МЕТОД ОБНАРУЖЕНИЯ АТАК РАЗЛИЧНОГО ГЕНЕЗА НА СЛОЖНЫЕ ОБЪЕКТЫ НА ОСНОВЕ ИНФОРМАЦИИ СОСТОЯНИЯ. ЧАСТЬ 2. АЛГОРИТМ, МОДЕЛЬ И ЭКСПЕРИМЕНТ

Израилов К.Е.[1], Буйневич М.В.[2]

Цель исследования: *создание метода обнаружения атак на сложные объекты и процессы путем оценивания и прогнозирования их состояния; метод основывается на 7 принципах, предложенных авторами ранее; особенностью метода является его инвариантность по отношению к генезу атак.*

Методы исследования: *системный анализ, методы аналитического моделирования, статистические методы и методы машинного обучения, разработка программного кода для реализации алгоритмов оценивания и прогнозирования.*

Полученный результат: *предложен метод обнаружения атак на сложный объект, использующий оценивание текущих и прогнозирование будущих состояний; описание метода даётся в схематичном и аналитическом виде с использованием сквозного примера из области информационной безопасности; теоретическая значимость заключается в развитии научно-методологического аппарата оценивания и прогнозирования состояний объектов различной структуры; практическая значимость заключается в возможности непосредственной реализации программного прототипа с потенциально высокой эффективностью.*

Во второй части статьи алгоритмизируются все этапы метода, что позволяет получить аналитическую модель обнаружения атак. Представлена методика управления процессом обнаружения, разработанная в интересах практического применения предложенного научно-методологического аппарата. Описывается ход эксперимента по применению метода для гипотетического примера атак на сетевой узел. Показана степень использования разработанных авторами в предыдущих исследованиях 7 принципов, положенных в основу способов оценивания и прогнозирования состояния сложных объектов.

Научная новизна *заключается в создании метода обнаружения атак на сложный объект (или процесс), в основе которого лежит принципиально новый подход к оцениванию и прогнозированию его состояния, полученный авторами в предыдущих исследованиях. Как результат, данный метод применим к предметной области без учета ее специфики, что, в частности, достигается за счет использования оригинальной авторской интеллектуальной нечеткой графо-ориентированной модели. В отличие от большого количества методов обнаружения атак на информационные системы, данный метод описан не только в виде графической схемы и последовательности шагов, но и с использованием аналитической записи алгоритмов, что позволяет применять к нему определенные математические аппараты (например, для обоснования работоспособности или оптимизации отдельных этапов).*

Ключевые слова: *информационные технологии, информационная безопасность, сложный объект, сложный процесс, метод обнаружения атак, аналитический алгоритм, эксперимент.*

DOI: 10.21681/2311-3456-2023-4-80-93

Введение

В первой части статьи [1] авторами формулируются предпосылки к созданию поэтапного метода обнаружения атак различного генеза на сложные объекты на основе информации состояния (далее – Метод).

1 Израилов Константин Евгеньевич, кандидат технических наук, доцент, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, Санкт-Петербург. ORCHID: https://orcid.org/0000-0002-9412-5693. Scopus Author ID: 56123238800. E-mail: konstantin.izrailov@mail.ru.

2 Буйневич Михаил Викторович, доктор технических наук, профессор, профессор кафедры прикладной математики и информационных технологий Санкт-Петербургского университета государственной противопожарной службы МЧС России, Санкт-Петербург. ORCHID: https://orcid.org/0000-0001-8146-0022. Scopus Author ID: 56122749800. E-mail: bmv1958@yandex.ru.

Приводится описание всех этапов Метода и базовой логики их выполнения. Поэлементно описывается схема обнаружения атак, представленная в графическом виде.

Аналитический алгоритм обнаружения атак

Используя детализацию Метода [1], опишем соответствующий алгоритм, представив его в аналитическом виде. Такая форма записи как частично обоснует с теоретической точки зрения работоспособность всего Метода (путем непротиворечивости последовательности вычисления аналитических функций и наличия всех необходимых входных и выходных параметров), так и позволит использовать определенные математические аппараты при реализации его этапов.

Этап 1. Анализ данных

Операция «1.1. Определение характеристик объекта» ($Operation_1^{Stage\ 1}$) имеет следующую запись:

$$Information_i = Detect_i\ (Object)$$

$$\left\{\bigcup_i \bigcup_j Characteristic_{i,j} = \right.$$

$$= Operation_1^{Stage\ 1}\left(\bigcup_i Information_i\right),$$

где $Object$ – исследуемый объект; $Detection_i()$ – операция сбора информации с датчиков [2] для i-го сценария функционирования объекта; $Information_i$ – информация об объекте согласно i-му сценарию; $Characteristic_{i,j}$ – j-ая характеристика об объекте согласно i-му сценарию (соответственно, множество $\bigcup_j Characteristic_{i,j}$ представляет собой набор характеристик для одного сценария).

Операция «1.2. Анализ изменений характеристик объекта» ($Operation_2^{Stage\ 1}$) имеет следующую запись:

$$\bigcup_i Graph_i^{PBH} =$$

$$= Operation_2^{Stage\ 1} \bigcup_i \bigcup_j Characteristic_{i,j},$$

где $Graph_i^{PBS}$ – Граф_ЧСП для i-го сценария поведения объекта (РВН – *аббр. от англ.* Private Behavior Scenarios, *перевод на русс.* – Частные Сценарии Поведения) [3].

Этап 2. Построение модели

Операция «2.1. Построение единого графа» ($Operation_1^{Stage\ 2}$) имеет следующую запись:

$$Graph^{CSS} = Operation_1^{Stage\ 2}\left(\bigcup_i Graph_i^{PSB}\right),$$

где $Grah^{CSS}$ – Граф_ПНХ (РВН – *аббр. от англ.* Characteristic Set Sequence, *перевод на русс.* – Последовательный Набор Характеристик).

Операция «2.2. Кластеризация узлов графов» ($Operation_2^{Stage\ 2}$) имеет следующую запись:

$$\begin{cases} Graph^{FBS} \equiv \left\langle \bigcup_s State_s \middle| \bigcup_l Link_l \middle| \bigcup_m Mark_m \right\rangle \\ State_s \in ID \\ Link \in \langle State_{From} | State_{To} \rangle \\ Mark_m \in (Scenario^{Normal}, Scenario^{Attack}) \\ Graph^{FBS} = Operation_2^{Stage\ 2}(Graph^{CSS}, \\ Algorithm_{Clustering}, N_{Clusters}) \\ N_{Clusters} = \\ = ObtainOptimalClustersNum\left(\bigcup_i Graph_i^{PSB}\ , \right. \\ \left. Environment\right) \end{cases}$$

где $Grah^{FBS}$ – Граф_НСП (FBS – *аббр. от англ.* Fuzzy Behavior States, *перевод на русс.* – Нечеткие Состояния Поведения); $\bigcup_s State_s$ – множество s-ых состояний в графе (которые могут быть заданы численным идентификатором ID); $\bigcup_l Link_l$ – множество l-ых соединений состояний в графе, каждое из которых представляет собой пару начального ($State_{From}$) и конечного ($State_{To}$) состояний; $\bigcup_m Mark_m$ – множество m-ых меток состояний (нормальный – $Scenario^{Normal}$, под атакой – $Scenario^{Attack}$); $Algorithm_{Clustering}$ – алгоритм кластеризации [4, 5]; $N_{Clusters}$ – число кластеров для выделения состояний в графе [6], определяемое экспертным или аналитическим способом [7] по Графу_ЧСП с учетом внешних условий $Environment$ (таких, как мнение специалистов, требуемая точность будущего прогнозирования, объективные критерии оптимальности и т.п.) путем применения операции $ObtainOptimalClustersNum()$. Таким образом, фактически, Граф_НСП представляет собой объединение Графов_ПНХ с выделением состояний, которые также имеют соответствующие маркеры.

