МЕТОД ОБНАРУЖЕНИЯ АТАК РАЗЛИЧНОГО ГЕНЕЗА НА СЛОЖНЫЕ ОБЪЕКТЫ НА ОСНОВЕ ИНФОРМАЦИИ СОСТОЯНИЯ. ЧАСТЬ 1. ПРЕДПОСЫЛКИ И СХЕМА

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.*

В первой части статьи формулируются предпосылки к созданию поэтапного метода обнаружения атак различного генеза на сложные объекты на основе информации состояния. Приводится описание всех этапов метода и базовой логики их выполнения. Поэлементно описывается схема обнаружения атак, представленная в графическом виде.

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:10.21681/2311-3456-2023-3-90-100

Введение

Одной из черт, характеризующих современный мир, стало существенное усложнение его образующих информационных систем, как из-за нетривиальности внутренних структур, так и по причине существенной разнородности циркулирующих в них данных; подобные (под)системы получили название «сложного объекта» (далее – СлО). Так, например, на смену традиционной системе управления городским хозяйством

1 Израилов Константин Евгеньевич, кандидат технических наук, доцент, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 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.

пришла концепция Умного города, предполагающая наличие различных (под)систем [1], каждая из которых реализует собственный функционал и оперирует собственным набором данными. Или же одиночные программы, выполняемые в рамках одной операционной системы, эволюционировали в целые комплексы, выполняемые на различных программных платформах и распределенные в небезопасной глобальной сети (например, Интернет). Как результат, актуализировалась проблема обеспечения корректного функционирования СлО, автоматически повлекшая за собой потребность в решении задачи не только оценивания их текущего состояния, но и прогнозирования будущего поведения. Понимание того, в каком состоянии может оказаться СлО через некоторое время, позволяет (в случае необходимости) принять превентивные меры, не допускающие нарушения функционирования его и связанных с ним процессов [2]. Особо актуально задачи оценивания и прогнозирования стоят в случае, когда СлО подвергается атакам различного генеза (как внешним, так и внутренним или даже инфраструктурным [3]), которые изначально направлены если не на его уничтожение (физическое, информационное или иное), то на реализацию целенаправленных деструктивных воздействий. Сложность же полноценного (с научно-практической точки зрения) решения задачи, в том числе, заключается в узкоспециализированности применяемых подходов, не подходящих для всего многообразия СлО. Результатом разрешения этого противоречия, описанного в предыдущей авторской статье [4], стали 7 принципов, которые как раз и могут лежать в основе способов, решающих данную задачу. Продолжая данное исследование, авторами далее будет предложен метод обнаружения атак на СлО, построенный на этих принципах (далее – Метод), а также проведена его проверка с помощью гипотетического эксперимента. Успешность последнего, в частности, позволит говорить о практической обоснованности использования декларированных принципов.

Принципы в основе способа оценивания и прогнозирования

Приведем здесь названия и определения вышеупомянутых принципов, используя которые, возможно построение инвариантных способов оценивания и прогнозирования состояния СлО (а также его процессов, которые рассматриваются, как расширенная интерпретация состояний). Под инвариантностью в данном случае понимается независимость способа от предметной области – т.е. одинаковость его работы для объектов любой природы (физической[3], информационной[4], социальной[5] и т.п.).

1) Принцип ***единства*** – «Процессы оценивания и прогнозирования должны представлять части единого процесса, который может быть обобщенно назван *моделированием состояния СлО*) и (или) оценки ситуационной осведомленности о СлО. В основе же процессов должна лежать общая модель».

2) Принцип ***междисциплинарности*** – «Математический инструментарий процессов оценивания и прогнозирования не обязан строиться исключительно на машинном обучении или другом частном подходе, а должен применять несколько методов и междисциплинарный подход».

3) Принцип ***эффективности*** – «При создании моделей и методов оценивания и прогнозирования состояния СлО должны быть учтены возможности по повышению эффективности процедур – улучшение результативности, снижение времени работы, экономия ресурсов».

4) Принцип ***абстрактности*** – «Модели и методы оценивания и прогнозирования состояния СлО должны строиться на абстрактных данных, но с возможностью формирования решений, учитывающих специфику любой требуемой предметной области».

5) Принцип ***тождественности*** – «Сложный процесс можно рассматривать, как последовательность состояний СлО, и применять к нему тождественные методы оценивания и прогнозирования».

6) Принцип ***адаптации*** – «В условиях недостаточности и неопределенности данных должна происходить адаптация состояний в процессе анализа новых значений характеристик СлО».

7) Принцип ***обусловленности*** – «Выбор формы характеристик СлО, а также их содержимого и допустимых границ, должен основываться на закономерностях среды (как правило, всего физического мира), в котором данный СлО функционирует».

И хотя, помимо самих принципов, авторами в [4] также был предложен и основанный на них гипотети-

3 Баранов Г.В. Основные множества физического разнообразия природы // Бюллетень науки и практики. 2016. № 11 (12). С. 321-327.

4 Израилов К.Е., Покусов В.В., Столярова Е.С. Информационные объекты в системе обеспечения информационной безопасности // Теоретические и прикладные вопросы комплексной безопасности: материалы I Международной научно-практической конференции. Петровская академия наук и искусств (Санкт-Петербург, 28 марта 2018 г.). 2018. С. 166-169.

5 Тулупьева Т.В., Абрамов М.В., Тулупьев А.Л. Цифровая культура: социальные сети и социоинженерные атаки // Психологическое здоровье и технологии здоровьесбережения в современной образовательной среде: коллективная монография. Санкт-Петербург: ООО «НИЦ АРТ», 2019. С. 322-346.

