МЕТОДИКА ОЦЕНКИ ОПАСНОСТИ ДЕСТРУКТИВНЫХ ПРОГРАММНЫХ ВОЗДЕЙСТВИЙ НА АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Мельников А. В.[1], Кобяков Н. С.[2]

DOI: 10.21681/2311-3456-2025-5-28-40

Цель исследования: *моделирование показателя опасности деструктивных программных воздействий, с учетом актуальности поведенческих паттернов вредоносных программ для автоматизированных систем специального назначения органов внутренних дел.*

Методы исследования: *для формирования моделей оценки опасности деструктивных программных воздействий и определения численных значений признаков АССН ОВД используется метод анализа иерархий.*

Результат исследования: *определены базовые и частные признаки АССН ОВД, характеризующие актуальность поведенческих паттернов вредоносных программ в зависимости от функциональных особенностей АССН ОВД. Разработаны базовые и частные модели оценки опасности деструктивных программных воздействий на АССН ОВД с учетом актуальности поведенческих паттернов вредоносных программ. Разработан алгоритм планирования и реализации процессов жизненного цикла АССН ОВД в условиях деструктивных программных воздействий. Выполнена верификация разработанной методики на примере формирования моделей оценки опасности деструктивного программного воздействия вредоносных программ класса «Вредоносные утилиты» на тестовую автоматизированную систему специального назначения. Верификация разработанных моделей выполнена на тестовом наборе данных, сформированном путем опроса экспертов.*

Практическая значимость: *разработанная методика может быть использована администраторами безопасности автоматизированных систем специального назначения при оценке опасности деструктивных программных воздействий и определении целей и перечня реализуемых мер обеспечения защиты информации при появлении неизвестных вредоносных программ.*

Ключевые слова: *вредоносные программы, признаки автоматизированных систем, защита информации, метод анализа иерархий.*

Введение

В настоящее время цифровизация процессов обработки информации в силовых ведомствах при всех ее преимуществах приводит к повышению активности злоумышленников по нанесению ущерба информации, которая хранится и обрабатывается в автоматизированных системах специального назначения органов внутренних дел (АССН ОВД). АССН ОВД – это система, состоящая из комплекса средств автоматизации оперативно-служебной и (или) повседневной деятельности, реализующая информационную технологию выполнения установленных функций, а также сотрудников органов внутренних дел, обеспечивающих её функционирование, с учетом требований по защите информации.

Одним из важных критериев, который необходимо учесть при формировании моделей оценки опасности деструктивных программных воздействий (ООДПВ) на АССН ОВД (J), это их функциональные особенности (признаки) (H,F), например, как это учтено в методическом документе ФСТЭК России[3]. В зависимости от признаков АССН ОВД можно определить актуальные поведенческие паттерны вредоносных программ (p), для реализации деструктивного программного воздействия. Под поведенческими паттернами вредоносных программ понимаются деструктивные функции, реализуемые вредоносной программой. В рамках работы будут рассмотрены базовые признаки АССН ОВД, характеризующие

1 Мельников Александр Владимирович, доктор технических наук, доцент, профессор кафедры автоматизированных информационных систем органов внутренних дел Воронежского института Министерства внутренних дел Российской Федерации, г. Воронеж, Россия. ORCID: https://orcid.org/0000-0001-5080-1162. E-mail: meln78@mail.ru

2 Кобяков Николай Сергеевич, адъюнкт кафедры автоматизированных информационных систем органов внутренних дел Воронежского института Министерства внутренних дел Российской Федерации, г. Воронеж, Россия. ORCID: https://orcid.org/0000-0002-4950-7879. E-mail: kkobyakov1234@gmail.com

3 Методический документ «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств». Утвержден ФСТЭК России 28 октября 2022 г.

классы защищенности автоматизированных систем (подключение к сервису электронной почты и др.) и частные признаки, характеризующие конкретную автоматизированную систему (тип используемой операционной системы и др.).

Авторы в работах [1, 2] отмечают необходимость постоянного совершенствования системы защиты информации автоматизированных систем, в том числе от новых угроз. В работе [3] описаны следующие подходы к формированию требований в области информационной безопасности:

1. Экспертный анализ угроз безопасности информации, их идентификация, с последующей обработкой рисков и их снижения до приемлемого уровня.
2. Распространение на систему действия некоторого набора нормативных документов, в которых требования по информационной безопасности заранее определены.

Также, на практике может применяться комбинированный подход. В работах [4–8] представлены результаты исследований по моделированию угроз безопасности информации, но, в них не рассматриваются вопросы оценки опасности деструктивных программных воздействий с учетом признаков автоматизированных систем.

Для реализации достаточных дополнительных мер защиты информации в АССН ОВД необходимо оценить опасность деструктивных программных воздействий вредоносных программ. В рамках данной работы для формирования моделей ООДПВ будут использованы экспертные и многокритериальные методы принятий решений.

Авторы в работе [9] рассматривают современные подходы к моделированию с использованием метода анализа иерархий и делают вывод о том, что применение метода анализа иерархий, в ситуациях, когда исследуемая область характеризуется связанными признаками, может привести к ошибкам при верификации моделей. В работе [10] разработан численный метод модификации моделей, разработанных на основе метода анализа иерархий, с использованием искусственной нейронной сети. Данный численный метод может быть использован для модификации моделей, в которых определены пары связанных признаков, совместная реализация которых, приводит к повышению значения показателя качества. Применение данного метода позволяет учесть связь признаков при формировании моделей ООДПВ с использованием метода анализа иерархий и повысить точность сформированных моделей.

Цель исследования

Моделирование оценки опасности деструктивных программных воздействий на АССН ОВД с учетом их базовых и частных признаков.

Для достижения цели работы необходимо решить следующие задачи:

1. Определить базовые и частные признаки АССН ОВД, характеризующие актуальность поведенческих паттернов вредоносных программ в зависимости от функциональных особенностей АССН ОВД.
2. Выполнить моделирование оценки опасности деструктивных программных воздействий с учетом базовых, частных признаков АССН ОВД.
3. Разработать алгоритм планирования и реализации процессов жизненного цикла АССН ОВД в условиях деструктивных программных воздействий.
4. Выполнить вычислительный эксперимент, по оценке опасности деструктивных программных воздействий на АССН ОВД.

Порядок разработки моделей ООДПВ на АССН ОВД представлен на рисунке 1.

Для формирования моделей оценки опасности деструктивных программных воздействий необходимо использовать следующие исходные данные на каждом этапе, в соответствии с рисунком 1:

1. **Данные о вредоносных программах.** Вредоносные программы реализуют характерные для них поведенческие паттерны. Множество поведенческих паттернов $P = \{p_1, p_2, ..., p_n\}$, n – количество поведенческих паттернов вредоносных программ.