Операция «2.3. Построение классификаторов состояний» ($Operation_3^{Stage\ 2}$) имеет следующую запись:

$$\begin{cases} Graph^{CBS} \equiv \\ \equiv \left\langle Graph^{FBS} \middle| \bigcup_i Classificator_i^{CurrentState} \right\rangle \\ Graph^{CBS} = Operation_3^{Stage\ 2}(Graph^{FSS}, \\ Algorithm_{Classification}) \end{cases}$$

где $Graph^{FBS}$ – Граф_КСП (CBS – *аббр. от англ.* Classifiable Behavior States, *перевод на русс.* – Классифицируемые Состояния Поведения); $Classificator_i^{CurrentState}$ – обученный классификатор *i*-го состояния в графе по набору характеристик объекта, полученный в процессе работы операции [8, 9]; $Algorithm_{Classification}$ – алгоритм классификации. Таким образом, фактически, Граф_КСП представляет собой расширение Графа_НСП классификаторами в каждом узле для определения состояния объекта, что отражено в первом уравнении системы.

Операция «2.4. Построение классификаторов перехода между состояниями» ($Operation_4^{Stage\ 2}$) имеет следующую запись:

$$\begin{cases} Model^{IFGO} \equiv \\ \equiv \left\langle Graph^{CBS} \middle| \bigcup_i Classificator_i^{NextState} \middle| \bigcup_t^T State_{-t} \right\rangle, \\ Model^{IFGO} = Operation_4^{Stage\ 2}(Graph^{CBS}, \\ Algorithm_{Classification}) \end{cases}$$

где $Model^{IFGO}$ – Модель_ИНГО (IFGO – *аббр. от англ.* Intelligent Fuzzy Graph-Jriented, *перевод на русс.* – Интеллектуальный Нечеткий Графо-Ориентированный); $Classificator_i^{NextState}$ – обученный классификатор, определяющий состояние, следующее за *i*-м, используя для этого предыдущие состояния [10]; $State_{-t}$ – состояние в момент, отстающий от текущего состояния на время t (в данном случае знак «–» перед «*t*» как раз и указывает на предшествующее время); соответственно, $\bigcup_t^T State_{-t}$ – хронология изменений состояний объекта за диапазон времени T; $Algorithm_{Classification}$ – алгоритм классификации. Таким образом, фактически, Модель_ИНГО представляет собой расширение Графа_КСП хронологией изменения состояний и классификаторами в каждом узле для определения будущего состояния, что отражено в первом уравнении системы.

Этап 3. Графо-ориентированное моделирование

Операция «3.1. Определение характеристик объекта» ($Operation_1^{Stage\ 3}$) имеет следующую запись:

$$\bigcup_j Characteristic_{0,j} = Operation_1^{Stage\ 3}(Information_0),$$

где $Information_0$ – информация о текущем состоянии объекта (здесь и далее индекс «0» означает момент времени «T+0»), $Characteristic_{0,j}$ – j-ая характеристика об объекте для текущего состояния).

Операция «3.2. Классификация состояниями объекта» ($Operation_2^{Stage\ 3}$) имеет следующую запись:

$$State_0 = Operation_2^{Stage\ 3}\left(\bigcup_j Characteristic_{0,j}, Graph^{CBS}, Settings_{Classification}\right),$$

где $State_0$ – текущее состояние объекта, полученное путем классификации текущего набора его характеристик; $Settings_{Classification}$ – настройки классификации, например, минимально допустимый уровень достоверности результата (т.е. вероятность выбора класса-состояния). Следует отметить, что для получения текущего состояния объекта достаточно использовать Граф_КСП вместо всей Модели_ИНГО, поскольку последняя включает первый.

Операция «3.3. Актуализация состояния объекта» ($Operation_3^{Stage\ 3}$) имеет следующую запись:

$$\bigcup_t^T State_{-t} = Operation_3^{Stage\ 3}(Graph^{CBS}, State_0).$$

Операция «3.4. Обновление статистики предыдущих состояний» ($Operation_4^{Stage\ 3}$) имеет следующую запись:

$$Model^{IFGO} = Operation_4^{Stage\ 3}(Model^{IFGO}, State_0).$$

Этап 4. Имитационное моделирование

Операция «4.1. Определение перехода на следующее состояние» ($Operation_1^{Stage\ 4}$) имеет следующую запись:

$$t = 1..F: State'_{t+1} = Operation_1^{Stage\ 4}(Model^{IFGO}, State_t),$$

где $State'_{t+1}$ – состояние в момент, следующий за моментом времени t (в данном случае знак «+» перед «t» как раз и указывает на последующее время); знак степени «$'$» здесь и далее означает, что состояние было предсказано, а не гарантированно свершилось; $State_t$ – состояние в момент времени t, для которого прогнозируется следующее состояние; F – глубина прогноза, означающая количество итераций с предсказанием состояния путем вызова данной операции [11]. Операция может выполняться итеративно, предсказывая состояния в момент времен +1, +2, +3 … от текущего; естественно, это будет приводить к нарастанию ошибки прогнозирования.

Операция «4.2. Имитация возможных атак» ($Operation_2^{Stage\ 4}$) имеет следующую запись:

$$\bigcup_a Rate_a = \\ = Operation_2^{Stage\ 4}\left(Model^{IFGO}, \bigcup_t State'_{0+t}\right),$$

где $State'_{0+t}$ – предсказанное состояние, в котором может оказаться объект в момент времени t после текущего (в данном случае значение «0+t» как раз и указывает на последующий момент времени); $Rate_a$ – степень реализации атаки [12], исходя из переходов между состояниями в Модели_ИНГО, хронологии предыдущих и предсказанных будущих состояний.

Операция «4.3. Оценка общей безопасности объекта» ($Operation_3^{Stage\ 4}$) имеет следующую запись:

$$Metric = \\ = Operation_3^{Stage\ 4}\left(Model^{IFGO}, \bigcup_a Rate_a\right),$$

где $Metric$ – метрика безопасности, характеризующая текущее и прогнозируемое состояния объекта, исходя из Модели_ИНГО и вычисленных степеней реализации атак.