ческий способ оценивания и прогнозирования, тем не менее, реализация полноценного метода является достаточно сложной научно-практической задачей. Поэтому далее будет произведена попытка создания Метода, который хоть и в разной степени, но использовал бы все 7 принципов, и при этом мог бы применяться для обнаружения атак на СлО. После описания Метода и проведения на нем эксперимента (пока гипотетического), будет обосновано, какие принципы и в каких частях Метода нашли свое отражение.

Предпосылки к созданию Метода

Исходя из сформулированных ранее принципов, авторского опыта и специфики предметной области (не в части объекта, а в части предмета исследования – в виде необходимости противодействия атакам), а также типичных способов описания СлО и процессов его функционирования, Метод может строиться согласно следующим предпосылкам:

- необходимо обнаруживать атаки различного генеза (информационного, социального, физического и др.), которым подвержен объект; в ином случае метод рискует потерять важнейшее свойство «абстрактности», заключающееся в единстве функционирования при гетерогенности данных;
- об объекте есть информация, описывающая детали его функционирования при различных сценариях; такая информация должна присутствовать для предсказания будущего поведения СлО;
- для имеющихся сценариев указано наличие в них атак (т.е. принадлежность соответствующей контекстной категории); это позволит предсказывать не только поведение СлО, но и уровень его подверженности опасности;
- количество характеристик объекта может быть огромным; что следует из введённого определения СлО;
- значения характеристик объекта может иметь существенный разброс; что соответствует современным реалиям функционирования СлО [5];
- объект в моменты времени с близкими, но несовпадающими характеристиками логически может находиться в одном и том же состоянии; что отражает реальность функционирования СлО, когда имеет место погрешность измерения или интерпретации значений;
- предсказание будущих состояний возможно производить на основании текущего и предыдущих состояний, а также собранной статистики функционирования объекта; что многократно обосновано исследованиями других ученых в данной предметной области [6];
- должна быть возможность подстройки процесса обнаружения атак; что на первых этапах позволит произвести экспертную оценку и доработку Метода;
- Метод (или его отдельные этапы) должны работать в режиме реального времени; что позволит применять Метод в реальных системах для обеспечения безопасности критических систем;
- для обнаружения атак целесообразно применять имитационное и графо-ориентированное моделирование; такие техники являются одними из ведущих для решения задач выявления атак, что говорит об их эффективности.

Здесь и далее будет использован следующий терминологический тезаурус:

1) Объект (исследования) – СлО, представляющая собой систему, исследуемую на предмет обнаружения атак (например, локальная, но с выходом в глобальную, сеть организации).

2) Информация (об объекте) – информация, содержащая необходимые детали функционирования объекта (например, соединения между сетевыми узлами).

3) Характеристики (объекта) – информация об объекте, формализованная в вид, подходящий для аналитической обработки (например, совокупность пар «*Характеристика : Значение*», соответствующая количеству сетевых соединений с определенным узлом).

4) Процесс функционирования (объекта) – последовательность изменений характеристик объекта.

5) Сценарий поведения (объекта) – процесс функционирования объекта в некотором временном диапазоне, относящийся к определенной контекстной категории (например, функционирование сети без или при наличии атак).

6) Состояние (объекта) – момент функционирования объекта, когда его характеристики имеют близкие по некоторому критерию значения [7].

Отметим, что понятия (за исключением названий некоторых терминов) полностью сочетаются с аналогичными, использованными в предыдущей авторской статье [4, см. Рис. 1. Онтологическая модель предметной области].

Метод обнаружения атак

Исходя из сделанных выше предпосылок к созданию Метода, суть его работы состоит в следующем.

Во-первых, собирается информация о процессах функционирования объекта для всех сценариев.

Во-вторых, для информации указывается маркер, относящий ее к сценарию при наличии атак.

В-третьих, по собранной информации строится граф изменения характеристик объекта. При этом чтобы близкие наборы характеристик считались одним состоянием объекта, применяется машинное обучение (далее – МО) в части кластеризации [8].

В-четвертых, для последующего определения уже существующих состояний объекта по новой информации о нем также применяется МО, но уже в части классификации [8]. Как результат, строится специальная модель классификации и предсказания, оперирующая нечеткими состояниями объекта, а также содержащая информацию о проведенных ранее атаках.

В-пятых, в режиме реального времени, используя полученную модель, определяется текущее состояние объекта, а также сохраняется хронология изменения предыдущих. При этом происходит обновление построенной модели для корректировки предсказания новых состояний.

В-шестых, в режиме реального времени, используя полученную модель, предсказываются будущие состояния объекта на основании текущего и предыдущих.

И, в-седьмых, оценивается текущая степень реализации угроз, а также общая метрика безопасности функционирования объекта.

Используя указанные предпосылки, предлагаемый Метод может быть разбит на 4 этапа, первые два из которых являются подготовительными (для обработки имеющейся информации об объекте и построения модели классификации и предсказания его состояний), третий предназначен для определения состояния объекта исследования, а четвертый – предсказания будущих состояний; такой набор этапов позволит как обнаруживать атаки (включая еще не завершенные), так и давать общую оценку безопасности объекту исследования.

Ниже приводится описание всех этапов Метода и базовой логики их выполнения.

Этап 1. Анализ данных

Назначением этапа является анализ информации о функционировании объекта.

Для этого определяется множество наборов характеристик объекта в некоторый момент времени. Затем, из наборов строится их последовательность согласно сценариям, описывающим функционирование объекта во времени. Часть сценариев может отражать небезопасное поведение объекта, что указывается с помощью соответствующего маркера – Нормальный (символ «Н») или под Атакой (символ «А); соответственно, маркер атаки может быть расширен ее типом или идентификатором.