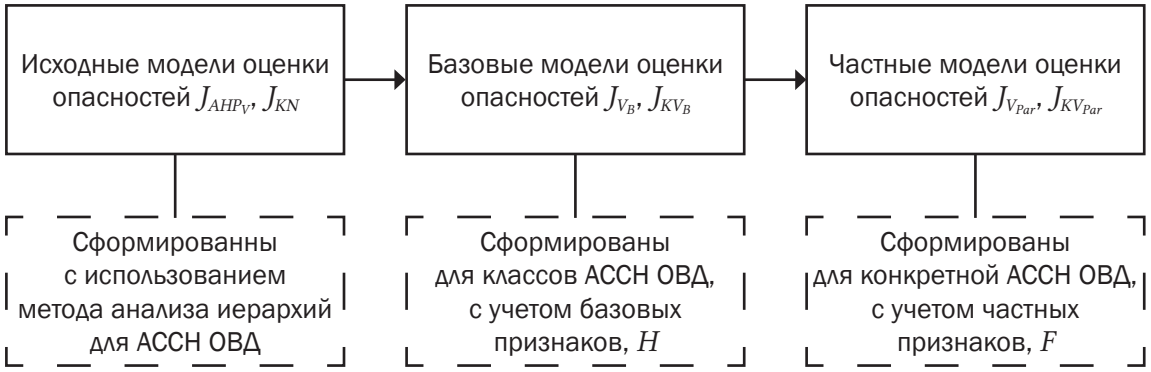

Рис. 1. Порядок разработки моделей оценки опасности деструктивных программных воздействий

Исходными моделями для формирования базовых и частных являются модели оценки опасности деструктивных программных воздействий: без учета связи поведенческих паттернов (J_{AHP_V}), сформированная в результате исследования [11], и с учетом связи поведенческих паттернов (J_{KN}), исследование [10].

2. **Данные об экспертной группе**. Экспертная группа формируется в соответствии с требованиями методического документа ФСТЭК России. Множество экспертов $T = \{t_1, t_2, ..., t_\tau\}$, τ – количество экспертов в экспертной группе.
3. **Данные об АССН ОВД для формирования базовых моделей**. Для формирования базовых моделей (J_{V_B}, J_{KV_B}) экспертной группой будет рассмотрен набор базовых признаков, $H = \{h_1, h_2, ..., h_\beta\}$, где β – количество базовых признаков, от которых зависит актуальность деструктивных программных воздействий вредоносных программ и мультимножество значений данных признаков для тестовой АССН ОВД $H^* = \{h_1^*, h_2^*, ..., h_\beta^*\}$. В результате работы экспертной группы формируется мультимножество значений базовых признаков для класса защищенности АС $\Psi = \{\psi_1, \psi_2, ..., \psi_n\}$.
4. **Данные об АССН ОВД для формирования частных моделей**. Для формирования частных моделей ($J_{V_{Par}}$, $J_{KV_{Par}}$) экспертной группой будет рассмотрен набор частных признаков $F = \{f_1, f_2, ..., f_\varphi\}$, φ – количество частных признаков, от которых зависит актуальность деструктивных программных воздействий вредоносных программ и мультимножество значений данных признаков для тестовой АССН ОВД $F^* = \{f_1^*, f_2^*, ..., f_\varphi^*\}$. В результате работы экспертной группы формируется мультимножество значений частных признаков для конкретной АССН ОВД $\Omega = \{\omega_1, \omega_2, ..., \omega_n\}$.

Допущения и ограничения, принятые в методике:

- на период эксплуатации состав компонентов АС остается неизменным;
- оцениваемые вредоносные программы реализуют поведенческие паттерны, описанные в работе [11]. В случае появления новых поведенческих паттернов необходимо уточнение исходных, базовых и частных моделей;
- в рамках данной работы будут рассмотрены вредоносные программы, используемые при проведении нецелевых компьютерных атак.
- в связи с большим количеством исследуемых поведенческих паттернов вредоносных программ (более 25) в работе будет рассмотрен процесс оценки опасности деструктивных программных воздействий только класса «Вредоносные утилиты».

Методика может быть применена для ситуаций, когда возможна реализация деструктивных функций вредоносных программ, сигнатуры которых не определены средствами антивирусной защиты (САВЗ) АС.

1. Формирование группы экспертов

Для каждой АС необходимо сформировать группу экспертов для оценки процессов, связанных с защитой информации. В соответствии с рекомендациями методического документа ФСТЭК России, формирование моделей оценки опасности деструктивного программного воздействия вредоносных программ на автоматизированные системы должно выполняться экспертной группой. В экспертную группу по результатам исследования [12] для оценки признаков АССН ОВД рекомендуется включить:

1. Должностные лица, ответственные за обеспечение безопасности информации, обрабатываемой в АССН.
2. Должностные лица, ответственные за функционирование ИТ-инфраструктуры АССН.
3. Должностные лица, выполняющее свои должностные обязанности в ходе эксплуатации АССН (хранение, обработка информации).

В рамках работы предлагается включить в экспертную группу будут 8 экспертов ($\tau = 8$). Данный набор экспертов обеспечивает выполнение требований по количеству и порядку подчиненности членов экспертной группы.

2. Формирование базовых моделей оценки опасности деструктивных программных воздействий

В общем виде модель оценки показателя опасности, сформированная с использованием метода анализа иерархий имеет вид:

$$J_{AHP} = \sum_{i=1}^{n} w_{AHP_i} \cdot p_i, \quad (1)$$

где: w_{AHP_i} – весовые коэффициенты поведенческих паттернов вредоносных программ; p_i – поведенческие паттерны вредоносных программ. Данная переменная принимает значение 1, если поведенческий паттерн реализован в вредоносной программе и значение 0, если не реализован; n – количество поведенческих паттернов вредоносных программ.

Далее, необходимо выполнить нормировку весовых коэффициентов поведенческих паттернов и нормализацию модели для приведения значения показателя опасности к лингвистической шкале. Для нормализации модели (1) необходимо разделить на значение самого высокого показателя опасности ($J_{\max}$) и умножить на максимальное значение лингвистической шкалы (A).

Исходная модель, без учета связи поведенческих паттернов, будет иметь вид:

$$J_{AHP_V} = \mathrm{A} \cdot \frac{J^*_{AHP_V}}{J_{\max}} = \frac{\sum_{i=1}^{n} w_i \cdot p_i}{J_{\max}}, \quad (2)$$

где w_i – нормализованные весовые коэффициенты поведенческих паттернов; $J^*_{AHP_V}$ – значение показателя опасности, рассчитанное с использованием классической модели, сформированной на основе метода анализа иерархий; $J_{\max}$ – максимальное значение опасности вредоносной программы (рассчитывается значение $J^*_{AHP_V}$ для существующих вредоносных программ и выбирается максимальное).

Для оценки опасности деструктивных программных воздействий разработана лингвистическая шкала по аналогии со стандартом CVSS v3.1 в диапазоне [0–10]. Следовательно, для формулы (2) значение $A = 10$.

Также в случае, если для исследуемого класса вредоносных программ характерны связанные поведенческие паттерны, то необходимо учесть данный факт в исходной модели. Исходная модель с учетом связи поведенческих паттернов будет иметь вид:

$$J_{KN} = 10 \cdot \frac{J^*_{KN}}{J_{KN_{\max}}} = \frac{\sum_{i=1}^{n} w_i \cdot p_i + \sum_{j=1}^{u} K_j}{J_{KN_{\max}}}, \quad (3)$$

где J^*_{KN} – значение показателя опасности, рассчитанное с использованием не нормализованной модели, с учетом связи поведенческих паттернов; $J_{KN_{\max}}$ – значение опасности самой опасной вредоносной программы; K – коэффициент, характеризующий связь поведенческих паттернов вредоносных программ; u – количество пар связанных поведенческих паттернов вредоносных программ.

Базовые модели формируются на основе исходных и предназначены для ООДПВ вредоносных программ с учетом класса защищенности АС. В работе [13] определена классификация АССН ОВД исходя из требований руководящих документов по классификации информационных и автоматизированных систем. Результаты работы представлены в таблице 1.

2.1. Определение весовых коэффициентов для классов АССН ОВД

Для каждого класса АССН необходимо определить весовой коэффициент, который будет учтен при построении частных моделей. Для этого предлагается выполнить эксперимент с использованием метода анализа иерархий, предложенный Т. Саати. После обобщения результатов опроса получена таблица парных сравнений, представленная в таблице 2.

