служебных документов для учета различных отчетных данных.

Для объективной оценки необходимости реализации организационных мер в работе [Мельников, Кобяков, 2023] предложен подход, согласно которому реализуемые меры выбираются исходя из оценки опасности вредоносных программ.

Для оценки опасности вредоносных программ в [Кобяков, 2023; Мельников, Кобяков, 2023; Кобяков и др., 2023] предложена лингвистическая шкала:

1. Низкая опасность [0 – 3.99].

2. Средняя опасность [4.0 – 6.99].

3. Высокая опасность [7.0 – 8.99].

4. Критическая опасность [9.0 – 10.0].

Целесообразно сформировать модель для оценки эффективности реализованных организационных мер с той же лингвистической шкалой. Следовательно, для вредоносных программ с низкой опасностью нужно реализовывать организационные меры с низкой эффективностью, и т.д.

Для формирования модели для оценки эффективности принятых организационных мер воспользуемся подходом на основе метода анализа иерархий, реализованного в работах [Жилин, 2022; Мельников, Сумин, Кобяков, 2023].

Основываясь на результатах опроса 10 специалистов в области обеспечения информационной безопасности автоматизированных систем специального назначения, получим следующую модель для оценки эффективности принятых организационных мер:

$$E_M = 10 \times (0{,}474 \times e_1 + 0{,}237 \times e_2 + 0{,}158 \times e_3 + 0{,}079 \times e_4 + 0{,}053 \times e_5) \quad (1)$$

Для верификации данной модели рассчитаем эффективность принятых мер с использованием модели и сравним результаты с мнением экспертов. Сравнение результатов представлено в таблице 1.

Таблица 1
Table 1

Сравнение результатов оценки эффективности мер
Comparison of the results of assessing the effectiveness of measures

№ п/п	Организационная мера	Достигнутые цели	Эфф. (модель)	Эфф. (опрос)	Эфф. (ИНС)
1.	Проведение комплексных занятий с пользователями	e_1, e_2, e_3, e_4, e_5	10	10	9.78
2.	Проведение практических занятий по недопущению нелегитимных действий пользователей	e_1, e_3, e_5	6,32	6,6	5.92
3.	Контроль за используемыми ресурсами АССН	e_1, e_4	5,53	5,75	6.15
4.	Выдача инструкций по порядку действий в случае обнаружения ВП, с описанием ее функций	e_3, e_5	2,11	2,5	3.07
5.	Проведение информирования с пользователями	e_4, e_5	1,32	3,1	3.3
6.	Проведение практических занятий по порядку эксплуатации АССН, с акцентом на информацию о ВП и ответственности за нарушение требований по ИБ	e_2, e_4, e_5	3,69	6	5.42
7.	Проведение практических занятий по порядку эксплуатации АССН, с акцентом на недопущение действий, которые могут привести к созданию угроз ИБ	e_1, e_2	7,11	7,5	7.09
8.	Выдача инструкций в случае обнаружения ВП и обязательный учет работы пользователей в АССН	e_3, e_4	2,37	3	3.68
9.	Проведение информирования с пользователями о функциях ВП и действиях, которые могут привести к их реализации	e_1, e_5	5,27	5,7	5.54
10.	Проведение практических занятий по порядку эксплуатации АССН, с акцентом на информацию о ВП	e_2, e_5	2,9	3,25	4.25

Окончание табл.1
End table 1

№ п/п	Организационная мера	Достигнутые цели	Эфф. (модель)	Эфф. (опрос)	Эфф. (ИНС)
11.	Проведение практических занятий по порядку эксплуатации АССН и порядку действий при обнаружении признаков реализации функций ВП	e_2, e_3	4	4,5	4.63
12.	Проведение практических занятий по недопущению нелегитимных действий пользователей и учет работы пользователей в АССН	e_1, e_3, e_4	6,399	6,5	7.09
13.	Проведение практических занятий по недопущению нелегитимных действий пользователей и порядку эксплуатации АССН	e_1, e_2, e_3	8,69	8	8.04
14.	Проведение занятий по порядку действий при обнаружении признаков реализации функций ВП и учет работы пользователей в АССН	e_3, e_4, e_5	2,9	5,35	4.25

Как мы видим, в 3-ех случаях (№5, №6, №14) сильно разнится мнение экспертов об оценке эффективности применения организационных мер и результат оценки с использованием модели. Для уточнения результатов сформируем искусственную нейронную сеть. Параметры искусственной нейронной сети представлены в таблице 2.