На вход этапа поступает собранная информация о работе объекта (в различных режимах за определенные периоды времени).

На выходе этапа множество сценариев функционирования транспонируется в описание поведения объекта в виде последовательностей наборов его характеристик, что представляет собой «Графы частных сценариев поведения» (далее – Граф_ЧСП), имеющих топологию множества последовательных отрезков.

Этап 2. Построение модели

Назначением этапа является построение графо-ориентированной модели [9], позволяющей также проводить имитационное моделирование.

Для этого из списка Графов_ЧСП путем их объединения строится общий граф, представляющий собой последовательность изменений характеристик объекта согласно множеству сценариев. Очевидно, что полное совпадение характеристик встречается редко, и топология такого графа в основном будет представлять собой множество несоединенных последовательностей отрезков; хотя часть таких подграфов, имеющих одинаковые наборы характеристик, будет пересекаться и иметь более сложные структуры. Итоговая система наборов характеристик со связями может быть названа «Графом последовательных наборов характеристик» (далее – Граф_ПНХ).

Для уменьшения количества узлов в Графе_ПНХ производится оптимизация его представления путем следующей пошаговой процедуры абстрагирования набора характеристик в состояния объекта.

Шаг 1. С помощью МО в части кластеризации выделяются группы узлов с близкими наборами характеристик.

Шаг 2. Полученные наборы заменяются на отдельные сущности – «состояния объекта», что приводит, в том числе, к «склеиванию» некоторых Подграфов_ПНХ.

Шаг 3. Соединения отдельных наборов характеристик, оказавшихся в результате кластеризации в одном состоянии, заменяются на соединения между состояниями; число новых соединений, очевидно, будет в большинстве случаев меньше исходного, что, в том

DOI:10.21681/2311-3456-2023-3-90-100

числе, определяется настройками кластеризации (его алгоритмом, заданным числом групп и т.п.).

Граф, полученный на последнем шаге, приобретает свойство «нечеткости»[6],[7],[8], которое в данном случае означает следующее. В процессе функционирования объект будет иметь различные, близкие друг к другу, наборы характеристик (например, при плавном течении процесса из 0-й точки отсчёта, или при его приближении к предыдущим значениям), что, однако, на графе отобразится как один узел. Следовательно, состояние объекта будет соответствовать целому набору близлежащих (в фазовом пространстве[9], в рамках одного кластера) характеристик; а значит, одно состояние графа будет определять конкретную точку процесса функционирования объекта лишь примерно, или «нечетко». Полученный промежуточный граф может именоваться как «Граф нечетких состояний поведения» (далее – Граф_НСП).

Затем, для определения принадлежности новых наборов характеристик объекта к состояниям Граф_НСП (например, в процессе моделирования в режиме реального времени) производится процесс настройки классификаторов, расположенных в каждом из новых узлов графа – т.е. в состояниях объекта. Так, классификатор по некоторому набору характеристик и на основании ранее проведенной кластеризации сможет отнести объект к соответствующему состоянию. Полученный промежуточный граф может именоваться как «Граф классифицируемых состояний поведения» (далее – Граф_КСП).

Также на основании многочисленной хронологии переходов между состояниями объекта можно спрогнозировать (естественно, с некоторой вероятностью) его следующее состояние. Хотя для решения такой задачи классически применяется МО в части регрессии, однако данный подход использовать не удастся, поскольку возможные будущие состояния уже определены и требуется произвести выбор среди них. Поэтому для определения следующего состояния по текущему (и набору предыдущих) можно воспользоваться классификаторами, расположенными в каждом узле Граф_КСП (т.е., аналогично классификаторам для Графа_НСП). Таким образом, граф приобретает свойство «интеллектуальности», поскольку он обучается предсказывать будущее функционирование объекта. Полученный граф является полноценной моделью и может именоваться как «Интеллектуальная нечеткая графо-ориентированная модель» (далее – Модель_ИНГО).

Отметим, что поскольку сценарии отмечены маркером нормального поведения или под атакой, то состояния будут иметь такую же отметку.

На вход этапа поступает множество сценариев поведения объекта в виде последовательностей наборов характеристик объекта.

На выходе этапа создается интеллектуальная нечеткая графо-ориентированная модель.

Этап 3. Графо-ориентированное моделирование

Назначением этапа является проведение графо-ориентированного моделирования путем определения состояний объекта в соответствующей модели на основании набора его характеристик.

При этом для определения нового состояния по текущему набору используется первый классификатор, построенный на Этапе 2. Таким образом, объект переходит в новое состояние (отмеченное также маркером нормальности или нахождения под атакой), обновляя тем самым хронологию предыдущих за некоторый промежуток итераций (фрейм).

На вход этапа поступает информация об объекте в текущий момент времени, а также построенная на Этапе 2 Модель_ИНГО.

На выходе этапа обновляется текущее состояние объекта и хронология их изменений.

Этап 4. Имитационное моделирование

Назначением этапа является имитационное моделирование поведения объекта путем прогнозирования его будущих состояний из текущего по соответствующей Модели_ИНГО; что позволяет обнаруживать атаки.

В процессе работы этапа анализируются различные пути возможных изменений состояния объекта, часть из которых на Этапе 2 была помечена, как находящиеся под атакой. Для этих случаев вычисляется степень реализации атаки; например, как доля оставшихся состояний до полного ее завершения. Дополнительно вычисляется интегральная метрика безопасности функционирования объекта на основании степени реализации всех возможных атак [10].

