УДК 004.056 DOI:10.31854/1813-324X-2020-6-4-91-103

# Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры

**Е.А. Максимова**[1*]

[1]МИРЭА – Российский технологический университет,
Москва, 119454, Российская Федерация
[*]Адрес для переписки: maksimova@mirea.ru

**Информация о статье**
Поступила в редакцию 21.09.2020
Принята к публикации 20.10.2020

**Ссылка для цитирования:** Максимова Е.А. Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры // Труды учебных заведений связи. 2020. Т. 6. № 4. С. 91–103. DOI:10.31854/1813-324X-2020-6-4-91-103

**Аннотация:** *Безопасность субъекта критической информационной инфраструктуры (КИИ) – один из ключевых вопросов его жизнеобеспечения. Существующий в настоящее время подход (нормативно-правовой) регламентирует решения данного вопроса без учета фактора влияния нарушителя, способного деструктивно воздействовать на субъекта КИИ. Это приводит к значительным погрешностям при анализе информационной безопасности субъекта КИИ, следовательно, снижает эффективность декларированных для объектов КИИ средств защиты информации. Целью данной работы является разработка модели нарушителя информационной безопасности (ИБ), представленной в формализованном виде с использованием параметра «потенциал нарушителя» в пространстве реализаций им деструктивных воздействий на объектах КИИ. Предложенная модель оценки возможностей нарушителя по реализации деструктивных воздействий на субъекте КИИ как совокупности объектов реализована в разработанной когнитивной карте «Оценка ИБ субъекта КИИ» для динамического изменения параметров вершины «Злоумышленные действия на объекте КИИ».*

**Ключевые слова:** *нарушитель, субъект, критическая информационная инфраструктура, категория, деструктивные воздействия, модель, когнитивная модель, информационная безопасность.*

## Введение

Особое место в социальной инфраструктуре любого государства занимают объекты критической информационной инфраструктуры (КИИ). Нарушение функционирования таких объектов может иметь разрушающий характер, сопровождаться человеческими жертвами. Поэтому меры по противодействию злоумышленным воздействиям на них должны в полной мере перекрывать угрозы и уязвимости информационной безопасности (ИБ). Прогнозирование злоумышленных воздействий при этом должно быть комплексным и всеобъемлющим по отношению к конкретному объекту.

Одним из ключевых вопросов в процессе прогнозирования злоумышленных воздействий является формирование модели потенциального злоумышленника, способного нанести значительный урон, привести к деструктивным (разрушающим) последствиям. Деструктивные злоумышленные воздействия (ДЗВ) инфраструктурного характера не декларированы, что приводит к погрешности в оценки ИБ объектов КИИ.

## Постановка задачи

В процессе моделирования действий злоумышленника, в качестве основы, например, рассматриваются описательные модели сетей и злоумышленников [1], структурированное описание на базе деревьев [2], объектно-ориентированное дискретное событийное моделирование [3], регулятивное моделирования [4] и др.

Однако, при построении системы защиты субъекта критической информационной инфраструктуры (КИИ) используется алгоритм действий, прописанный в Федеральном законе Российской Федерации от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и не учитывающий «силу» деструктивных воздействий как одного из значимых показателей потенциального нарушителя. Таким образом, целью исследования является построение модели оценки возможностей нарушителей по реализации деструктивных воздействий на объектах КИИ как элемента комплексной, регулятивной мо-

дели оценки информационной безопасности субъекта КИИ. Субъект КИИ при этом в рамках данного исследования рассматривается как совокупность объектов КИИ, являющихся его структурными составляющими

**Анализ методов анализа и оценки деструктивного воздействия на объектах КИИ**

Первое упоминание о модели нарушителя (злоумышленника) в Российской Федерации относится к Руководящему документу Гостехкомиссии России 1992 г. [5]. В нем нормативно устанавливался термин и его пояснение, как «абстрактное описание». На тот момент понятие «действий злоумышленника» рассматривалось в большей степени как какие-либо физические методы воздействия без упоминания технических или программных возможностей. В дальнейшем определение закреплялось и уточнялось в государственных стандартах.