Таблица 2
Table 2

Параметры искусственной нейронной сети
Artificial neural network parameters

Название параметра	Описание
Язык программирования	Python
Используемые библиотеки	Numpy, Keras, Tensorflow
Количество слоев	1
Количество входных нейронов	5
Функция активации	ReLU (Rectified Linear Unit)
Функция потерь	MSE (Mean squared error)
Функция оптимизации	SGD (Stochastic gradient descent)
Количество эпох обучения	600

Обучив нейронную сеть, получим следующую модель для оценки эффективности организационных мер:

$$E_M = 10 \times (0{,}425 \times e_1 + 0{,}233 \times e_2 + 0{,}121 \times e_3 + 0{,}148 \times e_4 + 0{,}072 \times e_5) \quad (2)$$

При сравнении результатов, рассчитанных с использованием данной модели, точность повышается, но, вместе с тем, в примере №10 в ходе опроса определен уровень эффективности «низкий», а в ходе моделирования с использованием искусственной нейронной сети «средний».

Рассмотрим весовые коэффициенты искусственной нейронной сети и метода анализа иерархий, представленные на рисунке 1.

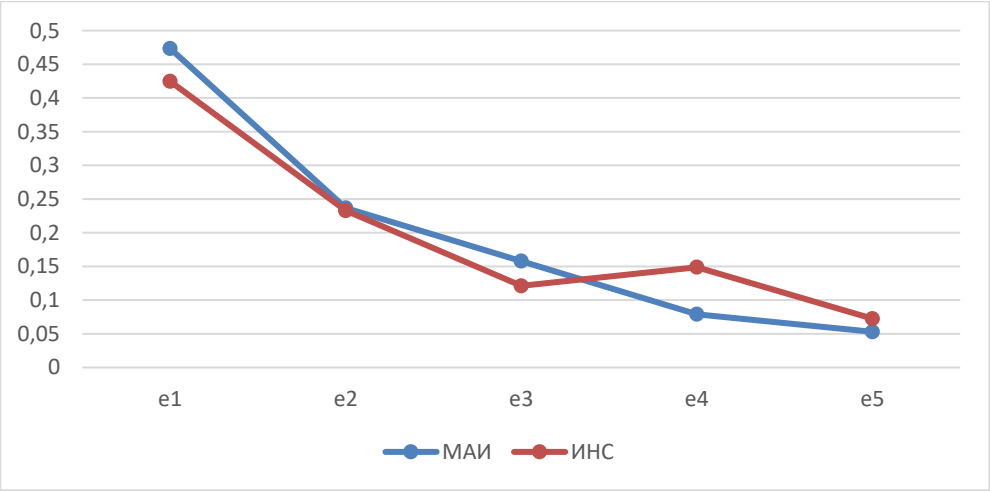

Рис 1. Сравнение весовых коэффициентов достигаемых целей
Fig.1 Comparison of weighting coefficients of achieved goals

Исходя из графика, видно, что в ходе моделирования искусственной нейронной сетью весовые коэффициенты у целей №4 и №5 (e_4, e_5) выше, чем в методе анализа иерархий. Для учета совместного достижения целей, приводящих к повышению эффективности принятых организационных мер, целесообразно использовать мультипликатор (e_4, e_5), принимающий значение 1, когда принятие организационной меры включает в себя достижение целей №4 и №5, и значение 0, если не включает.