Выбор данного типа модели обосновывается тем, что для прогнозирования будущего поведения анали-

6 Тебуева Ф.Б., Перепелица В.А. Подходы к решению дискретных задач оптимизации на графах с нечеткими весами // Вестник Ставропольского государственного университета. 2010. № 5. С. 5-10.

7 Петрунина Е.В. Нечеткие графы в функционально-логическом моделировании гетерогенных систем // Международный журнал прикладных и фундаментальных исследований. 2012. № 7. С. 78-79.

8 Боженюк А.В. Определение нечеткого множества баз нечеткого темпорального графа // Сборник научных трудов SWorld. 2012. Т. 3. № 4. С. 20-24.

9 Садовников Б.И., Иноземцева Н.Г., Перепёлкин Е.Е. Обобщенное фазовое пространство и консервативные системы // Доклады Академии наук. 2013. Т. 451. № 5. С. 505.

тическое моделирование оказывается неприменимым из-за практической невозможности построения функциональных зависимостей между состояниями, через которые «проходит» объект, подверженный атакам. Это следует из того, что инициатором атаки, как правило, является человек (т.е. злоумышленник или их группа) [11], обладающий недетерминированным поведением (с элементами случайности), обусловленным сложно формализуемыми установленными целями (мотивами) и совершаемыми для их достижения действиями [12]. Для решения подобного рода задач хорошо себя зарекомендовывавшим подходом считается имитационное моделирование, которое может описывать пошаговое поведение объекта способами, отличными от математических закономерностей, и реализуемыми с помощью компьютерных программ. В случае же предсказания состояний объекта имитационное моделирование относится к дискретно-событийному виду, поскольку оперирует не непрерывным, а дискретным течением времени – переходами между состояниями, события которого означают различные наборы характеристик, расположенные в одном кластере. Таким образом, не имея точных математических формул, описывающих поведение объекта, но используя предыдущую статистику переходов между состояниями, можно для текущего набора характеристик с некоторой вероятностью предсказывать будущие состояния (т.е. классифицировать их с позиции МО), часть из которых относятся к находящимся под атакой – это и будет означать *обнаружение атак на основе имитационного моделирования*.

На вход этапа поступает хронология состояний объекта, полученная на Этапе 2, а также Модель_ИНГО, построенная на Этапе 3.

На выходе этапа вычисляется степень реализации атак, а также интегральная метрика безопасности функционирования объекта.

Схема обнаружения атак

Опишем схему обнаружения атак в графическом виде.

Представление схемы

Схема описанных этапов приведена на рисунке 1 с использованием следующих правил. В начале каждого этапа указывается точка входа – с помощью широкой стрелки. Основной частью схемы являются элементы для входных и выходных данных, а также операции по их преобразованию. Для каждой операции в начале названия указаны через точку номер этапа и ее порядковый номер – «*Номер_Этапа.Порядковый_Номер)*». Так, например, на вход Этапа 1, предназначенного для анализа данных, поступает множество данных «Информация об объекте», которое с помощью Операции «1.1. Определение характеристик объекта» преобразуются в «Набор характеристик объекта», а на выходе из Этапа 4 после Операции «4.2. Оценка общей безопасности объекта» вычисляется «Метрика безопасности функционирования объекта» и т.д.

В схеме применяются следующие графические обозначения: элементы прямоугольной формы соответствуют операциям, а параллелограммы с непрямыми углами – обрабатываемым данным; серый фон соответствует названиям этапов, а зеленый – результатам работы операций этапа; непрерывные стрелки показывают ход выполнения этапов, а пунктирные – использование операциями дополнительных данных; пунктирные линии с круглыми концевиками – взаимосвязь данных, где круг на конце указывает факт вхождения в этот элемент данных от другого элемента, не помеченного кругом (например, «Граф нечетких состояний поведения» входит в «Граф классифицируемых состояний поведения», данные «Интеллектуальная нечеткая графо-ориентированная модель» на Этапах 2 и 3 тождественны); круг с синим фоном и символом «Н» означает наличие маркеров нормального поведения объекта, с красным фоном и символом «А» – наличие маркеров функционирования под атакой, а с оранжевым фоном и символами «МО» – применение в операции машинного обучения; символ «человека» означает ручную настройку параметров операции экспертом; «RT» – работа этапа в режиме реального времени (*аббр. от англ.* Real Time, *перевод на русс.* Реальное Время).

Элементы схемы

Опишем элементы этапов, представленные на рисунке 1. При этом, для репрезентативности логики их работы, будем использовать сквозной пример. В качестве последнего возьмем достаточно тривиальную ситуацию (а именно следующую – детектирование сетевых соединений с узлом, по которым возможно определение факта атаки) [13], которая хотя и вряд ли встретится в практике, тем не менее, сможет отразить работу всех операций на схеме Метода, а также получаемых в процессе этого данных. Пример имеет следующие условия и ограничения:

— процесс функционирования объекта происходит по двум следующим сценариям [14]: нормальный – т.е. штатный, при отсутствии атак; атаку-

