«Информатика»

Научная статья
УДК 004.942
DOI: 10.17072/1993-0550-2023-4-89-95

Разработка модели для оценки опасности деструктивных воздействий вредоносных утилит на автоматизированные системы специального назначения с использованием регрессионного анализа

Николай Сергеевич Кобяков
Пермский военный институт войск национальной гвардии Российской Федерации, Пермь, Россия
kkobyakov1234@gmail.com

Аннотация. В работе рассматривается вопрос использования регрессионного анализа для разработки модели оценки опасности вредоносных утилит на автоматизированные системы. Исходными данными для моделирования являются результаты опроса высококвалифицированных специалистов в области обеспечения информационной безопасности. Для моделирования использовался пакет прикладных программ Excel и STATISTICA. Результаты моделирования верифицированы на тестовом наборе данных. Сформированная модель может быть использована специалистами, обеспечивающими информационную безопасность при обработке информации в автоматизированных системах специального назначения, от деструктивного воздействия ранее неизвестных вредоносных утилит.

Ключевые слова: *регрессионный анализ; вредоносные утилиты; автоматизированные системы*

Для цитирования: *Кобяков Н. С.* Разработка модели для оценки опасности деструктивных воздействий вредоносных утилит на автоматизированные системы специального назначения с использованием регрессионного анализа // Вестник Пермского университета. Математика. Механика. Информатика. 2023. Вып. 4(63). С. 89–95. DOI: 10.17072/1993-0550-2023-4-89-95.

Статья поступила в редакцию 10.10.2023; одобрена после рецензирования 26.10.2023; принята к публикации 27.11.2023.

«Computer Science»

Research article

Model Development for Assessing the Danger of Malicious Utilities' Destructive Effects on Automated Special-Purpose Systems Using Regression Analysis

Nikolay S. Kobyakov
Perm military Institute of National Guard Troops, Perm, Russia
kkobyakov1234@gmail.com

Abstract The paper examines the issue of using regression analysis to develop a model for assessing the danger of malicious utilities on automated systems. The initial data for modeling are the results of a survey of highly qualified specialists in the field of information security. The application package Excel and STATISTICA were used for modeling. The modeling results were verified on a test data set. The generated model can be used by specialists who ensure information security when processing information in automated systems for special purposes, from the destructive effects of previously unknown malicious utilities.

Keywords: *regression analysis; malicious utilities; automated systems*

For citation: *Kobyakov N. S.* Model Development for Assessing the Danger of Malicious Utilities' Destructive Effects on Automated Special-Purpose Systems Using Regression Analysis. Bulletin of Perm University. Mathematics. Mechanics. Computer Science. 2023;4(63):89-95. (In Russ.). DOI: 10.17072/1993-0550-2023-4-89-95.

The article was submitted 10.10.2023; approved after reviewing 26.10.2023; accepted for publication 27.11.2023.

Введение

Обеспечение информационной безопасности в условиях постоянно совершенствующихся методов реализации атак на автоматизированные системы специального назначения становится все более актуальным вопросом. Согласно методического документа [1] актуальными угрозами для систем и сетей являются:

1) использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей);

2) внедрение вредоносного программного обеспечения;

3) использование недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств;

4) установка программных и (или) программно-аппаратных закладок в программное обеспечение и (или) программно-аппаратные средства;

5) формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных;

6) перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей) для доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;

7) инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;

8) нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию);

9) ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств.

В рамках данной работы рассмотрим угрозу внедрения вредоносного программного обеспечения, а именно вредоносных утилит [2].

Исследованию защищенности автоматизированных систем специального назначения посвящено множество работ [3–5], но в данных работах не приводятся модели для численных оценок опасности вредоносных программ.

Цель исследования. Разработать модель для оценки опасности деструктивных воздействий вредоносных утилит на автоматизированные системы.

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

1. Определить исходные данные для моделирования (поведенческие паттерны вредоносных утилит, вид регрессии).