Модель обнаружения атак

Согласно приведенным аналитическим выражениям всех операций этапов, а также получаемых в процессе их работы данных, аналитическую модель обнаружения атак [13] можно записать следующим образом:

$$\begin{cases} Model^{IFGO} \equiv \\ \equiv \left\langle Graph^{CBS} \middle| \bigcup_i Classificator_i^{NextState} \middle| \bigcup_t^T State_{-t} \right\rangle \\ Graph^{CBS} \equiv \\ \equiv \left\langle Graph^{FBS} \middle| \bigcup_i Classificator_i^{CurrentState} \right\rangle \\ Graph^{FBS} \equiv \left\langle \bigcup_s State_s \middle| \bigcup_l Link_l \middle| \bigcup_m Mark_m \right\rangle \\ State_s \in ID \\ Link \in \langle State_{From} | State_{To} \rangle \\ Mark_m \in (Scenario^{Normal}, Scenario^{Attack}) \end{cases}$$

При этом $Graph^{FBS}$ получается из $Graph^{CSS}$ путем кластеризации, а $Graph^{CSS}$ через ряд тривиальных операций строится из информации об объекте, собранной для всех сценариев его функционирования (такая логика получения данных посредством операций показана с помощью символа «$\Leftarrow$»):

$$Graph^{FBS} \Leftarrow Graph^{CSS} \Leftarrow Information_i \\ \Leftarrow Characteristic_{i,j} \Leftarrow Object.$$

Способ обнаружения атак с использованием данной модели можно записать аналогичным образом:

$$Rate_a, Metric \Leftarrow Model^{IFGO}, State_0.$$

Детализация процесса обработки данных

Детализация процесса обработки входных и получения выходных данных каждой из операций Метода (см. [1], рисунок 1) представлены в таблице 1. Так, в ней каждая строка соответствует одной операции, а в столбцах содержатся следующие элементы: в 1-м – входные данные, во 2-м – выходные данные, в 3-м – название операции, а 4-м – специфика операции (в случае ее наличия). Также, для сокращения записи данных (как входных, так и выходных) введены условные обозначения вида «Д_N»; при этом, при первом появлении название данных будем указывать полностью, при последующих – только обозначение. Таким образом, таблица представляет собой описание интерфейсов, как внешних (т.е. между Методом и информационным окружением, что может быть востребовано при встраивании метода в общее архитектурное решение), так и внутренних (т.е. между собственными модулями, что позволит обоснованно выбирать их реализации).

Методика управления процессом обнаружения

Несмотря на достаточную абстрактность и автоматичность (в смысле отсутствия прямой необходимости участия человека) выполнения как схемы Метода, так и аналитического алгоритма, соответствующий им процесс обнаружения атак требует определенного контроля и настройки своих параметров. Таким образом, для практического применения предложенного научно-методологического аппарата потребуется соответствующая *методика управления процессом обнаружения*, заключающаяся в экспертных настройках следующих операций (как элементов на схеме Метода, см. [1], рисунок 1):

Таблица 1

Детализация процесса обработки данных в методе

Входные данные	Выходные данные	Название операция	Специфика операции
Этап 1. Анализ данных			
Д_1. Информация об объекте с датчиков (для каждого сценария в режиме обучения)	Д_2. Характеристики объекта (для каждого сценария)	1.1. Определение характеристик объекта	Требует экспертной настройки
Д_2	Д_3. Граф частных сценариев поведения (для каждого сценария)	1.2. Анализ изменений характеристик объекта	
Этап 2. Построение модели			
Д_3	Д_4. Граф последовательных наборов характеристик	2.1. Построение единого графа	Требует экспертной настройки
Д_4	Д_5. Граф нечетких состояний поведения	2.2. Кластеризация узлов графов	Применяется МО
Д_5	Д_6. Граф классифицируемых состояний поведения	2.3. Построение классификаторов состояний	Применяется МО, требует экспертной настройки
Д_6	Д_7. Интеллектуальная нечетко графо-ориентированная модель	2.4. Построение классификаторов перехода между состояниями	Требует экспертной настройки
Этап 3. Графо-ориентированное моделирование			
Д_7. Информация об объекте с датчиков (в режиме реального времени)	Д_8. Характеристики объекта	3.1. Определение характеристик объекта	
Д_8	Д_9. Состояние объекта (текущее)	3.2. Классификация состояниями объекта	Применяется МО
Д_9, Д_10. Хронология состояний объекта (предыдущая)	Д_10. (новая)	3.3. Актуализация состояния объекта	
Д_7, Д_9	Д_7	3.4. Обновление статистики предыдущих состояний	
Этап 4. Имитационное моделирование			
Д_7, Д_9	Д_10. Будущие состояния объекта (предсказанные)	4.1. Определение перехода на следующее состояние	Применяется МО
Д_7, Д_10	Д_11. Степень реализации атак	4.2. Имитация возможных атак	Требует экспертной настройки
Д_11	Д_12. Метрика безопасности объекта	4.3. Оценка общей безопасности объекта	Требует экспертной настройки

— для Операции 1.1 необходимо специализировать характеристики, согласно которым будет строиться состояние объекта (например, выбор лишь определенного набора датчиков);
— для Операции 2.2 может потребоваться ручная модификация единого Графа_НСП (например, путем объединения, разделения, добавления, удаления кластеров, а также редактирования составляющих их точек) для учета специфики предметной области объекта и особенностей процесса функционирования объекта (например, деление кластеров, связанных с наиболее критичными атакующими воздействиями, на более мелкие группы);
— для Операции 2.3 требуется выбор алгоритма классификации состояний по набору характеристик, а также указание его характеристик (например, SVM или дерево решений [14]);
— для Операции 2.4, аналогично Операции 2.3 требуется выбор алгоритма и параметров классификатора предсказания новых состояний (например, топологии рекуррентной нейронной сети);
— для Операции 4.2 необходимо установить параметры имитации возможных атак (например, глубина предсказания или возможность пропуска некоторых состояний в рамках одной атаки);
— для Операции 4.4 возможно потребуется указание формул для вычисления различных интегральных показателей безопасности функционирования объекта (например, экспертный выбор весовых коэффициентов атак согласно их критичности для объекта).

Гипотетический эксперимент

Как альтернативу аналитического алгоритма (обосновывающего работоспособность Метода с теоретической точки зрения), проведем гипотетический эксперимент, который наглядно покажет основные этапы и операции обнаружения атак (что также подтвердит работу Метода, но уже с практической точки зрения) [15].