В начале XXI столетия с развитием компьютерных технологий потребовалась корректировка понятия «злоумышленник» и подходов к оценке его возможностей. Серьезным шагом в нормативном закреплении модели злоумышленника стал выход методического документа ФСТЭК России «Методика определения угроз безопасности информации в информационных системах» от 14 февраля 2008 г., и утвержденных в 2015 г. методических рекомендаций ФСБ России «по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах (ИС) персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» [6]. В этих документах регуляторы обозначили последовательные алгоритмы действий при разработке модели злоумышленника.

В силу различий в «зонах ответственности» (ФСБ России – область защиты криптографическими средствами, ФСТЭК России – техническая защита информации), подходы и методы регуляторов отличаются. ФСБ России при описании злоумышленника берет в расчет в основном его воздействие на криптографические средства и среду их функционирования. ФСТЭК России делает упор на атаки на систему в целом.

ФСТЭК России в своей методике разделяет нарушителей на три вида по их потенциалу. Он (потенциал) может быть низким, средним и высоким. Каждый определен своими возможностями и осведомленностью о системе. Например, низкий потенциал показывает, что получение информации и реализация злоумышленных действий может идти только по общедоступным каналам. Средний – имеет доступ к коду используемых программ, может искать уязвимости и пользоваться ими. Высокий – способен самолично вносить НДВ в прикладные программы и использовать спецсредства. У злоумышленников с высоким потенциалом практически неограниченные возможности.

ФСБ России выделяет шесть групп злоумышленников, в зависимости от специфических возможностей к проведению атак. Атаки могут производиться внутри или вне контролируемой зоны. Также к возможностям относится наличие или отсутствие физического доступа к помещениям, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем средств вычислительной техники и возможность найма и привлечения квалифицированных специалистов.

Не смотря на различие в количестве групп злоумышленников в методиках, это деление взаимосвязано и может быть условно соотнесено.

Альтернативные методики и подходы к вопросу, связанному с разработкой модели нарушителя предлагаются рядом ученых. Так, в 2007 г. Бояринцев А.В., Ничиков А.В., Редькин В.Б. при рассмотрении общего подхода к разработке моделей нарушителей [7] описали методологию, предполагающую четыре подхода к данному вопросу. Первым описанным подходом был метод, который назвали «позицией пессимизма», т. е. предполагающей, что злоумышленник максимально подготовлен для реализации угрозы. Второй подход – «позиция оптимизма», согласно которому предположения выдвигаются на основании лучшего из возможных вариантов событий. Третий – «позиция реализма», где эксперты выдвигают наиболее вероятную модель. Четвертый – «позиция оправданного пессимизма», отличающаяся тем, что характеристики злоумышленника не абсолютируются, но и не занижаются.

В 2010 г. Спивак А.И. при описании методики оценки эффективности злоумышленника [8] предложил дополнительный инструмент для описательной части модели нарушителя. В методике было введено понятие величины деструктивного воздействия. Эта величина математически представляла собой приращение вероятности реализации угрозы после воздействия злоумышленника. Введение величины деструктивного воздействия рассматривало новую сторону в вопросе разработки модели злоумышленника. Однако данная величина была актуальна только при условии ограниченности знания или полной неосведомленности о деятельности нарушителя. Это не позволяло применять методику на практике в ряде случаев взаимодействия в реальном времени.