2. Провести опрос специалистов в области информационной безопасности (в результате получить сведения об опасности вредоносных утилит на основе их поведенческих паттернов).

3. С использованием прикладных программ сформировать модель для оценки опасности вредоносных утилит.

4. Выполнить верификацию полученной модели на тестовом наборе данных.

1. Модели и алгоритмы реализации организационных мер защиты информации в АССН от деструктивных воздействий ранее неизвестных вредоносных программ

В работе [6] описан процесс разработки информационно-логической модели комплексной системы защиты информации от ранее неизвестных вредоносных программ. В ходе моделирования определены группы должностных лиц, участвующие в процессе обеспечения информационной безопасности:

1. Руководители подразделений, обеспечивающих информационную безопасность автоматизированных систем специального назначения.

2. Специалисты, обеспечивающие информационную безопасность автоматизированных систем специального назначения.

3. Пользователи автоматизированных систем специального назначения.

Для каждой группы должностных лиц определены на основе модели Захмана [7] реализуемые мероприятия при появлении ранее неизвестных вредоносных программ, ответственные должностные лица, временные рамки и результат выполнения действий.

Поскольку реализуемые мероприятия зависят от опасности вредоносной программы ([0–3.99] – низкая, [4.0–6.99] – средняя, [7.0–8.99] – высокая, [9.0–10.0] – критическая), для обеспечения корректного функционирования комплексной системы защиты информации необходимо разработать модель для оценки опасности деструктивных воздействий.

2. Регрессионный анализ

Использование регрессионного анализа направлено на решение следующих задач [8]:

1. Предсказание значения зависимой переменной с помощью независимых переменных.

2. Определение вклада отдельных независимых переменных в вариацию зависимой переменной.

В зависимости от взаимосвязи между величинами регрессия может быть линейной или нелинейной.

Существуют следующие основные виды регрессий:

1. Парная регрессия, предназначенная для описания наиболее вероятных значений одной переменной, исходя из значений другой.

2. Множественная регрессия, которая является расширением парной регрессии. При построении моделей множественной регрессии оценивается степень влияния нескольких признаков на исследуемый параметр.

Также возможно разделение регрессионных моделей, исходя из типов исходных данных:

1. Пространственная выборка (значения показателей относятся к одному моменту времени).

2. Временная выборка (значения одного показателя, относящиеся к различным моментам времени).

Процесс формирования математической модели включает в себя последовательную реализацию следующих этапов [8]:

1. Этап спецификации – качественное изучение моделируемого процесса (объекта, явления).

2. Информационный этап – сбор информации.

3. Идентификация модели – выполнение статистического анализа модели и оценка неопределенных параметров.

4. Верификация – проверка истинности модели (ее адекватности).

3. Этап спецификации

Согласно ранее проведенных исследований [2], актуальными для АССН являются следующие классы вредоносных программ:

1. Вредоносные утилиты.

2. Троянские программы.

3. Вирусы и черви.

Возможность создания модели оценки опасности деструктивных воздействий вредоносных программ на автоматизированные системы специального назначения рассмотрим на примере вредоносных утилит.

Вредоносные утилиты реализуют поведенческие паттерны, представленные в табл. 1:

Таблица 1. *Поведенческие паттерны вредоносных утилит*

Наименование поведенческого паттерна	Обозначение
Проникновение на компьютер-жертву	p_1
Скрытие следов присутствия преступников в системе	p_2
Внесение в список разрешенных посетителей системы новых пользователей	p_3
Прекращение работы системы	p_4
Проведение атак типа "Отказ в обслуживании"	p_5
Сбор и анализ сетевых пакетов	p_6
Подмена адреса отправителя письма по электронной почте	p_7
Создание вредоносных программ	p_8
Навязывание ложной информации (уведомление об опасности, нарушениях)	p_9
Модификация вредоносных программ	p_{10}
Распространение флуда (бесполезных сообщений по каналам электронной почты)	p_{11}

Согласно [1] при оценке угроз необходимо определить негативные последствия их реализации.