С использованием программного обеспечения Mathcad получен первый собственный вектор матрицы парных сравнений $v_1 = (3{,}30193; 1{,}71712; 1)$. Выполнение нормировки первого собственного вектора может быть выполнено путем деления значения

Таблица 1.

Классы защиты (уровни доверия) средств защиты информации и соответствующие классы защищенности (КЗ) информационных систем (ИС)

КЗ ФСТЭК	Предназначение	КЗ ИСПДН	КЗ ГИС	КЗ ИС ОП	КЗ АССН ОВД
1, 2, 3	Предназначен для установки в средствах вычислительной техники и автоматизированных системах, обрабатывающих сведения, составляющие государственную тайну	–	–	–	1, 2, 3
4	Предназначен для установки в средствах вычислительной техники и автоматизированных системах, входящих в состав государственных информационных систем, информационных систем общего пользования и информационных систем, обрабатывающих персональные данные.	1	1	2	4
5		2	2	–	5
6		3	3	–	6

Таблица 2.

Парные сравнения классов АССН

	4 класс	5 класс	6 класс
4 класс	1	2	3
5 класс	1/2	1	2
6 класс	1/3	1/2	1

каждого элемента на их сумму [14]. Получим следующие весовые коэффициенты D для классов АССН ОВД:

4 класс АССН – 0,54;
5 класс АССН – 0,3;
6 класс АССН – 0,16.

Для определения итоговых весовых коэффициентов классов АССН ОВД необходимо учесть, что наиболее важная информация хранится и обрабатывается в АССН 4 класса. Следовательно, весовой коэффициент D для него примем за 1, а коэффициенты для остальных классов рассчитаем, используя пропорцию:

4 класс АССН – 1;
5 класс АССН – 0,56;
6 класс АССН – 0,3.

2.2. Формирование базовых моделей оценки опасности деструктивных программных воздействий в общем виде

Базовые модели оценки опасности деструктивных программных воздействий разрабатываются для классов АС на основе исходных моделей и имеет вид:

Без учета связи поведенческих паттернов:

$$J_{V_B} = 10 \cdot \frac{J^*_{V_B}}{J_{B_{\max}}} = \frac{\sum\limits_{i=1}^{n} \psi_i \cdot w_i \cdot p_i}{J_{B_{\max}}}, \quad (4)$$

где J_{V_B} – скорректированное значение показателя опасности для базовой модели без учета связи поведенческих паттернов; ψ – значение весовых коэффициентов базовых признаков актуальности для соответствующих поведенческих паттернов; $J_{B_{\max}}$ – значение опасности самой опасной вредоносной программы для базовой модели без учета связи поведенческих паттернов.

С учетом связи поведенческих паттернов:

$$J_{KV_B} = 10 \cdot \frac{J^*_{KV_B}}{J_{KB_{\max}}} = \frac{\sum\limits_{i=1}^{n} \psi_i \cdot w_i \cdot p_i + \sum\limits_{j=1}^{u} \psi_j \cdot K_j}{J_{KB_{\max}}}, \quad (5)$$

где: $J^*_{KV_B}$ – скорректированное значение показателя опасности для базовой модели с учетом связи поведенческих паттернов; $J_{KB_{\max}}$ – значение опасности самой опасной вредоносной программы для базовой модели с учетом связи поведенческих паттернов.

Для формирования базовых моделей ООДПВ на АС необходимо выделить признаки, которые влияют на актуальность поведенческих паттернов вредоносных программ. Исходя из результатов исследований [15, 16] определены базовые признаки автоматизированных систем. В таблице 3 представлены базовые признаки АС и значения, которые они могут принимать и весовые коэффициенты для каждого значения.

Полученные значения коэффициентов меньше 0,1 будем считать незначительными, и приравнивать к 0.

Каждый из этих признаков влияет на актуальность поведенческих паттернов вредоносных программ. Для каждого класса АС необходимо сформировать мультимножество значений базовых признаков актуальности для поведенческих паттернов.

$$\Psi = \{\psi_1, \psi_2, \ldots, \psi_n, \ldots, \psi_u\}, \quad (6)$$

где $\psi = \frac{\Sigma h^*}{b}$, h^* – весовые коэффициенты значений базовых признаков АС, влияющих на поведенческий

Таблица 3.

Базовые признаки автоматизированных систем

Наименование признака АССН ОВД, h	Принимаемые значения признака	Значение коэффициента, h^*
Технология, используемая для построения системы хранения данных (СХД), h_1	NAS	1
	SAN	0,49
Доступ к сервису электронной почты (СЭП), h_2	Возможна отправка и получение писем внутри организации и в сети общего доступа	1
	Возможность отправки и получения писем только внутри организации	0,44
	Отсутствует доступ к сервису электронной почты	0,08
Подключение к сетям общего доступа (СОД), h_3	Возможность доступа ко всем ресурсам сети общего доступа	1
	Возможность доступа только к разрешенным ресурсам сети общего доступа	0,58
	Отсутствует подключение к сети общего доступа	0,09

Таблица 4.

Характеристики поведенческих паттернов вредоносных утилит

Поведенческий паттерн	Свойство информации	Базовый признак АССН ОВД	Частный признак АССН ОВД
Проникновение на компьютер-жертву, p_1	К	h_1,h_3	f_4,f_5,f_6
Скрытие следов присутствия преступников в системе, p_2	К	h_3	f_4,f_5
Внесение в список разрешенных посетителей системы новых пользователей, p_3	К	h_1,h_3	f_4,f_5,f_6
Прекращение работы системы, p_4	Д	h_1,h_3	f_1,f_3
Проведение атак типа «Отказ в обслуживании», p_5	Д	h_3	f_2,f_3,f_7
Сбор и анализ сетевых пакетов, p_6	К	h_1,h_3	f_1,f_2
Подмена адреса отправителя письма по электронной почте, p_7	Ц	h_2	f_6
Создание вредоносных программ, p_8	Ц	h_3	f_4
Навязывание ложной информации (уведомление об опасности, нарушениях), p_9	Ц	h_1	f_4
Модификация вредоносных программ, p_{10}	Ц	h_3	f_4
Распространение флуда (бесполезных сообщений по каналам электронной почты), p_{11}	Ц	h_2	f_6

паттерн, b – количество влияющих на поведенческий паттерн признаков АС (таблица 4).

2.3. Формирование базовых моделей оценки опасности деструктивных программных воздействий для АССН «Тестовая АССН ОВД»

Рассмотрим пример формирования базовых моделей оценки опасности деструктивных программных воздействий для АССН «Тестовая АССН ОВД» для вредоносных программ класса «Вредоносные утилиты».

Поведенческие паттерны вредоносных утилит влияют на конфиденциальность (К), целостность (Ц) и доступность (Д) информации, обрабатываемой в АССН ОВД. В таблице 4 представлены свойства информации, на которые воздействует паттерн и признак АССН ОВД, от которого зависит актуальность поведенческого паттерна.