В результате моделирования с использованием искусственной нейронной сети с мультипликатором получим следующую модель для оценки эффективности организационных мер обеспечения информационной безопасности:

$$E_M = 10 \times (0{,}479 \times e_1 + 0{,}246 \times e_2 + 0{,}128 \times e_3 + 0{,}046 \times e_4 - 0{,}113 \times e_5 + 0{,}214 \times e_{4,5}) \quad (3)$$

Данную модель целесообразно использовать для оценки эффективности принятых организационных мер, т.к. в ходе верификации получены непротиворечивые результаты. Вместе с тем, в модели присутствует отрицательный весовой коэффициент. Использование данной модели будет означать, что достижение цели e_5 приводит к снижению эффективности реализации мер. Руководителю подразделения по обеспечению информационной безопасности для принятия управленческих решений и разработке методических документов будет более объективна и понятна модель, сформированная на основе экспертного опроса. Для внесения изменений в модель (1) необходимо определить корректирующий коэффициент.

Для расчета корректирующего коэффициента необходимо в обученной искусственной нейронной сети предположить значение эффективности организационных мер, реализация которых достигает целей e_4 и e_5. Рассмотрим численный метод вычисления корректирующего коэффициента.

$$K = \frac{\frac{z_{4ИНС}}{z_{4МАИ}} + \frac{z_{5ИНС}}{z_{5МАИ}}}{2}, \quad (4)$$

где $z_{4ИНС}$ – эффективность меры, реализация которой обеспечивает достижение цели e_4, вычисленное с использованием искусственной нейронной сети; $z_{4МАИ}$ – эффективность меры, реализация которой обеспечивает достижение цели e_4, вычисленное с использованием модели, сформированной на основе метода анализа иерархий.

В нашем случае корректирующий коэффициент примет следующий вид:

$$K = \frac{\frac{2{,}18}{0{,}79} + \frac{1{,}71}{0{,}53}}{2} \quad (5)$$

Корректирующий коэффициент К=2,99. Следовательно, необходимо скорректировать модель, полученную с использованием метода анализа иерархий, в случае, когда реализация организационной меры приводит к достижению целей e_4 и e_5. Таким образом, модель (1) в случае совместного достижения целей e_4 и e_5 примет вид:

$$E_M = 10 \times (0{,}474 \times e_1 + 0{,}237 \times e_2 + 0{,}158 \times e_3 + 0{,}236 \times e_4 + 0{,}159 \times e_5) \quad (6)$$

Целесообразно верифицировать данную модель на примерах из таблицы 1, которые сильно отличались от результатов опроса. Повторная верификация представлена в таблице 3.

Таблица 3
Table 3

Сравнение результатов оценки эффективности мер
Comparison of the results of assessing the effectiveness of measures

№ п/п	Организационная мера	Достигнутые цели	Эффективность (модель)	Эффективность (опрос)	Эффективность (модель с коэффициентом)
1.	Проведение информирования с пользователями	e_4, e_5	1,32	3	3,95
2.	Проведение практических занятий по порядку эксплуатации АССН, с акцентом на информацию о ВП и ответственности за нарушение требований по ИБ	e_2, e_4, e_5	3,69	6	6,32
3.	Проведение занятий по порядку действий при обнаружении признаков реализации функций ВП и учет работы пользователей в АССН	e_3, e_4, e_5	2,9	5,25	5,53

Исходя из результатов повторной верификации, мы видим, что численный метод с корректирующим коэффициентом позволяет более точно оценить эффективность применения организационных мер.

Заключение

Для оценки эффективности принятых организационных мер для обеспечения информационной безопасности автоматизированных систем специального назначения предложено разработать модель на основе метода анализа иерархий и искусственных нейронных сетей. В ходе моделирования были решены следующие задачи:

1. Определены цели реализации организационных мер по подготовке пользователей АССН для обеспечения информационной безопасности (5 целей).

2. Определен перечень организационных мер по подготовке пользователей АССН для обеспечения информационной безопасности (14 мер).

3. Разработана модель оценки эффективности принятых организационных мер на основе метода анализа иерархий. Сформирован корректирующий коэффициент для мер, реализация которых обеспечивает совместное достижение целей e4 и e5.