В случае, если в отношении автоматизированной системе специального назначения будет реализована угроза внедрения вредоносного программного обеспечения, могут быть следующие негативные последствия:

1. Нарушение конфиденциальности информации, обрабатываемой в автоматизированной системе.

2. Нарушение доступности отдельных элементов или в целом автоматизированной системы.

3. Нарушение целостности, обрабатываемой в автоматизированной системе.

Кроме того, реализация угрозы на большое количество элементов системы может повлечь за собой нарушение функционирования отдельных подразделений и, как следствие, несвоевременное выполнение задач.

Исходя из определенных параметров модели для оценки опасности деструктивных воздействий вредоносных утилит на АССН целесообразно использовать множественную линейную регрессию. Общий вид модели, сформированной на основе множественной линейной регрессии имеет вид:

$$Y = a + b_1 * p_1 + b_2 * p_2 + \ldots + b_n * p_n \ , \quad (1)$$

где:

Y – значение исследуемой величины;

a – коэффициент множественной линейной регрессии;

$b_{1,\ldots n}$ – коэффициенты чистой регрессии;

$p_{1,\ldots,n}$ – поведенческие паттерны вредоносных утилит.

4. Информационный этап

Для построения модели оценки опасности деструктивных воздействий вредоносных утилит на автоматизированные системы специального назначения среди специалистов в области обеспечения информационной безопасности был проведен опрос. В ходе опроса специалистам было предложено оценить опасности вредоносных утилит, исходя из реализуемых ими поведенческих паттернов (p).

Результаты опроса обобщены и представлены в табл. 2.

Таблица 2. *Результаты опроса*

№ п/п	Реализуемые поведенческие паттерны	Опасность
1.	p1, p2, p5	10
2.	p2, p8, p10	4,4
3.	p7, p11	1,78
4.	p5, p6	2,98
5.	p8, p10	0,89
6.	p4,p5,p6	5,33
7.	p7, p11	1,78
8.	p4,p5	3,84
9.	p4,p9	2,87
10.	p4,p6	3,84
11.	p3, p9	2,87
12.	p3, p6	3,84
13.	p6	1,49
14.	p2	3,5
15.	p6, p11	1,78
16.	p5 p9	2,02
17.	p3, p8	2,87
18.	p7 p10	1,86
19.	p3 p7	3,84
20.	p1, p11	5,3
21.	p1, p4, p6, p9	9,36
22.	p2, p11	3,8
23.	p3, p10	2,71
24.	p4, p9	2,87
25.	p6,p7	2,98

5. Идентификация модели

В ходе моделирования необходимо выявить зависимость между переменной J (характеризующую опасность вредоносной утилиты) и $p_{1,..,11}$ (поведенческими паттернами вредоносных утилит). Для идентификации модели воспользуемся пакетами прикладных программ Excel и STATISTICA.

Внесем полученные в табл. 2 значения опасности и реализуемые поведенческие паттерны в редактор Excel. Для этого в столбец J внесем значение опасности, оцененное экспертами, а в соответствующих столбцах $p_{1,\ldots,11}$ значение "0", если паттерн не реализован в вредоносной утилите и "1", если реализован.

Пример заполнения сведений об опасности вредоносных утилит представлен на рис. 1.

	J	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10	p11
1	10	1	1	0	0	1	0	0	0	0	0	0
2	4,4	0	1	0	0	0	0	0	1	0	1	0
3	1,78	0	0	0	0	0	0	1	0	0	0	1
4	2,98	0	0	0	0	1	1	0	0	0	0	0
5	0,89	0	0	0	0	0	0	0	1	0	1	0
6	5,33	0	0	0	1	1	1	0	0	0	0	0
7	1,78	0	0	0	0	0	0	1	0	0	0	1
8	3,84	0	0	0	1	1	0	0	0	0	0	0

Рис. 1. *Заполнение сведений о вредоносных утилитах*

Используя опцию регрессия функции анализа данных, получим значения коэффициентов, представленных на рис. 2.