В работе [17] разработана исходная модель для оценки опасности деструктивного программного воздействия вредоносных утилит:

$$J_{AHP_V} = 10 \cdot (0{,}258 \cdot p_1 + 0{,}181 \cdot p_2 + 0{,}121 \cdot p_3 + 0{,}121 \cdot p_4 + 0{,}077 \cdot p_5 + 0{,}077 \cdot p_6 + 0{,}077 \cdot p_7 + 0{,}027 \cdot p_8 + 0{,}027 \cdot p_9 + 0{,}019 \cdot p_{10} + 0{,}015 \cdot p_{11}) / 0{,}516. \quad (7)$$

В работе [10] определено множество связанных поведенческих паттернов вредоносных утилит

$$L = \{\{p_4,p_5\};\{p_7,p_{11}\};\{p_8,p_{10}\}\}.$$

С учетом связи поведенческих паттернов модель (7) примет следующий вид:

1. Если во вредоносной утилите совместно реализуется пара паттернов p_4,p_5:

$$J_{KN_{4,5}} = 10 \cdot (0{,}224 \cdot p_1 + 0{,}157 \cdot p_2 + 0{,}105 \cdot p_3 + 0{,}105 \cdot p_4 + 0{,}067 \cdot p_5 + 0{,}067 \cdot p_6 + 0{,}067 \cdot p_7 + 0{,}024 \cdot p_8 + 0{,}024 \cdot p_9 + 0{,}017 \cdot p_{10} + 0{,}013 \cdot p_{11} + 0{,}13 \cdot p_{4,5}) / 0{,}487. \quad (8)$$

2 .Если во вредоносной утилите совместно реализуется пара паттернов p_7,p_{11}:

$$J_{KN_{7,11}} = 10 \cdot (0{,}232 \cdot p_1 + 0{,}163 \cdot p_2 + 0{,}109 \cdot p_3 + 0{,}109 \cdot p_4 + 0{,}07 \cdot p_5 + 0{,}07 \cdot p_6 + 0{,}07 \cdot p_7 + 0{,}024 \cdot p_8 + 0{,}024 \cdot p_9 + 0{,}017 \cdot p_{10} + 0{,}014 \cdot p_{11} + 0{,}1 \cdot p_{7,11}) / 0{,}504. \quad (9)$$

3. Если во вредоносной утилите совместно реализуется пара паттернов p_8,p_{10}:

$$J_{KN_{8,10}} = 10 \cdot (0{,}244 \cdot p_1 + 0{,}171 \cdot p_2 + 0{,}114 \cdot p_3 + 0{,}114 \cdot p_4 + 0{,}073 \cdot p_5 + 0{,}073 \cdot p_6 + 0{,}073 \cdot p_7 + 0{,}026 \cdot p_8 + 0{,}026 \cdot p_9 + 0{,}018 \cdot p_{10} + 0{,}014 \cdot p_{11} + 0{,}056 \cdot p_{8,10}) / 0{,}529. \quad (10)$$

АССН «Тестовая АССН» относится к 4 классу и имеет следующие базовые признаки:

- Класс АССН – 4.
- СХД (h_1) – SAN ($h_1^* = 0{,}49$).
- Доступ к СЭП (h_2) – возможность отправки и получения писем только внутри организации (ведомства) ($h_2^* = 0{,}44$).
- Подключение АС к СОД (h_3) – отсутствует подключение к сети общего доступа ($h_3^* = 0{,}09$).

Составим мультимножество значений базовых признаков актуальности поведенческих паттернов для данного класса АССН ОВД:

$$\Psi_4 = \{0{,}25;0;0{,}25;0{,}25;0;0{,}25;0{,}44;0;0{,}49;0;0{,}44;0{,}44\}. \quad (11)$$

Значения базовых признаков актуальности для коэффициентов K определяются как средние значения базовых признаков для соответствующих связанных поведенческих паттернов.

Выполнив вычисления и нормировку элементов [18] получим следующие базовые модели ООДПВ:

1. При отсутствии связанных признаков:

$$J^*_{V_4} = 0{,}326 \cdot p_1 + 0{,}153 \cdot p_3 + 0{,}153 \cdot p_4 + \\ + 0{,}098 \cdot p_6 + 0{,}172 \cdot p_7 + 0{,}067 \cdot p_9 + 0{,}03 \cdot p_{11}. \quad (12)$$

2. При совместной реализации поведенческих паттернов p_7,p_{11}:

$$J^*_{KV_{4_{7,11}}} = 0{,}26 \cdot p_1 + 0{,}12 \cdot p_3 + 0{,}12 \cdot p_4 + 0{,}079 \cdot p_6 + \\ + 0{,}138 \cdot p_7 + 0{,}053 \cdot p_9 + 0{,}03 \cdot p_{11} + 0{,}2 \cdot K_{7,11}. \quad (13)$$

В данном случае не рассматриваются остальные пары связанных поведенческих паттернов, поскольку они не актуальны для данной АССН ОВД.

Затем необходимо определить значение $J_{4_{\max}}$ исходя из весовых коэффициентов поведенческих паттернов. Самой опасной вредоносной утилитой будет Linux.Siggen.172223, которая реализует поведенческие паттерны p_1, p_4, p_6, p_9. Для систем 4 класса ее опасность равна 0,644. При появлении новых вредоносных утилит, опасность которых будет выше, чем у Linux.Siggen.172223, необходимо будет выполнить уточнение сформированных моделей. Для формулы (10) самой опасной также будет вредоносная утилита Linux.Siggen.172223 и ее опасность равна 0,512.

Таким образом, базовые модели оценки опасности деструктивных программных воздействий вредоносных утилит для 4 класса АССН ОВД будут иметь вид:

$$J_{V_4} = 10 \cdot (0{,}326 \cdot p_1 + 0{,}153 \cdot p_3 + 0{,}153 \cdot p_4 + \\ + 0{,}098 \cdot p_6 + 0{,}172 \cdot p_7 + 0{,}067 \cdot p_9 + \\ + 0{,}03 \cdot p_{11}) / 0{,}644. \quad (14)$$

$$J_{KV_{4_{7,11}}} = 10 \cdot (0{,}26 \cdot p_1 + 0{,}12 \cdot p_3 + 0{,}12 \cdot p_4 + \\ + 0{,}079 \cdot p_6 + 0{,}138 \cdot p_7 + 0{,}053 \cdot p_9 + 0{,}03 \cdot p_{11} + \\ + 0{,}2 \cdot K_{7,11}) / 0{,}512. \quad (15)$$

3. Формирование частных моделей оценки опасности деструктивных программных воздействий

Частные модели предназначены для оценки опасности деструктивных программных воздействий вредоносных программ на конкретную АС.

3.1. Формирование частных моделей оценки опасности деструктивных программных воздействий в общем виде

Частные модели оценки опасности деструктивных программных воздействий разрабатываются для конкретной АС на основе базовых моделей и имеют вид:

Без учета связи поведенческих паттернов:

$$J_{V_B} = 10 \cdot \frac{J^*_{V_{Par}}}{J_{Par_{\max}}} = \frac{\sum_{i=1}^{n} \omega_i \cdot w_{ci} \cdot p_i}{J_{Par_{\max}}}, \quad (16)$$

где $J^*_{V_{Par}}$ – скорректированное значение показателя опасности для частной модели без учета связи признаков; ω – значение весовых коэффициентов частных признаков актуальности для соответствующих поведенческих паттернов; w_{ci} – скорректированное значение весовых коэффициентов поведенческих паттернов, рассчитанное в базовой модели по формуле: $w_{ci} = \psi_i \cdot w_i$; $J_{Par_{\max}}$ – значение опасности самой опасной вредоносной программы для частной модели без учета связи поведенческих паттернов.

С учетом связи поведенческих паттернов:

$$J_{KV_{Par}} = 10 \cdot \frac{J^*_{KV_{Par}}}{J_{KPar_{\max}}} = \frac{\sum_{i=1}^{n} \omega_i \cdot w_{ci} \cdot p_i + \sum_{j=1}^{u} \omega_j \cdot K_{cj}}{J_{KPar_{\max}}}, \quad (17)$$

где K_{cj} – скорректированное значение коэффициента для учета связи признаков, рассчитанное в базовой модели по формуле $K_{cj} = \psi_j \cdot K_j$; $J^*_{KV_{Par}}$ – скорректированное значение показателя опасности для частной модели без учета связи признаков; $J_{KPar_{\max}}$ – значение опасности самой опасной вредоносной программы для частной модели без учета связи поведенческих паттернов.