Для проведения эксперимента воспользуемся описанным ранее сквозным примером – детектированием сетевых соединений с узлом для определения атаки, указывая на каждом этапе и для каждой операции Метода примеры обрабатываемых данных, представляя их, по возможности, в графическом виде. В качестве информации об объекте используются показатели датчиков трафика в виде количества сетевых соединений – N, указанных в условных единицах (например, количество соединений за промежуток времени между моментами измерений). Дополнительно, для упрощения, будем считать, что изначально есть информация лишь о двух сценариях поведения сетевого трафика на узле – «нормальном» (помеченным верхним индексом *N* от англ. *Normal*) и «под атаки» (помеченным верхним индексом *A* от англ. *Attack*). Также, информация о количестве соединений с узлом будет получена в четыре момента времени – $t_i, где\ 1 \le i \le 4$.

Этап 1. Анализ данных

На данном этапе строятся Графы_ЧСП, отражающие в аспекте сквозного примера все возможные изменения количества соединений с узлом для всех сценариев.

После выполнения Операции 1.1 будут получены характеристики сетевого трафика, т.е. исходные данные для построения Графа_ЧСП. Используя выбранные условия проведения эксперимента, для простоты и определенности возьмем следующие наборы характеристик (для каждого из сценариев – нормального и под атакой), представленные в таблице 2.

Таблица 2

Количество сетевых соединений (для сквозного примера)

Сценарий	t_1	t_2	t_3	t_4
Нормальный	10	6	4	6
Под атакой	1	4	6	10

Следуя таблице 2, при нормальном сценарии происходит постепенное снижение количества соединений, за которым следует повышение. В случае же сценария под атакой происходит постепенное повышение количества соединений. Отметим, что в одинаковые моменты изменения значения характеристик у двух сценариев не совпадают; данное замечание будет иметь важное значение для результатов операций следующего этапа.

В процессе выполнения Операции 1.2 характеристики объекта для всех сценариев и моментов времени (т.е. значения в таблице 2) будут проанализированы, в результате построятся Графы_ЧСП. Графическая интерпретация таких графов представлена на рисунке 2.

Визуальное отображение графов (см. рисунок 2) наглядно отражает динамику изменения числа сетевых соединений – для сценария под атакой она возрастающая.

Этап 2. Построение модели

На данном этапе будет построена Модель_ИНГО, отражающая в аспекте сквозного примера состояния

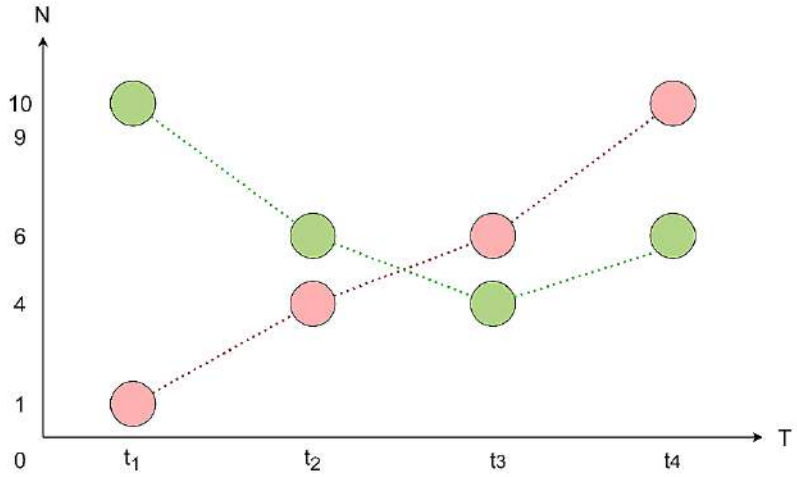

Рисунок 2. Графы частных сценариев поведения (для сквозного примера)

Примечание. На рисунке зеленым фоном отмечены узлы и их переходы для нормального сценария, а красным – под атакой.

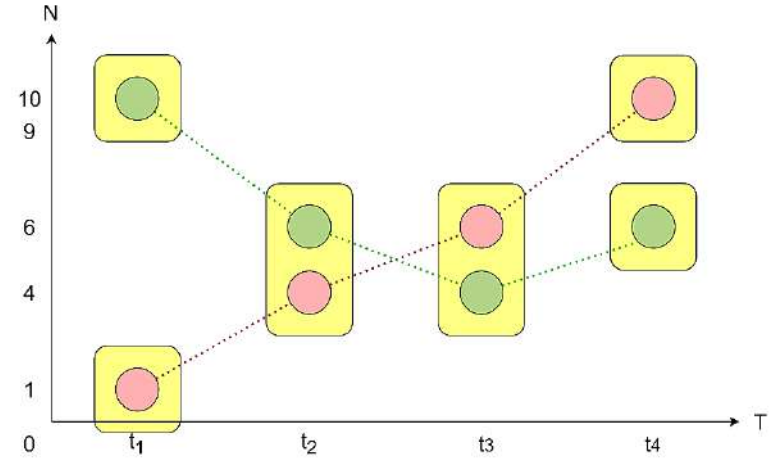

Рисунок 3 – Выделение кластеров узлов единого графа (для сквозного примера)

Примечание. На рисунке желтым фоном отмечены кластеры из близких узлов.

сетевого трафика (с позиции количества соединений с узлом) в отчетные временные точки.

При выполнении Операции 2.1 происходит построение единого Граф_ПНХ из всех Графов_ЧСП. Для текущего примера новый граф не будет отличаться от совокупности предыдущих, поскольку графы для разных сценариев не имеют общих узлов. Однако, после Операции 2.2 близкие узлы будут объединены в кластеры, как показано на рисунке 3; для отдельно стоящих узлов будут также построены кластеры.

Как результат, будет построен новый Граф_НСП, представленный на рисунке 4, в котором узлы сформированы не на основании имеющихся ранее характеристик сетевого трафика, а путем выделения из них (с помощью процесса кластеризации) новых сущностей – состояний (далее – Состояние) объекта исследования.

Как хорошо видно по рисунку 4, совокупность узлов и связей представляет собой классический граф, отражающий возможные последовательности поведения объекта при нормальном сценарии или под атакой. При этом, даже для неидентичных, но близких значений характеристик объект будет находиться в одном состоянии (таком, как 1.1, 1.2, 4.1 и 4.2). Также для каждого состояния можно указать его принадлежность к одному из рассматриваемых сценариев; на-

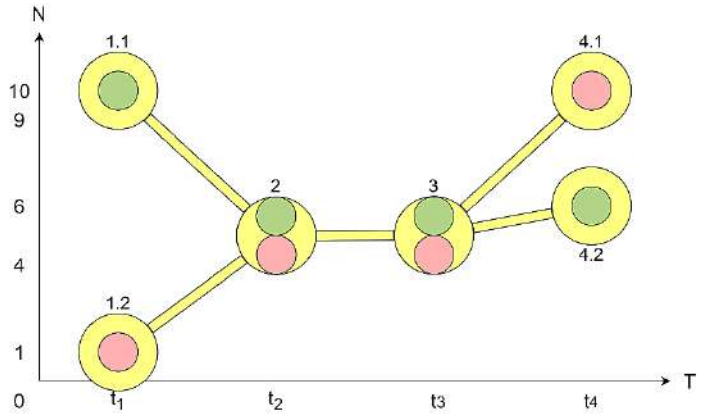

Рисунок 4. Графы нечетких состояний поведения (для сквозного примера)

Примечание. На рисунке желтым фоном обозначены узлы нового типа – состояний; номер у такого узла означает идентификатор состояния. Круги зеленого и красного фона внутри желтых кругов обозначают принадлежность состояния к одному из двух сценариев – нормальному или под атакой.