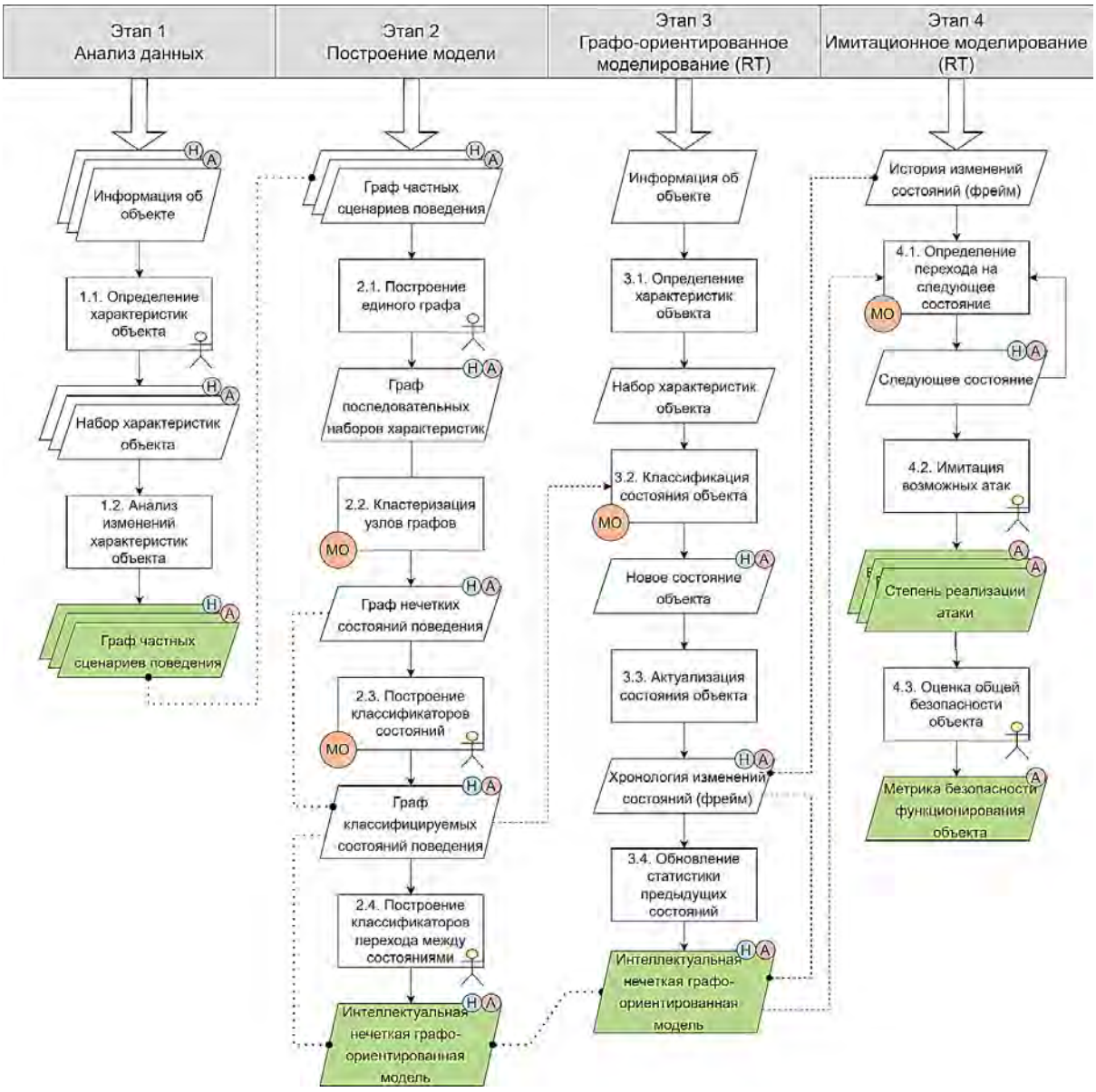

Рис. 1. Схема метода обнаружения в реальном времени атак на основе имитационного и графо-ориентированного моделирования

емый – т.е. находящийся под воздействием атаки, а именно – попытке «взлома» сетевого узла;

— процесс функционирования объекта будет делиться на фазы, идущие друг за другом, о которых собирается информация [15]; фазы описывают сетевой обмен с критически важным узлом[10];

— в качестве информации, описывающей поведение объекта, выбрана только одна характеристика, названная основной, а именно —сетевые соединения с критически важным узлом [16];

— характеристика объекта представляет собой скалярную величину, а именно – количество сетевых соединений с критически важным узлом [17]; следовательно, график сценария поведения объекта может быть представлен в виде плоскости, где ось абсциссы является временем, а ось ординаты – количеством соединений.

Этап 1 содержит следующие элементы:

— Множество данных «Информация об объекте», в которых хранится описание поведения объекта для всех возможных сценариев его функци-

10 Chechulin A.A., Kotenko I.V. Attack tree-based approach for real-time security event processing // Automatic Control and Computer Sciences. 2015. Т. 49. № 8. С. 701-704.

онирования, собранная ранее (например, для режимов нормального и атакуемого сценариев работы);
- Операция «1.1. Определение характеристик объекта», формализующая описание поведения объекта с помощью характеристик; может требовать ручной настройки экспертом;
- Множество данных «Набор характеристик объекта», в которых хранятся последовательности характеристик объекта для разных сценариев функционирования (например, полученный от датчиков массива значений «Сетевые соединения : Число соединений»);
- Операция «1.2. Анализ изменений характеристик объекта», обрабатывающая сценарии функционирования объекта;
- Множество данных «Граф частных сценариев поведения», содержащее набор графов, каждый из которых описывает последовательность изменений характеристик объекта для всех сценариев (т.е. имеет топологию шины или прямой) – в виде совокупности узлов-наборов характеристик и соединений между ними (например, две последовательности сетевых соединений – без атаки и при ее наличии).