Для формирования частных моделей экспертам необходимо оценить влияние частных признаков АС на актуальность поведенческих паттернов. В работах [19, 20] определены признаки автоматизированных систем, которые рекомендуется рассматривать при моделировании процессов, связанных с информационной безопасностью: Состав и принимаемые значения для данных признаков могут изменяться исходя из особенностей построения и функционирования автоматизированных систем.

В результате работы экспертной группы для конкретной АС будет сформировано мультимножество значений частных признаков актуальности для поведенческих паттернов:

$$\Omega = \{\omega_1,\omega_2,...,\omega_n,...,\omega_u\}, \quad (18)$$

где $\omega = \frac{\Sigma f^*}{r}$, f^* – весовые коэффициенты значений базовых признаков АС, влияющих на поведенческий паттерн; r – количество влияющих на поведенческий паттерн признаков АС.

3.2. Формирование частных моделей оценки опасности деструктивных программных воздействий для АССН «Тестовая АССН ОВД»

Частные признаки АССН ОВД и принимаемые ими значения, с соответствующими весовыми коэффициентами (рассчитанными с использованием метода анализа иерархий) представлены в таблице 5. Весовые коэффициентов частных признаков могут быть уточнены в процессе формирования моделей, при изменении признаков, или принимаемых ими значений.

В нашем случае экспертная группа будет оценивать признаки АССН «Тестовая АССН ОВД», которая относится к 4 классу и имеет следующие частные признаки:

Назначение автоматизированной системы (f_1) – обеспечение оперативно-служебной деятельности $(f_1^* = 1)$.

Используемая топология построения автоматизированной системы (f_2) – древовидная структура $(f_2^* = 0{,}49)$.

Задачи, решаемые интеграцией с внешними автоматизированными системами (f_3) – отсутствует интеграция с внешними системами $(f_3^* = 0)$.

Тип используемой операционной системы (f_4) – ОС семейства Linux в защищенном исполнении $(f_4^* = 0{,}19)$.

Таблица 5.

Частные признаки АССН ОВД

Наименование признака АССН ОВД, , f	**Принимаемые значения признака**	**Значение коэффициента, f^***
Назначение автоматизированной системы, f_1	Обеспечение оперативно-служебной деятельности	1
	Обеспечение повседневной деятельности	0,57
	Обеспечение других видов деятельности	0,21
Используемая топология построения автоматизированной системы, f_2	Звезда-шина	1
	Древовидная структура	0,49
Задачи, решаемые интеграцией с внешними автоматизированными системами, f_3	Обмен файлами	1
	Общая база данных	0,44
	Отсутствует интеграция с внешними системами	0,08
Тип используемой операционной системы, f_4	ОС семейства Windows	1
	ОС семейства Linux	0,53
	ОС семейства Linux в защищенном исполнении	0,19
Тип используемой системы управления базами данных, f_5	Oracle	1
	MySQL	1
	PostgreSQL	0,33
Количество доменов безопасности в автоматизированной системе, f_6	Применение одного домена безопасности в нескольких АССН	1
	Отдельный домен безопасности для каждой АССН	0,49
Процент задействования ресурсов (оперативная, постоянная память), автоматизированной системы, в моменты пиковой нагрузки, f_7	[75% – 100%]	1
	[50% – 75%)	0,41
	[0% – 50%)	0,16

Тип используемой системы управления базами данных (f_5) – PostgreSQL ($f_5^* = 0{,}33$).

Количество доменов безопасности в автоматизированной системе (f_6) – отдельный домен безопасности для каждой АССН ($f_6^* = 0{,}49$).

Процент задействования ресурсов (оперативная, постоянная память), автоматизированной системы, задействованной в моменты пиковой нагрузки (f_7) – [50 % – 75 %] ($f_7^* = 0{,}41$).

Таким образом, мультимножество значений частных признаков актуальности поведенческих паттернов для АССН «Тестовая АССН ОВД» будет иметь вид:

$$\Omega_{Par} = \{0{,}34;0{,}26;0{,}34;0{,}5;0{,}3;0{,}75; 0{,}49;0{,}19;0{,}19;0{,}19;0{,}49;0{,}49\}. \quad (19)$$

Выполнив вычисления и нормировку элементов множества путем деления на их сумму, получим следующие частные модели оценки опасности деструктивных программных воздействий:

1. При отсутствии связанных поведенческих паттернов:

$$J^*_{V_{Par}} = 0{,}261 \cdot p_1 + 0{,}123 \cdot p_3 + 0{,}18 \cdot p_4 + 0{,}173 \cdot p_6 + 0{,}199 \cdot p_7 + 0{,}03 \cdot p_9 + 0{,}034 \cdot p_{11}. \quad (20)$$

2. При совместной реализации поведенческих паттернов p_7, p_{11}:

$$J^*_{KV_{Par_{7,11}}} = 0{,}21 \cdot p_1 + 0{,}09 \cdot p_3 + 0{,}14 \cdot p_4 + 0{,}14 \cdot p_6 + 0{,}15 \cdot p_7 + 0{,}02 \cdot p_9 + 0{,}03 \cdot p_{11} + 0{,}22 \cdot K_{7,11}. \quad (21)$$

Самой опасной вредоносной утилитой для автоматизированной системы «Тестовая АССН ОВД» также будет являться Linux.Siggen.172223, и ее опасность $J_{Par_{\max}}$ равна 0,647, а $J^*_{KPar_{7,11_{\max}}}$ равна 0,51. Также