	Коэффициенты
Y-пересечение	0,20834616
Переменная X 1	5,066050423
Переменная X 2	3,355314361
Переменная X 3	2,196232151
Переменная X 4	2,246651596
Переменная X 5	1,39056984
Переменная X 6	1,416477567
Переменная X 7	1,390236255
Переменная X 8	0,470499356
Переменная X 9	0,427796886
Переменная X 10	0,28595847
Переменная X 11	0,116139912

Рис. 2. *Коэффициенты регрессионной модели*

На основе полученных коэффициентов составим модель множественной регрессии (1):

$$Y = 0{,}21 + 5{,}07 * p_1 + 3{,}36 * p_2 + 2{,}2 * p_3 + 2{,}25 * p_4 + 1{,}39 * p_5 + 1{,}42 * p_6 + 1{,}39 * p_7 + 0{,}47 * p_8 + 0{,}43 * p_9 + 0{,}29 * p_{10} + 0{,}12 * p_{11} \quad . \quad (2)$$

6. Верификация модели

С точки зрения регрессионного анализа адекватность модели может быть подтверждена данными, представленными на рис. 3.

Регрессионная статистика	
Множественный R	0,999432309
R-квадрат	0,998864941
Нормированный R-	0,997904506
Стандартная ошибк	0,098815022
Наблюдения	25

Рис. 3. *Регрессионная статистика*

Проверка возможности применения сформированной модели для оценки опасности ранее неизвестных вредоносных утилит выполнена на 10 примерах. Тестовый набор данных является репрезентативным, так как включает в себя примеры с различными комбинациями поведенческих паттернов.

Результаты верификации модели представлены в табл. 3.

Таблица 3. *Результаты верификации*

№ п/п	Реализуемые поведенческие паттерны	Вычисленная опасность	Уровень опасности
1.	p_1, p_2, p_8, p_{10}	9,4	Критический
2.	p_1, p_2	8,64	Высокий
3.	p_4, p_5, p_{10}	4,17	Средний
4.	p_1, p_6	6,7	Средний
5.	p_3, p_7, p_{11}	3,92	Низкий
6.	p_1	5,28	Средний
7.	p_3, p_{11}	2,53	Низкий
8.	p_6, p_9	2,06	Низкий
9.	p_7, p_9	2,03	Низкий
10.	p_9, p_{11}	0,76	Низкий

Верификация модели на тестовом наборе данных подтверждает целесообразность оценки опасности вредоносных утилит, основываясь на поведенческих паттернах. Вычисленные значения и уровни опасности вредоносных утилит логичны, поскольку соответствуют нанесенному автоматизированной системе ущербу.

Заключение

В данной статье рассмотрен вопрос разработки модели для оценки опасности деструктивных воздействий вредоносных утилит на автоматизированные системы специального назначения. В ходе моделирования с использованием пакета прикладных программ Excel и STATISTICA получены коэффициенты для каждого поведенческого паттерна.

Разработанная модель может быть использована специалистами в области обеспечения информационной безопасности для реализации превентивных мер защиты от деструктивных воздействий ранее неизвестных вредоносных утилит.