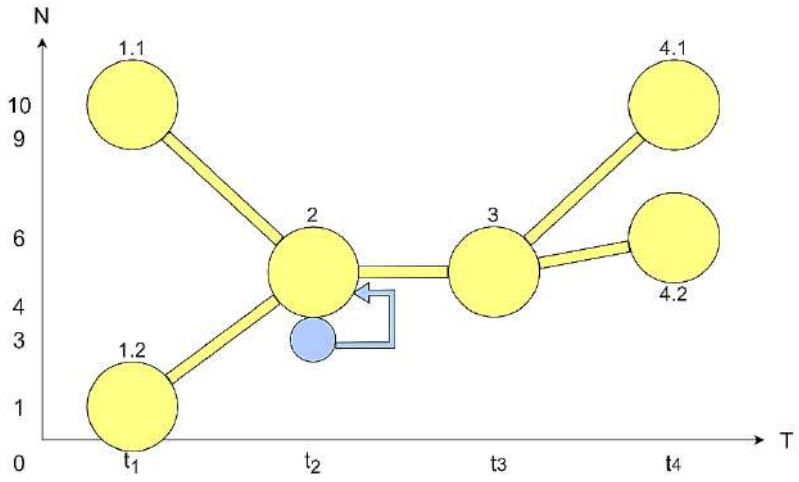

Рисунок 5. Графы классифицируемых состояний поведения (для сквозного примера)

Примечание. На рисунке синим фоном обозначен новый набор характеристик объекта, состояние которого необходимо классифицировать. Стрелка с синим фоном показывает результат классификации.

пример, Состояния 1.1 и 4.2 соответствуют нормальному сценарию, Состояния 1.2 и 4.1 – сценарию под атакой, а Состояния 2 и 4 – могут быть отнесены к обоим сценариям. При этом можно заключить, что сценарию нормального поведения соответствует следующая последовательность изменений состояний – «1.1 → 2 → 3 → 4.2», а сценарию под атакой – «1.2 → 2 → 3 → 4.1».

Поскольку в процессе функционирования объект (т.е. сетевой трафик в примере) может иметь характеристики, отличные от обнаруженных в сценариях, то необходимо уметь также его относить к одному из состояний – для этого предназначена Операция 2.3, в процессе которой для каждого состояния (узла Графа_НСП) строится соответствующий классификатор. Так, например, Состояние 2 было получено из двух наборов данных в момент времени t_2: $N = 6$ для нормального сценария и $N = 4$ для сценария под атакой. И если количество сетевых соединений с узлом будет $N = 3$, то объект в результате классификации отнесется к Состоянию 2. Графическое представление описанной классификации представлено на рисунке 5.

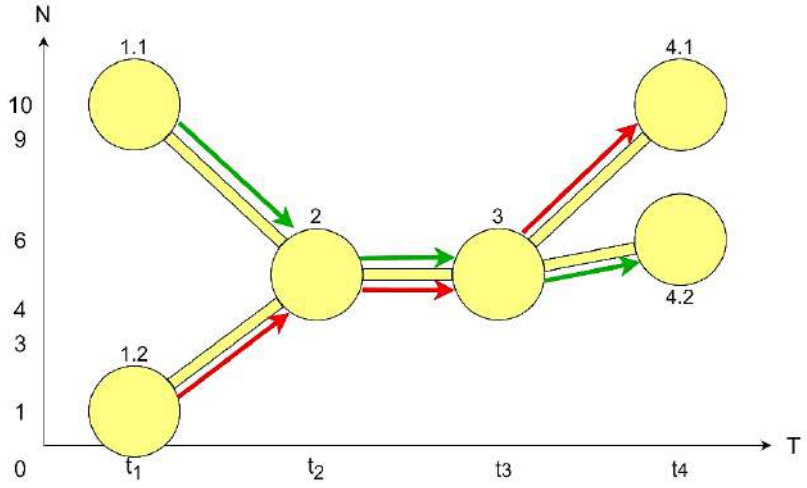

Рисунок 6. Графы классифицируемых состояний поведения (для сквозного примера)

Примечание. На рисунке зеленые стрелки обозначают переходы между состояниями в нормальном сценарии, а красные – под атакой.

После добавления классификаторов в Граф_НСП и их обучения на имеющих наборах данных, он логично перейдет в Граф_КСП.

Аналогично предыдущей операции, в процессе выполнения Операции 2.4. для каждого узла-состояния будут построены классификаторы, предсказывающие последующие состояния по набору предыдущих. Например, хотя из Состояния 3 объект может перейти как в Состояние 4.1, так и в Состояние 4.2, однако на наиболее вероятный переход будет влиять история изменения состояний – т.е. для сквозного примера то, в каком состоянии объект находился в момент времени t_1. Графическое представление такой классификации представлено на рисунке 6.

После добавления классификаторов в Граф_КСП будет получен итоговый граф первых двух этапов Метода, представляющий собой также отдельную Модель_ИНГО.

Этап 3. Графо-ориентированное моделирование

На данном этапе в аспекте сквозного примера по мере получения информации о соединениях с узлом будет определяться состояние сетевого трафика с обновлением Модель_ИНГО в части предсказания будущих состояний.

В процессе функционирования сети – т.е. в режиме реального времени – с помощью Операции 3.1 будут получаться наборы характеристик, включающих в себя количество соединений с узлом. Предположим, что для первых 3 отсчетных точек времени они следующие:

$$\begin{cases} t_1 : N = 3 \\ t_2 : N = 5. \\ t_3 : N = 5 \end{cases}$$

После каждого выполнения Операции 3.1., следующая за ней Операция 3.2 путем классификации по Графу_КСП, входящему в Модель_ИНГО, определит новые состояния сети. Графическое представление такой классификации представлено на рисунке 7.

Согласно результатам работы Операций 3.1 и 3.2 (см. рисунок 7), сетевой трафик будет переходить между следующими Состояниями: 1.2 → 2 → 3. Эти состояния сохраняются в истории с помощью Операции 3.3, имеющей таким образом номинальное значение. А поскольку получены новые статистические данные касательно переходов между состояниями, то согласно им Операция 3.4 обновит Модель_ИНГО в части классификации таких переходов.

Этап 4. Имитационное моделирование

На данном этапе в аспекте сквозного примера по мере обновления текущего состояния сетевого трафика будут прогнозироваться его новые состояния, часть из которых может привести к осуществлению атаки на узел. Данный этап работает совместно (т.е. параллельно) с Этапом 3, поскольку при каждом новом переходе объекта в состояние осуществляется попытка предсказания будущего функционирования объекта.