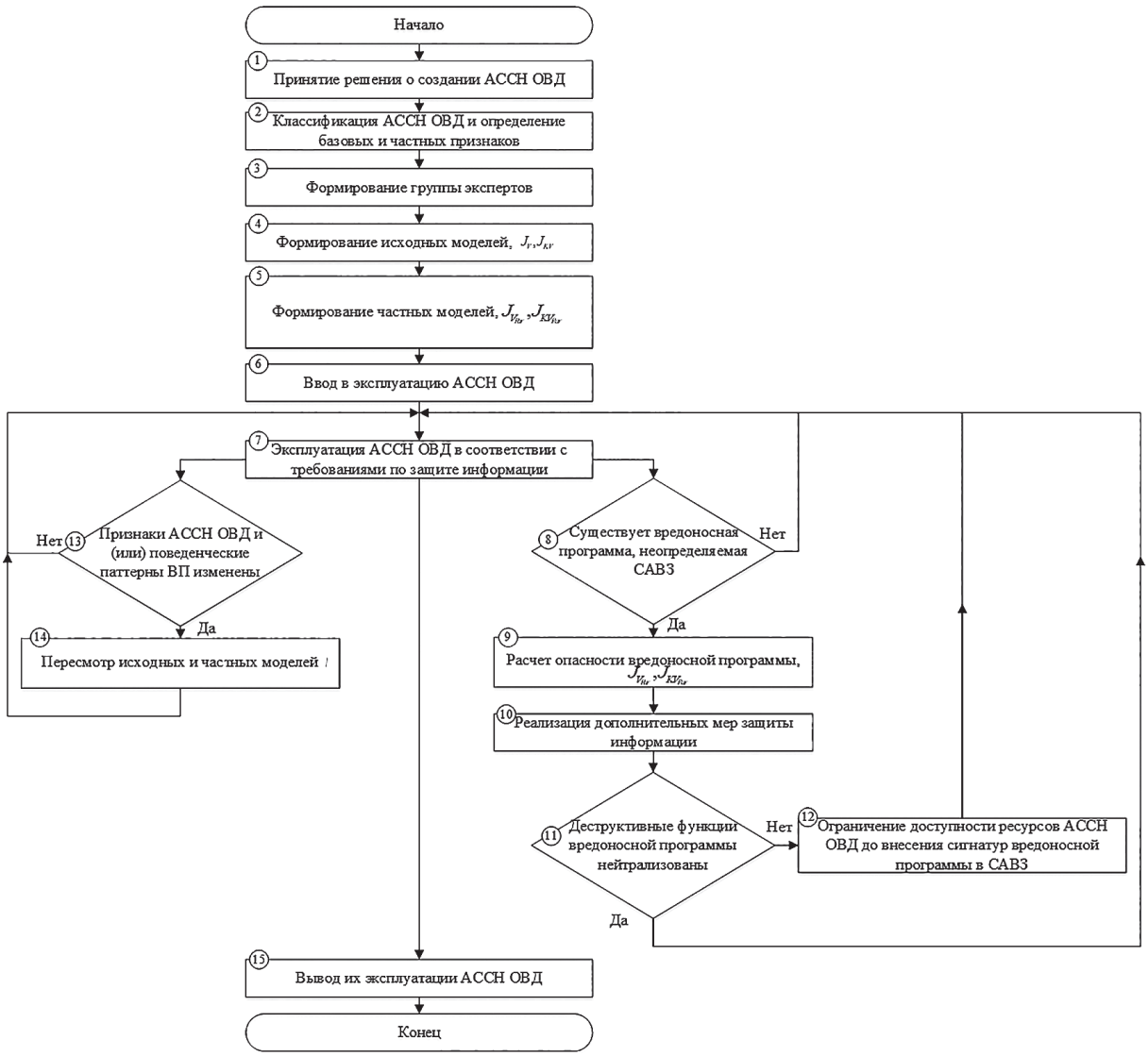

Рис. 2. Алгоритм планирования и реализации процессов жизненного цикла АССН ОВД в условиях деструктивных программных воздействий

необходимо учесть коэффициенты для корректировки частной модели в зависимости от класса (уровня) защищенности.

Автоматизированная система «Тестовая АССН ОВД» относится к 4 классу АССН, следовательно, частные модели будет иметь вид:

1. Без учета связи поведенческих паттернов:

$$J_{KV_{Par}} = 1 \cdot (10 \cdot (0{,}261 \cdot p_1 + 0{,}123 \cdot p_3 + 0{,}18 \cdot p_4 + 0{,}173 \cdot p_6 + 0{,}199 \cdot p_7 + 0{,}03 \cdot p_9 + 0{,}034 \cdot p_{11}) / 0{,}647). \quad (22)$$

2. С учетом связи поведенческих паттернов p_7,p_{11}:

$$J_{KV_{Par_{7,11}}} = 1 \cdot (10 \cdot (0{,}21 \cdot p_1 + 0{,}09 \cdot p_3 + 0{,}14 \cdot p_4 + 0{,}14 \cdot p_6 + 0{,}15 \cdot p_7 + 0{,}02 \cdot p_9 + 0{,}03 \cdot p_{11} + 0{,}22 \cdot K_{7,11}) / 0{,}51). \quad (23)$$

Таким образом, алгоритм планирования и реализации процессов жизненного цикла АССН ОВД в условиях деструктивных программных воздействий представлен на рисунке 2.

4. Верификация сформированных моделей оценки опасности деструктивных программных воздействий

Верификация сформированных моделей выполнена на тестовом наборе данных вредоносных утилит и представлена в таблице 6.

В ходе вычислительного эксперимента определено, что учет связи поведенческих паттернов вредоносных программ и признаков автоматизированных систем влияет на уровень опасности вредоносных утилит. Например, для вредоносной утилиты № 1 Constructor.DarkHorse в исходной модели определен уровень опасности «Критический», а для базовой и частной «Средний». Во вредоносной утилите № 3 DDoS.Siggen.41 в исходной модели определен уровень опасности «Средний», а в базовой и частной «Низкий». Снижение уровня опасности вызвано тем, что реализуемые в данных примерах связанные поведенческие паттерны не актуальны для АССН «Тестовая АССН ОВД», а признаки АССН снижают актуальность для остальных реализуемых паттернов. Для вредоносной утилиты № 5 Tool.TermService уровень опасности, рассчитанный с использованием исходной модели «Средний», а с использованием базовой и частной «Критический». Отличие в значениях показателя опасности вызвано тем, что признаки АССН повышают актуальность реализуемых во вредоносной программе поведенческих паттернов. Формирование частных моделей для каждой АССН ОВД позволит принимать адекватные и достаточные меры по обеспечению безопасности информации при появлении неизвестных вредоносных программ.

Заключение

Разработанная методика ООДПВ, отличается от существующих учетом признаков АССН ОВД, способствует формированию единого подхода к реализации мер по защиты информации. При разработке методики были решены следующие задачи:

1. Определены базовые и частные признаки АССН ОВД, характеризующие актуальность поведенческих паттернов вредоносных программ в зависимости от функциональных особенностей АССН ОВД.

Таблица 6.

Верификация сформированных моделей

№ п/п	Название вредоносной утилиты	Реализуемые поведенческие паттерны	Исходные модели J_{AHP_V},J_{KN}	Базовые модели J_{V_4},J_{KV_4}	Частные модели $J_{V_{Par}}$,$J_{KV_{Par}}$
1.	Constructor.DarkHorse	p_1, p_2, p_8, p_{10}	9,74	5,06	4,03
2.	Spy-Net 0.9	p_1, p_2	8,51	5,06	4,03
3.	DDoS.Siggen.41	p_4, p_5, p_{10}	6,2	2,38	2,78
4.	Linux.Siggen.5542	p_1, p_6	6,49	6,58	6,7
5.	Tool.TermService	p_3, p_7, p_{11}	5,8	9,53	9,61
6.	Linux.Siggen.322	p_1	5	5,06	4,03
7.	Tool.UDPFlood	p_3, p_{11}	2,64	2,84	2,43
8.	Tool.InstallToolbar.5	p_6, p_9	2,02	2,56	3,13
9.	Tool.Wpakill.4	p_7, p_9	2,02	3,71	3,6
10.	Tool.Spamer.18	p_9, p_{11}	0,81	1,09	0,99

2. Выполнено моделирование оценки опасности деструктивных программных воздействий с учетом базовых, частных признаков АССН ОВД.
3. Разработан алгоритм планирования и реализации процессов жизненного цикла АССН ОВД в условиях деструктивных программных воздействий.
4. Выполнен вычислительный эксперимент, по оценке опасности деструктивных программных воздействий для АССН ОВД. В ходе вычислительного эксперимента получены непротиворечивые результаты, которые подтверждают зависимость уровня опасности вредоносных программ от признаков АССН ОВД.

Результаты исследования могут быть применены администраторами безопасности АССН ОВД, для обеспечения бесперебойного функционирования на всех этапах эксплуатации систем.

Перспективы дальнейших исследований:

- определение набора достаточных дополнительных мер защиты информации, при появлении неизвестных вредоносных программ;
- формирование моделей для оценки опасности деструктивных программных воздействий с учетом актуальности поведенческих паттернов для других классов вредоносных программ.