4. Выполнена верификация полученных моделей.

Предложенный в работе подход к моделированию оценки опасности эффективности принятых мер целесообразно использовать и для других мер по обеспечению информационной безопасности. Прогнозирование эффективности принятых организационных мер позволит должностному лицу, ответственному за обеспечение информационной безопасности, принимать корректные управленческие решения при появлении неизвестной вредоносной программы, в зависимости от ее опасности.

Список литературы

Горячев С.Н., Кобяков Н.С. 2022. Анализ деструктивных функций и процессов реализации угроз вредоносных программ на ИС органов внутренних дел. Защита информации. Инсайд. 2(104): 42-45. EDN FOWCTU.

Жилин Р.А. 2022. Модели и численные методы оценки эффективности функционирования систем безопасности объектов органов внутренних дел: специальность 01.01.00 "Математика": диссертация на соискание ученой степени кандидата технических наук. Воронеж, 146 с. EDN BSEFXL.

Жиляков Е.Г., Лубков И.И., Болгова Е.В. 2022. Анализ и аппроксимация функций по эмпирическим данным на основе субполосных представлений. Экономика. Информатика. 49(4): 833-853. DOI 10.52575/2687-0932-2022-49-4-833-853. EDN FAVCQO

Жиляков Е.Г., Черноморец А.А., Заливин А.Н., Болгова Е.В. 2021. Субполосные представления в задачах обработки эмпирических данных. Дифференциальные уравнения, математическое моделирование и вычислительные алгоритмы: Сборник материалов международной конференции, Белгород, 25–29 октября 2021 года. Белгород: Белгородский государственный национальный исследовательский университет, С. 111-113. EDN QUGWTW.

Кобяков Н.С. 2023. Оценка опасности вредоносных программ классов "Троянские программы". Альманах Пермского военного института войск национальной гвардии. 2(10): 31-38. EDN OYZHVV.

Мельников А.В., Кобяков Н.С., Жилин Р.А. 2023. Модели и алгоритмы реализации организационных мер защиты информации в АССН от деструктивных воздействий ранее неизвестных вредоносных программ. Вестник Воронежского института МВД России. № 3: 80-87. EDN ZILKNA.

Мельников А.В., Сумин В.И., Кобяков Н.С. 2023. Модель оценки опасности вредоносных утилит. Промышленные АСУ и контроллеры. № 7: 33-40. DOI 10.25791/asu.7.2023.1448. EDN KBALDV.

Мельников А.В., Кобяков Н.С. 2023. Подход к оценке опасности деструктивных воздействий вредоносных программ на автоматизированные системы специального назначения. Безопасность информационных технологий. 30(3): 51-60. DOI 10.26583/bit.2023.3.03. EDN RJWWZH.

Наталичев Р.В., Горбатов В.С., Гавдан Г.П., Дураковский А.П. 2021. Эволюция и парадоксы нормативной базы обеспечения безопасности объектов критической информационной инфраструктуры. Безопасность информационных технологий. 28(3): 6-27. DOI 10.26583/bit.2021.3.01. EDN JIMDXU.

Кобяков Н.С., Мельников А.В., Поляков К.А., Плюхин А.Ю. 2023. Свидетельство о государственной регистрации программы для ЭВМ № 2023662134 Российская Федерация. «Расчет опасности вредоносных программ»: № 2023660462: заявл. 23.05.2023: опубл. 06.06.2023. EDN CBJXFU.

Середкин С.П. 2022. Особенности кибератак на объекты критической информационной инфраструктуры в современных условиях. Информационные технологии и математическое моделирование в управлении сложными системами. 4(16): 56-66. DOI 10.26731/2658-3704.2022.4(16).56-66. – EDN YTMDFF.

Сумин В.И. 2023. Оптимизация функционирования информационных систем специального назначения. Информационные процессы, системы и технологии. Т. 4, № 1(25): 16-21. DOI 10.52529/27821617_2023_4_1_16. – EDN ATIRON.