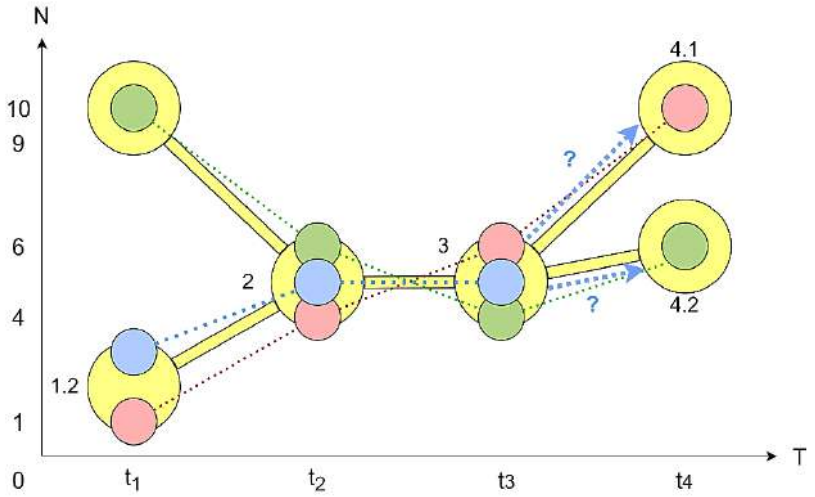

Рисунок 7.Состояния объекта в режиме реального времени (для сквозного примера)

Примечание. На рисунке круги с синим фоном обозначают узлы для характеристик объекта, полученных в режиме реального времени; синие линии показывают историю изменения характеристик. Синие пунктирные стрелки (с знаком «?») показывают возможные переходы объекта в новые состояния.

После выполнения Операции 4.1. предскажется следующее состояние сетевого трафика, используя историю изменения состояний, актуализируемую в Модели_ИНГО Операцией 3.3. Так, в тот момент, когда количество состояний сетевого трафика станет равным 3, Операция 4.1 должна будет выбрать следующее состояние среди двух – 4.1 и 4.2. И как хорошо видно по рисунку 7, от дальнейшего выбора будет зависеть и предсказание сценария, по которому пойдет функционирование объекта: для Состояния 4.1 количество сетевых соединений N станет равным 10, что соответствует наличию атаки на узел; для Состояния 4.2 – равным 6, что будет означать нормальное (т.е. безопасное) функционирование сети. Таким образом, используя историю изменения состояний для текущего примера, будет предсказано Состояние 4.1 – выполнится сценарий под атакой.

Операция 4.2, используя данные об истории и предсказаниях количества соединений с узлами, вычислит степень реализации каждой из атак на узел. Для данного примера операция определит, что атака на узел состоится при переходе объекта в следующее состояние. Данная информация позволит принять превентивные меры противодействия.

Операция 4.3 (дополнительно к прогнозированию атак с помощью Операции 4.2) получит некоторую оценку текущей безопасности узла в сети, что может соответствовать степени реализации атаки. Для текущего примера можно вычислить метрику безопасности функционирования сети, состоящую из 2-х следующих: средней степени реализации всех атак и степени прохождения объектом состояний под атакой среди всех состояний. Ввиду единственности атаки первая метрика соответствует результату работы Операции 4.2. Так, если в сценарии под атакой присутствует 4 состояния, а на данный момент сетевой трафик находится в 3-м (по порядку прохождения), то степень реализации составляет $\frac{3}{4} = 0.75\%$. Вторая же метрика аналогичным образом будет равна $\frac{\sum S_A}{\sum S_N + \sum S_A} = \frac{3}{4+4} = 37.5\%$, где $\sum S_N$ – число всех состояний для нормальных сценариев, а $\sum S_A$ – для всех сценариев под атакой.

Основополагающие принципы метода

Поскольку в основе Метода лежали 7 принципов, разработанных авторами в предыдущих исследованиях, укажем, какие из них, в каких аспектах Метода и в какой степени были использованы.

Принцип **единства** – применен полностью, поскольку Граф_КСП (ответственный за оценивание текущего состояния) входит в Модель_ИНГО (производя-

щую прогнозирования последующих состояний).

Принцип **междисциплинарности** – применен полностью, поскольку используются методы МО (в части кластеризации и классификации) и графо-ориентированная модель (все графы Модели_ИНГО).

Принцип **эффективности** – применен полностью, поскольку основные интеллектуальные операции Метода (на базе МО) могут быть соптимизированы путем выбора и подстройки своих алгоритмов с целью повышения необходимых показателей итоговой эффективности.

Принцип **абстрактности** – применен частично, поскольку хотя в данных никак не участвует их специфика, все же требуется наличие эксперта в части первоначальной подстройки алгоритмов работы Метода под особенности функционирования объекта (см. Раздел «Методика управления процессом обнаружения»).

Принцип **тождественности** – применен частично, поскольку, хотя в состояниях Модели_ИНГО явно и не отражены процессы функционирования объектов, однако, исходя из своей схемы, Метод может быть адаптирован и для их оценивания и прогнозирования (например, путем трактовки характеристик объекта не как статических, а как динамических или темпоральных сущностей).

Принцип **адаптации** – применен частично, поскольку Операция 3.4 обновляет статистику нахождения объекта в состояниях, производя тем самым их параметрическую (хотя и не структурную – т.е. с изменением топологии графов) адаптацию к текущим сценариям функционирования.

Принцип **обусловленности** – практически не применен, т.к. характеристики объекта никак не соотносятся с особенностями физического мира, в котором он функционирует (так, в сквозном примере не учитывается специфика сети и пропускных способностей ее каналов, которая должна была бы повлиять на количество и динамику сетевых соединений с узлом).

Таким образом, можно сделать предварительный вывод, что 3 принципа при разработке Метода применены полностью, 3 – частично, а один – практически не использовался. Тем не менее, это лишний раз говорит как о сложности решения задачи оценивания и прогнозирования состояния объектов[3], так и о возможностях по развитию предложенного Метода.

Заключение

Данное исследование явилось продолжением предыдущего авторского [16] в части перехода от теоретических принципов построения инвариантных способов оценивания и прогнозирования СлО к их применению на практике. В работе предложен 4 этапный Метод обнаружения атак на СлО, использующий оценивание текущих и прогнозирование будущих состояний, часть из которых изначально относятся к находящимся под атакой. Метод представлен в схематичном виде, базируется на имитационном и графо-ориентированном моделировании, а также имеет аналитическую запись, подчеркивающую строгость и корректность выполнения. Новизной Метода является существенная минимизация (по сравнению с аналогами) учета в нем специфики предметной области за счёт абстрагирования характеристик состояний и применения методов МО. Теоретическая значимость заключается в развитии научно-методологического аппарата оценивания и прогнозирования состояний объектов различной структуры за счет совместного применения имитационного и графо-ориентированного моделирования. Практическая значимость заключается в возможности непосредственной реализации программного прототипа Метода, который по предварительным оценкам будет иметь достаточную эффективность для применения в реальных системах.