Литература

1. F. Alkhudhayr, S. Alfarraj, B. Aljameeli and S. Elkhdiri, «Information Security: A Review of Information Security Issues and Techniques», 2019. 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019, pp. 1–6. DOI:10.1109/CAIS.2019.8769504.
2. Methodical approach to reducing the dimensionality of the task of requirements substantiation for protection of information systems against unauthorized access in organizational-technical systems / T. V. Meshcheryakova, A. V. Batskikh, O. A. Gulyaev, A. A. Abdullin // Journal of Physics: Conference Series: Applied Mathematics, Computational Science and Mechanics: Current Problems, Voronezh, 11–13 ноября 2019 года. – Bristol: Institute of Physics Publishing, 2020. – P. 012013. – DOI 10.1088/1742-6596/1479/1/012013.
3. Оценка соответствия модели угроз и требований доверия систем Интернета вещей массового применения / А. А. Бахтин, Д. С. Брагин, А. А. Конев, А. В. Шарамок // Наноиндустрия. – 2020. – Т. 13, № S4(99). – С. 137–138. – DOI 10.22184/1993-8578.2020.13.4s.137.138.
4. Язов Ю. К. Составные сети Петри-Маркова со специальными условиями построения для моделирования угроз безопасности информации / Ю. К. Язов, А. П. Панфилов // Вопросы кибербезопасности. – 2024. – № 2(60). – С. 53–65. – DOI 10.21681/2311-3456-2024-2-53-65.
5. Язов Ю. К. Составные сети Петри – Маркова на основе полумарковских процессов и их применение при моделировании динамики реализации угроз безопасности информации в информационных системах / Ю. К. Язов, А. О. Авсентьев, А. П. Панфилов, В. Н. Пржегорлинский // Вестник Воронежского института МВД России. – 2024. – № 2. – С. 63–78. – EDN UWINDW.
6. Мещеряков Р. В. Перспективные направления применения технологий искусственного интеллекта при защите информации // Мещеряков Р. В., Мельников С. Ю., Пересыпкин В. А., Хорев А. А. // Вопросы кибербезопасности. – 2024. – № 4(62). – С. 2–12. – DOI 10.21681/2311-3456-2024-4-02-12.
7. Models and methods of information reliability and data protection / G. I. Korshunov, V. A. Lipatnikov, V. A. Tichonov [et al.] // IOP Conference Series: Materials Science and Engineering: International Workshop «Advanced Technologies in Material Science, Mechanical and Automation Engineering – MIP: Engineering – 2019», Krasnoyarsk, 04–06 апреля 2019 года. – London: Institute of Physics and IOP P8ublishing Limited, 2019. – P. 52001. – DOI 10.1088/1757-899X/537/5/052001.
8. Атакищев О. И. Метаграмматический подход анализа иерархий для синтеза систем безопасности атомных электростанций / О. И. Атакищев, В. Г. Грибунин, И. Л. Борисенков, М. Н. Лысачев // Вопросы кибербезопасности. – 2023. – № 1(53). – С. 82–92. – DOI 10.21681/2311-3456-2023-1-82-92.
9. Munier N. Uses and Limitations of the AHP Method/ N. Munier, E. Hontoria // Management for Professionals. Springer Cham – 2021. – 130 pp. DOI 10.1007/978-3-030-60392-2.
10. Мельников А. В. Численный метод модификации моделей, разработанных на основе метода анализа иерархий, с использованием искусственной нейронной сети / А. В. Мельников, Н. С. Кобяков // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. – 2024. – № 4. – С. 5–22. – DOI 10.17308/sait/1995-5499/2024/4/5-21.
11. 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.
12. 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.
13. Кобяков, Н. С. Алгоритм классификации автоматизированных систем специального назначения / Н. С. Кобяков, В. Н. Париев // Альманах Пермского военного института войск национальной гвардии. – 2024. – № 2(14). – С. 15–21. – EDN PKWCCP.
14. Жилин Р. А. Численный метод предварительной экспертизы альтернатив нарушителей охраны объектов общекриминальной направленности / Р. А. Жилин, А. В. Мельников, И. В. Щербакова // Вестник Воронежского института МВД России. – 2019. – № 3. – С. 46–54. – EDN NEYIJN.
15. Авраменко В. С., Маликов А. В. Методика диагностирования компьютерных инцидентов безопасности в автоматизированных системах специального назначения. Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12, № 1. – С. 44–52. – DOI 10.36724/2409-5419-2020-12-1-44-52.
16. Долгачев, М. В., Костюнин В. А. Комплексный анализ поведения системы Windows для обнаружения киберугроз. Вопросы кибербезопасности. – 2025. – № 2(66). – С. 71–77. – DOI 10.21681/2311-3456-2025-2-71-77.
17. Мельников А. В. Модель оценки опасности вредоносных утилит / А. В. Мельников, В. И. Сумин, Н. С. Кобяков // Промышленные АСУ и контроллеры. – 2023. – № 7. – С. 33–40. – DOI 10.25791/asu.7.2023.1448.

18. Melnikov, A. V. Method of forming expert coalitions in the context of solving the expertise problem of alternatives with weakly formalized criteria / A. V. Melnikov, I. V. Shcherbakova, R. A. Zhilin // Journal of Physics: Conference Series: Applied Mathematics, Computational Science and Mechanics: Current Problems, Voronezh, 11–13 ноября 2019 года. – Bristol: Institute of Physics Publishing, 2020. – P. 012071. – DOI 10.1088/1742-6596/1479/1/012071.
19. 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.
20. Язов Ю. К., Авсентьев О. С., Авсентьев А. О., Рубцова И. О. Метод оценивания эффективности защиты электронного документооборота с применением аппарата сетей Петри – Маркова. Труды СПИИРАН. – 2019. – Т. 18, № 6. – С. 1269–1300. – DOI 10.15622/sp.2019.18.6.1269-1300.

METHOD OF ASSESSING THE DANGER OF DESTRUCTIVE SOFTWARE IMPACTS ON AUTOMATED SPECIAL-PURPOSE SYSTEMS OF INTERNAL AFFAIRS BODIES

Melnikov A. V.[4], Kobyakov N. S.[5]

Keywords: *malware, automated systems features, information security, analytic hierarchy process.*

The objective of the study: *modeling the hazard indicator of destructive software impacts, taking into account the relevance of the behavioral patterns of malware for automated special-purpose systems of the internal affairs agencies.*

Research methods: *the hierarchy analysis method is used to form models for assessing the hazard of destructive software impacts and to determine the numerical values of the attributes of the automated special-purpose systems of the internal affairs agencies.*

Research result: *the basic and specific attributes of the automated special-purpose systems of the internal affairs agencies are determined, characterizing the relevance of the behavioral patterns of malware depending on the functional features of the automated special-purpose systems of the internal affairs agencies. Basic and specific models for assessing the hazard of destructive software impacts on the automated special-purpose systems of the internal affairs agencies have been developed, taking into account the relevance of the behavioral patterns of malware. An algorithm for planning and implementing the life cycle processes of the automated special-purpose systems of the internal affairs agencies in the context of destructive software impacts has been developed. The developed methodology has been verified using the example of forming models for assessing the hazard of destructive software impacts of malware of the «Malicious Utilities» class on a test automated special-purpose system. The developed models have been verified on a test data set generated by interviewing experts.*

Practical significance: *the developed methodology can be used by security administrators of automated special-purpose systems when assessing the danger of destructive software impacts and determining the goals and list of measures to be implemented to ensure information protection when unknown malicious programs appear.*