Этап 2 содержит следующие элементы:

- Множество данных «Граф частных сценариев поведения», идентичные, полученным в результате выполнения Операции 1.2 (т.е. по завершению работы Этапа 1);
- Операция «2.1. Построение единого графа», которая объединяет набор графов для сценариев функционирования объекта; может требовать ручной настройки экспертом;
- Данные «Граф последовательных наборов характеристик», представляющие итоговый граф с характеристиками объекта для всех сценариев функционирования (например, в виде корневой точки в начальный момент времени, в которой сетевые соединения отсутствуют, из которой выходят два пути – изменение количества соединений для нормального и атакуемого сценариев);
- Операция «2.2. Кластеризация узлов графов», производящая группировку близких точек графа в пространстве характеристик, т.е. объединение в кластеры близких наборов характеристик объекта; следует отметить, что последовательности наборов характеристик при «плавном» течении процесса функционировании объекта автоматически попадут в один кластер, тем самым избавив от необходимости такого рода группировки и/или усреднения на Операции 1.2; для решения задачи кластеризации применяется МО;
- Данные «Граф нечетких состояний поведения», представляющие итоговый граф с состояниями объекта – кластерами близких наборов его характеристик (так, различные фазы процессов функционирования объекта будут иметь пересечения посредством кластеров, например, в момент времени, когда количество сетевых соединений в нормальном и атакуемом сценариях близки);
- Операция «2.3. Построение классификаторов состояний», обучающая классификатор в каждом из узлов графа определению текущего состояния объекта по набору его характеристик; для решения построения моделей классификаторов применяется МО; может требовать ручной настройки экспертом;
- Данные «Граф классифицируемых состояний поведения», представляющие итоговый граф с состояниями – т.е. кластерами близких наборов характеристик (например, некоторые фазы процессов сценариев нормального и атакуемого сценариев будут находиться одном состоянии – иметь общую точку на графе); в эти данные входят предыдущие – «Граф нечетких состояний поведения»;
- Операция «2.4. Построение классификаторов перехода между состояниями», обучающая классификатор в каждом из узлов графа предсказанию следующего состояния объекта по набору предыдущих (включая текущее);
- Данные «Интеллектуальная нечеткая графо-ориентированная модель», представляющие собой итоговую Модель_ИНГО функционирования объекта с нечеткими состояниями и следующим интеллектуальным (на базе МО) функционалом: определение текущего состояния объекта по набору его характеристик и предсказание будущего состояния по набору предыдущих (например, если ранее два набора характеристик со значением количества сетевых соединений объекта для нормального и атакуемого сценариев попали в одно состояние, то другой набор характеристик с близким числом соединений в результате классификации также попадет в это состояние); в эти дан-

ные входят предыдущие – «Граф классифицируемых состояний поведения».

Этап 3 содержит следующие элементы:

- Данные «Информация об объекте», в которых хранится текущее описание объекта (например, информация о сетевых соединениях, получаемая в режиме реального времени);
- Операция «3.1. Определение характеристик объекта», формализующая описание поведения объекта с помощью характеристик;
- Данные «Набор характеристик объекта», в которых хранится набор характеристик объекта в текущий момент времени (т.е. текущее количество сетевых соединений);
- Операция «3.2. Классификация состояния объекта», определяющая с помощью классификатора на базе МО состояние объекта по набору его характеристик;
- Данные «Новое состояние объекта», содержащие текущее определенное состояние объекта (т.е. состояние, в которое перешел объект согласно построенному графу и его обученным классификаторам);
- Операция «3.3. Актуализация состояния объекта», обновляющая набор предыдущих состояний (удаляя наиболее ранее состояние из фрейма ограниченного размера после помещения туда текущего – т.н. способ организации FIFO);
- Данные «Хронология изменений состояний (фрейм)», хранящие все предыдущие состояния объекта в фрейме заданной длины, начиная с текущего (например, количество сетевых соединений за некоторый период времени);
- Операция «3.4. Обновление статистики предыдущих состояний», уточняющая Модели_ИНГО в части предсказания состояний на основе новой статистики нахождения объекта в узлах графа модели (например, если ранее модель предсказывала одинаковую вероятность перехода в два состояния, то после фактического посещения одного из них данный прогноз изменится);
- Данные «Интеллектуальная нечеткая графо-ориентированная модель», идентичные данным, полученным в результате выполнения Операции 2.4 (т.е. по завершению работы Этапа 2).

Этап 4 содержит следующие элементы:

- Данные «Хронология изменений состояний (фрейм)», идентичные данным, полученным в результате выполнения Операции 3.4 (т.е. по завершению работы Этапа 3);
- Операция «4.1. Определение перехода на следующее состояние», прогнозирующая следующее состояние объекта по Модели_ИНГО с применением классификатора на базе МО;
- Данные «Следующее состояние», определяющие состояние объекта в следующий момент времени (так, например, если в предыдущем состоянии объект не находился в атакуемом процессе, а в текущем началась его атака путем повышения количества сетевых соединений с критически важным узлом, то будет спрогнозирована следующая фаза атакуемого процесса);
- Операция «4.2. Имитация возможных атак», определяющая показатели реализации атаки согласно предыдущим и предсказанным состояниями объекта; может потребовать ручной настройки экспертом;
- Множество данных «Степень реализации атаки», хранящих вычисленные параметры реализации каждой из возможных атак для объекта (например, может быть получено, что до полного завершения сетевой осталось пройти 90% фаз);
- Операция «4.3. Оценка общей безопасности объекта», вычисляющая безопасность функционирования объекта для всех возможных атак; может потребовать ручной настройки экспертом;
- Данные «Метрика безопасности функционирования объекта», хранящие интегральный показатель безопасности функционирования объекта (например, может быть получено, что на данный момент происходит реализация 10 сетевых атак, максимальная степень реализации атаки составляет 20%, а средняя вероятность реализации хотя бы одной атаки составляет 5%).