Сумин В.И., Громов Ю.Ю., Тютюнник В.М. 2023. Оптимизация функционирования информационных систем специального назначения. Научно-техническая информация. Серия 2: Информационные процессы и системы. № 5: 1-6. DOI 10.36535/0548-0027-2023-05-1. EDN TXKJUV.

Сумин В.И., Мельников А.В., Анциферова В.И., Сазонова С.А. 2023. Разработка логико-математических моделей принятия управленческих решений в сложных организационных системах специального назначения. Моделирование систем и процессов. 16(1): 26-34. DOI 10.12737/2219-0767-2023-16-1-26-34. EDN NGLTFU.

Язов Ю.К., Соловьев С.В. 2018. Организация защиты информации в информационных системах от несанкционированного доступа. Монография. Воронеж: Кварта, 588 с.

Sumin V.I., Zybin D G., Golovkin R.B. et al. 2021. Research of the process of functioning of hierarchical multi-level complex organizational systems. Journal of Physics: Conference Series: Current Problems, Voronezh, 07–09 декабря 2020 года. Voronezh, P. 012089. DOI 10.1088/1742-6596/1902/1/012089. EDN UYTLMY.

References

Goryachev S.N., Kobyakov N.S. 2022. Analiz destruktivnykh funktsiy i protsessov realizatsii ugroz vredonosnykh programm na IS organov vnutrennikh del [Analysis of destructive functions and processes of implementation of malware threats on the information systems of internal affairs bodies]. 2(104): 42-45. (in Russian).

Zhilin R.A. 2022. Modeli i chislennye metody otsenki effektivnosti funktsionirovaniya sistem bezopasnosti ob"ektov organov vnutrennikh del: spetsial'nost' 01.01.00 "Matematika": dissertatsiya na soiskanie uchenoy stepeni kandidata tekhnicheskikh nauk. Voronezh, 146 p. (in Russian).

Zhilyakov E.G., Lubkov I.I., Bolgova E.V. 2022. Analysis and Approximation of Functions from Empirical Data Based on Subband Representations. Economics. Information technologies. 49(4): 833–853. DOI 10.52575/2687-0932-2022-49-4-833-853.

Zhilyakov E.G., Chernomorets A.A., Zalivin A.N., Bolgova E.V. 2021. Subpolosnye predstavlenija v zadachah obrabotki jempiricheskih dannyh [Subband representations in empirical data processing problems]. Differencial'nye uravnenija, matematicheskoe modelirovanie i vychislitel'nye algoritmy: Sbornik materialov mezhdunarodnoj konferencii, Belgorod, 25–29 oktjabrja 2021 goda. Belgorod: Belgorodskij gosudarstvennyj nacional'nyj issledovatel'skij universi-tet, p. 111-113 (in Russian).

Kobyakov N.S 2023. Otsenka opasnosti vredonosnykh programm klassov "Troyanskie programmy" [Assessing the danger of malware classes Trojan programs] Al'manakh Permskogo voennogo instituta voysk natsional'noy gvardii. 2(10): 31-38. (in Russian)

Melnikov A.V., Kobyakov N.S., Zhilin R.A. 2023. Models and algorithms for implementing organizational measures to protect information in ASSN from the destructive effects of previously unknown malicious programs. Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. No. 3: 80-87.

Melnikov A.V., Sumin V.I., Kobyakov N.S. 2023. Model for assessing the danger of malicious utilities. Industrial automated control systems and controllers. No. 7: 33-40. DOI 10.25791/asu.7.2023.1448.

Melnikov A.V., Kobyakov N.S. Approach to assessing the danger of destructive effects of malicious programs on automated systems for special purposes. Security of information technologies. 2023. 30(3): 51-60. DOI 10.26583/bit.2023.3.03.

Natalichev R.V., Gorbatov V.S., Gavdan G.P., Durakovsky A.P. 2021. Evolution and paradoxes of the regulatory framework for ensuring the safety of critical information infrastructure objects. Security of information technologies. 28(3): 6-27. DOI 10.26583/bit.2021.3.01.