References

1. F. Alkhudhayr, S. Alfarraj, B. Aljameeli and S. Elkhdiri, «Information Security:A Review of Information Security Issues and Techniques», 2019. 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019, pp. 1–6, doi: 10.1109/CAIS.2019.8769504.
2. Methodical approach to reducing the dimensionality of the task of requirements substantiation for protection of information systems against unauthorized access in organizational-technical systems / T. V. Meshcheryakova, A. V. Batskikh, O. A. Gulyaev, A. A. Abdullin // Journal of Physics: Conference Series: Applied Mathematics, Computational Science and Mechanics: Current Problems, Voronezh, 11–13 ноября 2019 года. – Bristol: Institute of Physics Publishing, 2020. – P. 012013. – DOI 10.1088/1742-6596/1479/1/012013.
3. Ocenka sootvetstviya modeli ugroz i trebovanij doveriya sistem Interneta veshchej massovogo primeneniya / A. A. Bakhtin, D. S. Bragin, A. A. Konev, A. V. Sharamok // Nanoindustry. – 2020. – T. 13, № S4(99). – pp. 137-138. – DOI 10.22184/1993-8578.2020.13.4s.137.138.
4. Yazov, Yu. K. Sostavnye seti Petri-Markova so special'nymi usloviyami postroeniya dlya modelirovaniya ugroz bezopasnosti informacii / Yu. K. Yazov, A. P. Panfilov // Cybersecurity issues. – 2024. – № 2(60). – pp. 53-65. – DOI 10.21681/2311-3456-2024-2-53-65.
5. Sostavnye seti Petri – Markova na osnove polumarkovskih processov i ih primenenie pri modelirovanii dinamiki realizacii ugroz bezopasnosti informacii v informacionnyh sistemah / Yu. K. Yazov, A. O. Avsentiev, A. P. Panfilov, V. N. Przhegorlinsky // Vestnik Voronezhskogo instituta MVD Rossii. – 2024. – № 2. – pp. 63-78. – EDN UWINDW.
6. Perspektivnye napravleniya primeneniya tekhnologij iskusstvennogo intellekta pri zashchite informacii / R. V. Meshcheryakov, S. Yu. Melnikov, V. A. Peresypkin, A. A. Khorev // Cybersecurity issues. – 2024. – № 4(62). – pp. 2–12. – DOI 10.21681/2311-3456-2024-4-02-12.

4 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 the Russian Federation, Voronezh, Russia. ORCID: https://orcid.org/0000-0001-5080-1162. E-mail: meln78@mail.ru
5 Nikolai S. Kobyakov, postgraduate student of the Department of Automated Information Systems of Internal Affairs Bodies, Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation, Voronezh, Russia. ORCID: https://orcid.org/0000-0002-4950-7879. E-mail: kkobyakov1234@gmail.com

7. Models and methods of information reliability and data protection / G. I. Korshunov, V. A. Lipatnikov, V. A. Tichonov [et al.] // IOP Conference Series: Materials Science and Engineering: International Workshop «Advanced Technologies in Material Science, Mechanical and Automation Engineering – MIP: Engineering – 2019», Krasnoyarsk – London: Institute of Physics and IOP P8ublishing Limited, 2019. – P. 52001. – DOI 10.1088/1757-899X/537/5/052001.
8. Metagrammaticheskij podhod analiza ierarhij dlya sinteza sistem bezopasnosti atomnyh elektrostancij / O. I. Atakishchev, V. G. Gribunin, I. L. Borisenkov, M. N. Lysachev // Cybersecurity issues. – 2023. – № 1(53). – pp. 82–92. – DOI 10.21681/2311-3456-2023-1-82-92.
9. Munier N. Uses and Limitations of the AHP Method/ N. Munier, E. Hontoria // Management for Professionals. Springer Cham – 2021. – 130 pp. DOI 10.1007/978-3-030-60392-2.
10. Mel'nikov A. V. Kobjakov N. S. Chislennyj metod modifikacii modelej, razrabotannyh na osnove metoda analiza ierarhij, s ispol'zovaniem iskusstvennoj nejronnoj seti.VSU Bulletin. Series: System analysis and information technologies – 2024. – № 4. – S. 5–22. – DOI 10.17308/sait/1995-5499/2024/4/5-21.
11. Melnikov A. V. Podhod k ocenke opasnosti destruktivnyh vozdejstvij vredonosnyh programm na avtomatizirovannye sistemy special'nogo naznacheniya / A. V. Melnikov, N. S. Kobyakov // Bezopasnost' informacionnyh tekhnologij. – 2023. – T. 30, № 3. – pp. 51–60. – DOI 10.26583/bit.2023.3.03. – EDN RJWWZH.
12. Melnikov, A. V. Modeli i algoritmy realizacii organizacionnyh mer zashchity informacii v ASSN ot destruktivnyh vozdejstvij ranee neizvestnyh vredonosnyh programm / A. V. Melnikov, N. S. Kobyakov, R. A. Zhilin // Vestnik Voronezhskogo instituta MVD Rossii. – 2023. – № 3. – pp. 80–87. – EDN ZILKNA.
13. Zhilin R. A. CHislennyj metod predvaritel'noj ekspertizy al'ternativ narushitelej ohrany ob"ektov obshchekriminal'noj napravlennosti / R. A. Zhilin, A. V. Melnikov, I. V. Shcherbakova // Vestnik Voronezhskogo instituta MVD Rossii. – 2019. – № 3. – pp. 46–54. – EDN NEYIJN
14. Kobyakov, N. S. Algoritm klassifikacii avtomatizirovannyh sistem special'nogo naznacheniya / N. S. Kobyakov, V. N. Pariev // Al'manah Permskogo voennogo instituta vojsk nacional'noj gvardii. – 2024. – № 2(14). – pp. 15–21. – EDN PKWCCP.
15. Avramenko V. S., Malikov A. V. Metodika diagnostirovanija komp'juternyh incidentov bezopasnosti v avtomatizirovannyh sistemah special'nogo naznachenija. Naukoemkie tehnologii v kosmicheskih issledovanijah Zemli. – 2020. – T. 12, № 1. – S. 44–52. – DOI 10.36724/2409-5419-2020-12-1-44-52.
16. Dolgachev, M. V., Kostjunin V. A. Kompleksnyj analiz povedenija sistemy Windows dlja obnaruzhenija kiberugroz. Voprosy kiberbezopasnosti. – 2025. – № 2(66). – S. 71–77. – DOI 10.21681/2311-3456-2025-2-71-77.
17. Melnikov, A. V. Model' ocenki opasnosti vredonosnyh utilit / A. V. Melnikov, V. I. Sumin, N. S. Kobyakov // Promyshlennye ASU i kontrollery. – 2023. – № 7. – pp. 33–40. – DOI 10.25791/asu.7.2023.1448.
18. Melnikov, A. V. Method of forming expert coalitions in the context of solving the expertise problem of alternatives with weakly formalized criteria / A. V. Melnikov, I. V. Shcherbakova, R. A. Zhilin // Journal of Physics: Conference Series: Applied Mathematics, Computational Science and Mechanics: Current Problems, Voronezh, 11–13 ноября 2019 года. – Bristol: Institute of Physics Publishing, 2020. – P. 012071. – DOI 10.1088/1742-6596/1479/1/012071.
19. Yazov, Yu. K. Soloviev S.V. Metodologiya ocenki effektivnosti zashchity informacii v informacionnyh sistemah ot nesankcionirovannogo dostupa. Sankt-Peterburg: Izdatel'stvo «Naukoemkie tekhnologii» 2023. – 258 P. – ISBN 978-5-907618-36-7. – EDN WVCHKW.
20. Yazov Yu. K., Avsentiev O. S., Avsentiev A. O., Rubtsova I. O. Metod ocenivaniya effektivnosti zashchity elektronnogo dokumentooborota s primeneniem apparata setej Petri – Markova / Proceedings of SPIIRAS. – 2019. – T. 18, № 6. – pp. 1269–1300. – DOI 10.15622/sp.2019.18.6.1269-1300.