Отметим возможности применения МО для Операций 3.2 и 4.1 (на рисунке 1 соответствующие элементы содержат символы «МО» в оранжевом круге). Для первой операции могут применяться классические модели и методы из области МО, такие, как SVN или Дерево решений, поскольку задача условно сводится к нахождению шара в пространстве характеристик, попадание в который относило бы объект к центральному нечеткому состоянию в центре шара. Для второй операции целесообразно применять рекуррентную нейронную сеть, которая за счет внутренней памяти как раз и ориентирована на работу с последовательностью пространственных цепочек – т.е. с историей предыдущих состояний объекта.

Продолжение следует ...

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

Литература

1. Buinevich M., Izrailov K., Stolyarova E., Vladyko A. Combine method of forecasting VANET cybersecurity for application of high priority way // The proceedings of 20th International Conference on Advanced Communication Technology (Chuncheon, South Korea, 2018). IEEE, 2018. PP. 266-271.
2. Шориков А.Ф. Прогнозирование и минимаксное оценивание состояний производственной системы при наличии рисков // Прикладная информатика. 2022. Т. 17. № 4 (100). С. 97-112. DOI: 10.37791/2687-0649-2022-17-4-97-112
3. Максимова Е.А. Методы выявления и идентификации источников деструктивных воздействий инфраструктурного генеза // Электронный сетевой политематический журнал «Научные труды КубГТУ». 2022. № 2. С. 86-99.
4. 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
5. Балашов О.В., Букачев Д.С. Подход к определению качественных характеристик объектов // Международный журнал информационных технологий и энергоэффективности. 2021. Т. 6. № 4 (22). С. 18-23.
6. Попов С.В. О предсказании событий // Информационные системы и технологии. 2023. № 1 (135). С. 38-45.
7. Кубарев А.В., Лапсарь А.П., Назарян С.А. Параметрическое моделирование состояния объектов критической инфраструктуры в условиях деструктивного воздействия // Вопросы кибербезопасности. 2021. № 3 (43). С. 58-67. DOI: 10.21681/2311-3456-2021-3-58-67
8. Kotenko I., Izrailov K., Buinevich M. Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches // Sensors. 2022. Vol. 22. Iss. 4. PP. 1335. DOI: 10.3390/s22041335
9. Десницкий В.А. Подход к обнаружению атак в реальном времени на основе имитационного и графоориентированного моделирования // Информатизация и связь. 2021. № 7. С. 30-35. DOI: 10.34219/2078-8320-2021-12-7-30-35
10. Лаврова Д.С., Попова Е.А., Штыркина А.А., Штеренберг С.И. Предупреждение DoS-атак путем прогнозирования значений корреляционных параметров сетевого трафика // Проблемы информационной безопасности. Компьютерные системы. 2018. № 3. С. 70-77
11. Ахрамеева К.А., Федосенко М.Ю., Герлинг Е.Ю., Юркин Д.В., Анализ средств обмена скрытыми данными злоумышленниками в сети интернет посредством методов стеганографии // Телекоммуникации. 2020. № 8. С. 14-20.
12. Браницкий А.А., Шарма Яш.Д., Котенко И.В., Федорченко Е.В., Красов А.В., Ушаков И.А., Определение психического состояния пользователей социальной сети REDDIT на основе методов машинного обучения // Информационно-управляющие системы. 2022. № 1 (116). С. 8-18. DOI: 10.31799/1684-8853-2022-1-8-18
13. Израилов К.Е., Обрезков А.И., Курта П.А. Подход к выявлению последовательности одноцелевых сетевых атак с визуализацией их прогресса эксперту // Методы и технические средства обеспечения безопасности информации. 2020. № 29. С. 68-69.
14. Кузьмин В.Н., Менисов А.Б. Исследование путей и способов повышения результативности выявления компьютерных атак на объекты критической информационной инфраструктуры // Информационно-управляющие системы. 2022. № 4 (119). С. 29-43. DOI: 10.31799/1684-8853-2022-4-29-43
15. Захарченко Р.И., Королев И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры функционирующей в киберпространстве // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 52-61. DOI: 10.24411/2409-5419-2018-10041
16. Захаров Н.А., Клепиков В.И., Подхватилин Д.С. Сетевые встраиваемые системы // Автоматизация в промышленности. 2020. № 3. С. 58-61. DOI: 10.25728/avtprom.2020.03.14
17. Степанов Е.П., Смелянский Р.Л. Сравнительный анализ многопоточных транспортных протоколов // Системы и средства информатики. 2022. Т. 32. № 2. С. 155-170. DOI: 10.14357/08696527220215

DIFFERENT GENESIS ATTACKS TO COMPLEX OBJECTS DETECTING METHOD BASED ON CONDITION INFORMATION. PART 1. PREREQUISITES AND SCHEMA

***Izrailov K.E.*[11], *Buinevich M.V.*[12]**

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.*

11 Konstantin E. Izrailov, Ph.D., Docent, Associate Professor of Dep. Secured Communication Systems of The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Senior Researcher of Laboratory of Computer Security Problems of St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint-Petersburg, Russia. ORCHID: https://orcid.org/0000-0002-9412-5693. Scopus Author ID: 56123238800. E-mail: konstantin.izrailov@mail.ru.

12 Mikhail V. Buinevich, 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, Russia. ORCHID: https://orcid.org/0000-0001-8146-0022. Scopus Author ID: 56122749800. E-mail: bmv1958@yandex.ru.