Kobyakov N.S., Mel'nikov A.V., Polyakov K.A., Plyukhin A.Yu. 2023. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM № 2023662134 Rossiyskaya Federatsiya. «Raschet opasnosti vredonosnykh programm»: № 2023660462: zayavl. 23.05.2023: opubl. 06.06.2023 (in Russian).

Seredkin S.P. 2022. Features of cyber attacks on objects of critical information infrastructure in modern conditions. Information technologies and mathematical modeling in the management of complex systems. 4(16): 56-66. DOI 10.26731/2658-3704.2022.4(16).56-66.

Sumin V.I. 2023. Optimization of the functioning of special-purpose information systems. Information processes, systems and technologies. T. 4, No. 1(25): 16-21. DOI 10.52529/27821617_2023_4_1_16. EDN ATIRON.

Sumin V.I., Gromov Yu.Yu., Tyutyunnik V.M. Optimizatsiya funktsionirovaniya informatsionnykh sistem spetsial'nogo naznacheniya [Optimization of the functioning of special-purpose information systems]. Nauchno-tekhnicheskaya informatsiya. Seriya 2: Informatsionnye protsessy i sistemy. 2023. № 5: 1-6. DOI 10.36535/0548-0027-2023-05-1 (in Russian).

Sumin V.I., Melnikov A.V., Antsiferova V I., Sazonova S.A. 2023. Development of logical and mathematical models for making management decisions in complex organizational systems for special purposes Modeling of systems and processes. 16(1): 26-34. DOI 10.12737/2219-0767-2023-16-1-26-34. EDN NGLTFU.

Yazov Yu.K., Soloviev S.V. 2018. Organizatsiya zashchity informatsii v informatsionnykh sistemakh ot nesanktsionirovannogo dostupa [Organization of information protection in information systems from unauthorized access]. Monografiya. Voronezh: Kvarta, 588 p. ISBN 978-5-93737-158-4 (in Russian).

Sumin V.I., Zybin D G., Golovkin R.B. et al. 2021. Research of the process of functioning of hierarchical multi-level complex organizational systems. Journal of Physics: Conference Series: Current Problems, Voronezh, 07–09 декабря 2020 года. Voronezh, P. 012089. DOI 10.1088/1742-6596/1902/1/012089. EDN UYTLMY.

Конфликт интересов: о потенциальном конфликте интересов не сообщалось.
Conflict of interest: no potential conflict of interest related to this article was reported.

Поступила в редакцию 06.11.2023
Поступила после рецензирования 26.11.2023
Принята к публикации 01.12.2023

Received November 06, 2023
Revised November 26, 2023
Accepted December 01, 2023

ИНФОРМАЦИЯ ОБ АВТОРАХ

Мельников Александр Владимирович, доктор технических наук, доцент, профессор кафедры автоматизированных информационных систем органов внутренних дел, Воронежский институт МВД России, г. Воронеж, Россия

Сумин Виктор Иванович, доктор технических наук, профессор, профессор кафедры информационной безопасности телекоммуникационных систем, Воронежский институт ФСИН России, г. Воронеж, Россия

Кобяков Николай Сергеевич, адъюнкт кафедры автоматизированных информационных систем органов внутренних дел, Воронежский институт МВД России, г. Воронеж, Россия

INFORMATION ABOUT THE AUTHORS

Alexander V. Melnikov, Doctor of Technical Sciences, Associate Professor, Professor of the Department of Automated Information Systems of Internal Affairs Bodies, Voronezh Institute of the Ministry of Internal Affairs of Russia, Voronezh, Russia

Victor I. Sumin, Doctor of Technical Sciences, Professor, Professor of the Department of Information Security of Telecommunication Systems, Voronezh Institute of the Federal Penitentiary Service of Russia, Voronezh, Russia

Nikolay S. Kobyakov, adjunct of the Department of Automated Information Systems of Internal Affairs Bodies, Voronezh Institute of the Ministry of Internal Affairs of Russia, Voronezh, Russia