Продолжить исследование предполагается по следующим направлениям. Во-первых, поскольку все же Метод построен не на всех 7 принципах, то потребуется его модификация для учета недостающих аспектов. Во-вторых, практическая значимость Метода позволяет перейти к разработке программной архитектуры и реализации самого прототипа Метода с последующим проведением экспериментов. И, в-третьих, предполагается расширение Метода для решения задач, выходящих за рамки обнаружения атак (например, в сторону оптимизации процессов функционирования СлО [17]). Все эти пути планируется проделать и отразить авторами в своих будущих научных работах.

Работа выполнена при частичной финансовой поддержке бюджетной темы FFZF-2022-0007

3 Голосовский М.С. Модель оценивания погрешностей прогнозирования сроков разработки программного обеспечения // Программные системы и вычислительные методы. 2015. № 3. С. 311-322.

Литература

1. Израилов К.Е., Буйневич М.В. Метод обнаружения атак различного генеза на сложные объекты на основе информации состояния. Часть 1. Предпосылки и схема // Вопросы кибербезопасности. 2023. № 3(55. С. 90-100. DOI: 10.21681/2311-3456-2023-3-90-100
2. Третьяков В.А., Куликов Г.В., Лукьянец Ю.Ф. Принципы построения больших территориально распределенных автоматизированных систем // Российский технологический журнал. 2020. Т. 8. № 1 (33). С. 34-42. DOI: 10.32362/2500-316X-2020-8-1-34-42
3. Щепетов В.В., Никифоров А.В. Алгоритм построения графового представления сценария поведения объекта // Современные технологии в теории и практике программирования сборник материалов конференции (Санкт-Петербург, 26 апреля 2022 года). 2022. – С. 63-64.
4. Коцюруба Е.Р. Использование аппроксимационных способов для анализа неполной навигационной информации // Эксплуатация морского транспорта. 2019. № 4 (93). С. 38-44. DOI: 10.34046/aumsuomt93/7
5. Кудрова Н.А., Рожкова В.Е. Методический аппарат выявления тенденции развития региональных интегрированных структур // Транспортное дело России. 2012. № 6-1. С. 207-209.
6. Баданина Н.Д., Зинченко А.А., Судаков В.А. Ранжирование объектов на основе нечеткой кластеризации // Препринты ИПМ им. М.В. Келдыша. 2022. № 68. С. 1-12. DOI: 10.20948/prepr-2022-68
7. Орешков В.И. Выбор числа кластеров в алгоритме k-средних с использованием энтропии кластерных решений // Вестник Рязанского государственного радиотехнического университета. 2021. № 77. С. 81-92. DOI: 10.21667/1995-4565-2021-77-81-92
8. Клячкин В.Н., Кувайскова Ю.Е., Ломовцева Н.А. Диагностика состояния технического объекта с помощью классификации методами машинного обучения // Программные продукты и системы. 2021. № 4. С. 572-578. DOI: 10.15827/0236-235X.136.572-578
9. Манцеров С.А. Нейронечеткая классификация технических состояний объектов сложной структуры // Информационные технологии. 2023. Т. 29. № 2. С. 91-97. DOI: 10.17587/it.29.91-97
10. Сухопаров М.Е., Семенов В.В., Лебедев И.С. Модель поведения для классификации состояния информационной безопасности автономного объекта // Проблемы информационной безопасности. Компьютерные системы. 2019. № 4. С. 26-34.
11. Добрышин М.М., Закалкин П.В. Модель компьютерной атаки типа «phishing» на локальную компьютерную сеть // Вопросы кибербезопасности. 2021. № 2 (42). С. 17-25. DOI: 10.21681/2311-3456-2021-2-17-25
12. Коцыняк М.А., Лаута О.С., Иванов Д.А. Математическая модель таргетированной компьютерной атаки // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 2. С. 73-81. DOI: 10.24411/2409-5419-2018-10261
13. Галахов Е.М., Собчук В.В. Развитие моделей кибератак в плоскости информационной безопасности предприятия // Телекоммуникационные и информационные технологии. 2019. № 4 (65). С. 12-24.
14. Наврузов Э.Р. О формировании баз прецедентов для решения задач информационной безопасности // Вестник РГГУ. Серия: Информатика. Информационная безопасность. Математика. 2022. № 3. С. 66-84. DOI: 10.28995/2686-679X-2022-3-66-84
15. Сухов А.М., Крупенин А.В., Якунин В.И. Метод оценивания эффективности процессов функционирования системы обнаружения предупреждения и ликвидации последствий компьютерных атак // I-methods. 2021. Т. 13. № 3.
16. Израилов К.Е., Буйневич М.В., Котенко И.В., Десницкий В.А. Оценивание и прогнозирование состояния сложных объектов: применение для информационной безопасности // Вопросы кибербезопасности. 2022. № 6(52). С. 2-21. DOI: 10.21681/2311-3456-2022-6-2-21
17. Борисов А.В., Миллер Г.Б., Стефанович А.И. Управляемые марковские скачкообразные процессы. II. Мониторинг и оптимизация функционирования TCP-соединений // Известия Российской академии наук. Теория и системы управления. 2019. № 1. С. 13-30. DOI: 10.1134/S0002338819010049

DIFFERENT GENESIS ATTACKS TO COMPLEX OBJECTS DETECTING METHOD BASED ON CONDITION INFORMATION. PART 2. ALGORITHM, MODEL AND EXPERIMENT

Izrailov K.E.[4], Buinevich M.V.[5]

4 Izrailov Konstantin Evgenievich, PhD, Docent, Senior Researcher of Laboratory of Computer Security Problems of St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint-Petersburg. ORCHID: https://orcid.org/0000-0002-9412-5693. Scopus Author ID: 56123238800. E-mail: konstantin.izrailov@mail.ru.

5 Buinevich Mikhail Viktorovich, Dr.Sc., Professor, Professor of Dep. Applied Mathematics and Information Technologies of Saint-Petersburg University of State Fire Service of EMERCOM of Russia, Saint-Petersburg. ORCHID: https://orcid.org/0000-0001-8146-0022. Scopus Author ID: 56122749800. E-mail: bmv1958@yandex.ru.

The goal of the study *is to create a method of detecting attacks on complex objects and processes by evaluating and predicting their state; the method is based on 7 principles proposed by the authors earlier; a feature of method is its invariance with respect to the genesis of attacks.*

Research methods: *system analysis, analytical modeling methods, statistical methods and machine learning, software code development for the implementation of estimation and prediction algorithms.*

Result: *proposed method of attack detection on a complex object that uses assessment of current and future prediction states; the description of method is given in schematic and analytical form using a cross-cutting example from information security field; theoretical significance lies in the scientific and methodological apparatus of assessment and prediction development of states different structure objects; the practical significance lies in the possibility of direct implementation of software prototype with potentially high efficiency.*

In the second part of the paper all stages of the method are algorithmized, which allows us to obtain an analytical model of attack detection. A methodology for managing the detection process, developed in the interests of practical application of the proposed scientific and methodological apparatus, is presented. The course of the experiment on the application of the method for a hypothetical example of attacks on a network node is described. The degree of utilization of the 7 principles developed by the authors in previous studies, which form the basis of the methods of estimating and predicting the state of complex objects, is shown.