Список источников

1. *Методический* документ Методика оценки угроз безопасности информации Утвержден ФСТЭК России 5 февраля 2021 г.
2. *Мельников, А.В.* Подход к оценке опасности деструктивных воздействий вредоносных программ на автоматизированные системы специального назначения / А.В. Мельников, Н.С. Кобяков // Безопасность информационных технологий. 2023. Т. 30, № 3. С. 51–60. DOI 10.26583/bit.2023.3.03. EDN RJWWZH.
3. *Gromov Y.* Building an external classifier of negative impacts in assessing survivability and ensuring the security of information systems Minin Y., Eliseev A., Alrammahi A.A.H., Sari F.A. // В сб.: Proceedings – 2020 2nd International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency, SUMMA 2020. 2. 2020. С. 636–641.
4. *Сумин В.И.* Анализ функционирования и структурная декомпозиция информационных систем специального назначения / Сумин В.И., Смоленцева Т.Е., Громов Ю.Ю., Тютюнник В.М. // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2021. № 8. С. 5–14.
5. *Горячев С.Н.* Анализ деструктивных функций и процессов реализации угроз вредоносных программ на ИС органов внутренних дел / С.Н. Горячев, Н.С. Кобяков // Защита информации. Инсайд. 2022. № 2(104). С. 42–45. EDN FOWCTU.
6. *Мельников А.В.* Модели и алгоритмы реализации организационных мер защиты информации в АССН от деструктивных воздействий ранее неизвестных вредоносных программ / А.В. Мельников, Н.С. Кобяков, Р.А. Жилин // Вестник Воронежского института МВД России. 2023. № 3. С. 80–87. EDN ZILKNA.
7. *Zachman J.A.* "A framework for information systems architecture," in IBM Systems Journal. Vol. 26, no. 3, pp. 276–292, 1987, doi: 10.1147/sj.263.0276.
8. *Данилова О.Ю.* Правовая статистика: методы и модели / О.Ю. Данилова, В.В. Меньших, С.В. Синегубов. Воронеж: Воронежский институт Министерства внутренних дел Российской Федерации, 2018. 302 с. ISBN 978-5-88591-666-0. EDN YOZXWX.

References

1. *Methodological* document Methodology for assessing threats to information security Approved by the FSTEC of Russia on February 5. 2021. (In Russ.).
2. *Melnikov A.V., Kobyakov N.S.* Approach to assessing the danger of destructive effects of malware on special-purpose automated systems. IT Security (Russia), [S.l.]. 2023;(30(3):51–60. DOI 10.26583/bit.2023.3.03. EDN RJWWZH. (In Russ.).
3. *Gromov Y., Minin Y., Eliseev A., Alrammahi A.A.H., 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. Proceedings – 2020. 2020;2:636-641.
4. *Sumin V.I., Smolentseva T.E., Gromov Yu.Yu., Tyutyunnik V.M.* Analysis of the functioning and structural decomposition of special-purpose information systems. Scientific and technical information. Series 2: Information processes and systems. 2021;8:5-14.
5. *Goryachev S.N., Kobyakov N.S.* Analysis of destructive functions and processes of implementation of threats of malicious programs on the IS of internal affairs bodies. Information Protection. Insider. 2022;(2(104)):42-45. EDN FOWCTU. (In Russ.).
6. *Melnikov A.V., Kobyakov N.S., Zhilin R.A.* Models and algorithms for the implementation of organizational measures to protect information in ASSN from the destructive effects of previously unknown malware. Vestnik Voronezh Institute of the Ministry of Internal Affairs of Russia. 2023;(3):80-87. EDN ZILKNA. (In Russ.).
7. *Zachman J. A.* "A framework for information sys-tems architecture," in IBM Systems Journal. Vol. 26, no. 3, pp. 276-292, 1987, doi: 10.1147/sj.263.0276. (In Russ.).
8. *Danilova O.Yu., Menshikh V.V., Sinegubov S.V.* Legal statistics: methods and models. Voronezh: Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation; 2018. 302 p. ISBN 978-5-88591-666-0. EDN YOZXWX. (In Russ.).

Информация об авторе:

Н. С. Кобяков – начальник учебной лаборатории технической защиты информации кафедры информационных технологий и защиты информации, Пермский военный институт войск национальной гвардии Российской Федерации (614030, Россия, г. Пермь, ул. Гремячий Лог, д. 1), AuthorID 1126165.

Information about the author:

N. S. Kobyakov – Head of the technical information security educational laboratory of the information technology and information security department, Perm Military Institute of the National Guard of the Russian Federation, (1, Gremyachy Log St., Perm, Russia, 614030), AuthorID 1126165.