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.*

The first part of the article formulates the prerequisites for creating a step-by-step method for detecting at-tacks of different genesis on complex objects based on state information. The description of all stages of the method and the basic logic of their implementation are given. The attack detection scheme represented in graphical form is described element by element.

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. Buinevich M., Izrailov K., Stolyarova E., Vladyko A. Combine method of forecasting VANET cybersecurity for application of high priority way // Proceedings of the 20th International Conference on Advanced Communication Technology (ICACT, Chuncheon, South Korea, 2018). IEEE, 2018. PP. 266-271. DOI: 10.23919/ICACT.2018.8323720
2. Shorikov A.F. Prognozirovaniye i minimaksnoye otsenivaniye sostoyaniy proizvodstvennoy sistemy pri nalichii riskov // Prikladnaya informatika. 2022. T. 17. № 4 (100). S. 97-112. (in Russian) DOI: 10.37791/2687-0649-2022-17-4-97-112
3. Maksimova Ye.A. Metody vyyavleniya i identifikatsii istochnikov destruktivnykh vozdeystviy infrastrukturnogo geneza // Elektronnyy setevoy politematicheskiy zhurnal «Nauchnyye trudy KubGTU». 2022. № 2. S. 86-99. (in Russian)
4. 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
5. Balashov O.V., Bukachev D.S. Podkhod k opredeleniyu kachestvennykh kharakteristik ob"yektov // Mezhdunarodnyy zhurnal informatsionnykh tekhnologiy i energoeffektivnosti. 2021. T. 6. № 4 (22). S. 18-23. (in Russian)
6. Popov S.V. O predskazanii sobytiy // Informatsionnyye sistemy i tekhnologii. 2023. № 1 (135). S. 38-45. (in Russian)
7. Kubarev A.V., Lapsar' A.P., Nazaryan S.A. Parametricheskoye modelirovaniye sostoyaniya ob"yektov kriticheskoy infrastruktury v usloviyakh destruktivnogo vozdeystviya // Voprosy kiberbezopasnosti. 2021. № 3 (43). S. 58-67. (in Russian) DOI: 10.21681/2311-3456-2021-3-58-67
8. Kotenko I., Izrailov K., Buinevich M. Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches // Sensors. 2022. Vol. 22. Iss. 4. PP. 1335. DOI: 10.3390/s22041335
9. Desnitskiy V.A. Podkhod k obnaruzheniyu atak v real'nom vremeni na osnove imitatsionnogo i grafooriyentirovannogo modelirovaniya // Informatizatsiya i svyaz'. 2021. № 7. S. 30-35. (in Russian) DOI: 10.34219/2078-8320-2021-12-7-30-35
10. Lavrova D.S., Popova Ye.A., Shtyrkina A.A., Shterenberg S.I. Preduprezhdeniye DoS-atak putem prognozirovaniya znacheniy korrelyatsionnykh parametrov setevogo trafika // Problemy informatsionnoy bezopasnosti. Komp'yuternyye sistemy. 2018. № 3. S. 70-77. (in Russian)
11. Akhrameyeva K.A., Fedosenko M.YU., Gerling Ye.YU., Yurkin D.V., Analiz sredstv obmena skrytymi dannymi zloumyshlennikami v seti internet posredstvom metodov steganografii // Telekommunikatsii. 2020. № 8. S. 14-20. (in Russian)
12. Branitskiy A.A., Sharma Yash.D., Kotenko I.V., Fedorchenko Ye.V., Krasov A.V., Ushakov I.A., Opredeleniye psikhicheskogo sostoyaniya pol'zovateley sotsial'noy seti REDDIT na osnove metodov mashinnogo obucheniya // Informatsionno-upravlyayushchiye sistemy. 2022. № 1 (116). S. 8-18. (in Russian) DOI: 10.31799/1684-8853-2022-1-8-18
13. Izrailov K.Ye., Obrezkov A.I., Kurta P.A. Podkhod k vyyavleniyu posledovatel'nosti odnotselevykh setevykh atak s vizualizatsiyey ikh progressa ekspertu // Metody i tekhnicheskiye sredstva obespecheniya bezopasnosti informatsii. 2020. № 29. S. 68-69. (in Russian)
14. Kuz'min V.N., Menisov A.B. Issledovaniye putey i sposobov povysheniya rezul'tativno-sti vyyavleniya komp'yuternykh atak na ob"yekty kriticheskoy informatsionnoy infrastruktury // Informatsionno-upravlyayushchiye sistemy. 2022. № 4 (119). S. 29-43. (in Russian) DOI: 10.31799/1684-8853-2022-4-29-43
15. Zakharchenko R.I., Korolev I.D. Metodika otsenki ustoychivosti funktsionirovaniya ob"yektov kriticheskoy informatsionnoy infrastruktu-ry funktsioniruyushchey v kiberprostranstve // Naukoyemkiye tekhnologii v kosmicheskikh issledovaniyakh Zemli. 2018. T. 10. № 2. S. 52-61. (in Russian) DOI: 10.24411/2409-5419-2018-10041
16. Zakharov N.A., Klepikov V.I., Podkhvatilin D.S. Setevyye vstraivayemyye sistemy // Avtomatizatsiya v promyshlennosti. 2020. № 3. S. 58-61. (in Russian) DOI: 10.25728/avtprom.2020.03.14
17. Stepanov Ye.P., Smelyanskiy R.L. Sravnitel'nyy analiz mnogopotochnykh transportnykh protokolov // Sistemy i sredstva informatiki. 2022. T. 32. № 2. S. 155-170. (in Russian) DOI: 10.14357/08696527220215