The scientific novelty *is to create a method of detecting attacks on a complex object (or process), which is based on a fundamentally new approach to the evaluation and prediction of its state, obtained by the authors in previous studies. As a result, this method is applicable to subject area without taking into account its specificity, which in particular is achieved through the use of author's original intellectual fuzzy graph-oriented model. In contrast to the large number of information systems attacks detection methods, this method is described not only in terms of graphical scheme and steps sequence, but also using analytical record of algorithms that allows to apply to it certain mathematical apparatuses (for example, to justify the performance or optimization of individual steps).*

Keywords: *information technology, information security, complex object, complex process, attack detection method, analytical algorithm, experiment.*

References

1. Izrailov K.Ye., Buynevich M.V. Metod obnaruzheniya atak razlichnogo geneza na slozhnyye ob»yekty na osnove informatsii sostoyaniya. Chast' 1 // Voprosy kiberbezopasnosti. 2023. № 3(55). S. 90-100. (in Russian) DOI: 10.21681/2311-3456-2023-3-90-100
2. Tret'yakov V.A., Kulikov G.V., Luk'yanets YU.F. Printsipy postroyeniya bol'shikh territorial'no raspredelennykh avtomatizirovannykh sistem // Rossiyskiy tekhnologicheskiy zhurnal. 2020. T. 8. № 1 (33). S. 34-42. (in Russian) DOI: 10.32362/2500-316X-2020-8-1-34-42
3. Shchepetov V.V., Nikiforov A.V. Algoritm postroyeniya grafovogo predstavleniya stsenariya povedeniya ob»yekta // Sovremennyye tekhnologii v teorii i praktike programmirovaniya sbornik materialov konferentsii (Sankt-Peterburg, 26 aprelya 2022 goda). 2022. – S. 63-64. (in Russian)
4. Kotsyuruba Ye.R. Ispol'zovaniye approksimatsionnykh sposobov dlya analiza nepolnoy navigatsionnoy informatsii // Ekspluatatsiya morskogo transporta. 2019. № 4 (93). S. 38-44. (in Russian) DOI: 10.34046/aumsuomt93/7
5. Kudrova N.A., Rozhkova V.Ye. Metodicheskiy apparat vyyavleniya tendentsii razvitiya regional'nykh integrirovannykh struktur // Transportnoye delo Rossii. 2012. № 6-1. S. 207-209. (in Russian)
6. Badanina N.D., Zinchenko A.A., Sudakov V.A. Ranzhirovaniye ob"yektov na osnove nechetkoy klasterizatsii // Preprinty IPM im. M.V. Keldysha. 2022. № 68. S. 1-12. (in Russian) DOI: 10.20948/prepr-2022-68
7. Oreshkov V.I. Vybor chisla klasterov v algoritme k-srednikh s ispol'zovaniyem entropii klasternykh resheniy // Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta. 2021. № 77. S. 81-92. (in Russian) DOI: 10.21667/1995-4565-2021-77-81-92
8. Klyachkin V.N., Kuvayskova YU.Ye., Lomovtseva N.A. Diagnostika sostoyaniya tekhnicheskogo ob»yekta s pomoshch'yu klassifikatsii metodami mashinnogo obucheniya // Programmnyye produkty i sistemy. 2021. № 4. S. 572-578. (in Russian) DOI: 10.15827/0236-235X.136.572-578
9. Mantserov S.A. Neyronechetkaya klassifikatsiya tekhnicheskikh sostoyaniy ob»yektov slozhnoy struktury // Informatsionnyye tekhnologii. 2023. T. 29. № 2. S. 91-97. (in Russian) DOI: 10.17587/it.29.91-97
10. Sukhoparov M.Ye., Semenov V.V., Lebedev I.S. Model' povedeniya dlya klassifikatsii sostoyaniya informatsionnoy bezopasnosti avtonomnogo ob»yekta // Problemy informatsionnoy bezopasnosti. Komp'yuternyye sistemy. 2019. № 4. S. 26-34. (in Russian)
11. Dobryshin M.M., Zakalkin P.V. Model' komp'yuternoy ataki tipa «phishing» na lokal'nuyu komp'yuternuyu set' // Voprosy kiberbezopasnosti. 2021. № 2 (42). S. 17-25. DOI: 10.21681/2311-3456-2021-2-17-25 (in Russian)

12. Kotsynyak M.A., Lauta O.S., Ivanov D.A. Matematicheskaya model' targetirovannoy komp'yuternoy ataki // Naukoyemkiye tekhnologii v kosmicheskikh issledovaniyakh Zemli. 2019. T. 11. № 2. S. 73-81. (in Russian) DOI: 10.24411/2409-5419-2018-10261
13. Galakhov Ye.M., Sobchuk V.V. Razvitiye modeley kiberatak v ploskosti informatsionnoy bezopasnosti predpriyatiya // Telekommunikatsionnyye i informatsionnyye tekhnologii. 2019. № 4 (65). S. 12-24. (in Russian)
14. Navruzov E.R. O formirovanii baz pretsedentov dlya resheniya zadach informatsionnoy bezopasnosti // Vestnik RGGU. Seriya: Informatika. Informatsionnaya bezopasnost'. Matematika. 2022. № 3. S. 66-84. (in Russian) DOI: 10.28995/2686-679X-2022-3-66-84
15. Sukhov A.M., Krupenin A.V., Yakunin V.I. Metod otsenivaniya effektivnosti protsessov funktsionirovaniya sistemy obnaruzheniya preduprezhdeniya i likvidatsii posledstviy komp'yuternykh atak // I-methods. 2021. T. 13. № 3. (in Russian)
16. Izrailov K.Ye., Buynevich M.V., Kotenko I.V., Desnitskiy V.A. Otsenivaniye i prognozirovaniye sostoyaniya slozhnykh ob»yektov: primeneniye dlya informatsionnoy bezopasnosti // Voprosy kiberbezopasnosti. 2022. № 6(52). S. 2-21. (in Russian) DOI: 10.21681/2311-3456-2022-6-2-21
17. Borisov A.V., Miller G.B., Stefanovich A.I. Upravlyayemyye markovskiye skachkoobraznyye protsessy. II. Monitoring i optimizatsiya funktsionirovaniya TCP-soyedineniy // Izvestiya Rossiy-skoy akademii nauk. Teoriya i sistemy upravleniya. 2019. № 1. S. 13-30. (in Russian) DOI: 10.1134/S0002338819010049