В 2012 г. Жуков В.Г., Жукова М.Н. и Стефаров А.П. при описании модели нарушителя прав доступа в автоматизированных системах [9] предложили методику построения модели злоумышленника, совместившую основные на тот момент сетевые модели OSI/ISO и TCP/IP. Она была основана на классификации уровней воздействия нарушителя. К

этим уровням относились: уровень технических каналов, прикладной уровень стека протоколов TCP/IP, транспортный уровень стека протоколов TCP/IP, сетевой уровень стека протоколов TCP/IP, канальный уровень стека протоколов TCP/IP, физический уровень стека протоколов TCP/IP, уровень вредоносного воздействия, уровень закладных устройств, уровень системы защиты информации. На основании этих уровней предложено семь категорий злоумышленников. На основании уровней воздействия и категорий злоумышленников составлялась таблица актуальных угроз безопасности. Одним из главных плюсов этого подхода является то, что модель учитывала показатель осведомленности нарушителя и его технические средства. Однако представленная модель, в силу жесткого соотношения категория-уровень, не рассматривала возможной взаимосвязи категорий и их совместное действие. Модель позволяла не привлекать специалистов по защите информации на этапе предпроектного обследования, что могло привести к потере из вида специфических угроз.

В 2013 г. Ищейнов В.Я., Чудинов С.М. при оценке риска воздействия на объект информатизации [7] рассматривали математический подход к обоснованию модели злоумышленника с точки зрения аппарата нечетких множеств. Используемая функциональная модель угроз, состоящая из функции источника угроз и функций самих угроз по времени, позволяла в конечном итоге составить поле распределения рисковых показателей, где каждая строка соответствовала конкретной модели, а максимальное значение в строке являлось максимальным риском при действиях конкретного нарушителя. Несомненным плюсом такого подхода являлось прямое вычисление рисков для модели и наглядность за счет представления итоговых значений в виде таблицы. Тем не менее, оценка на основании нечетких множеств (интервалов) крайне зависела от предварительной оценки экспертной группы, которая при определенных условиях могла быть неточной.

В 2017 г. Савченко С.О. и Капчук Н.В., описывая алгоритм построения модели нарушителя [10] использовали методы и понятия теории игр. Описание нарушителя безопасности было представлено как одноходовая матричная игра с нулевой суммой. В этой модели существует два игрока – нарушитель и защитник. Они знают все о действиях соперника, но не могут скооперироваться. Модель дополняется элементами теории вероятностей и теории графов. Модель практически в полной мере описывает поведение «игроков» и позволяет довольно точно оценивать защищенность системы. Но условие о полном знании действий оппонента, как и противоположное условие в методике Спивака А.И. в 2010 г., не позволяет рассматривать ситуации, противоречащие этому условию, например, ситуацию скрытного воздействия на систему [7].

В 2018 г. Гафизов Р.М. и Ахматзода Ш.А. при разработке модели нарушителя беспроводной сети [11] вводят в рассмотрение мотивы злоумышленника и классифицируют нарушителей. В зависимости от мотивации ими выделено четыре группы нарушителей:

– идейные хакеры, т. е. те, кто совершает атаки на конкретные системы, имея своими мотивами месть, вымещение обиды и пр.;

– искатели приключений: таких нарушителей не интересует содержание системы, в основном они хотят проверить свои способности;

– хакеры-профессионалы, т. е. злоумышленники с широким спектром умений, совершающие попытки НСД в систему по заказу;

– ненадежные сотрудники, т. е. внутренние нарушители по умыслу или без него вредящие системе.

Введение понятия мотивации в алгоритм рассмотрения модели злоумышленника приводит к более точному выдвижению гипотез относительно возможных действий нарушителя. Тем не менее модель не рассматривает возможные уровни доступа злоумышленника в системе, а именно – градацию возможных ненадежных сотрудников или нарушителей по техническому или логическому доступу. Это не позволяет в должной мере оценить его (злоумышленника) возможности.

Рассмотренные подходы к разработке модели и оценке деструктивных злоумышленных воздействий, не смотря на свою определенную значимость, не описывают в полной мере модель поведения и действий нарушителя каким-либо простым и понятным показателем, удобным для дальнейшего применения в оценке или разработке комплекса защитных мер. Предложенная ниже методика использует сильные стороны существующих алгоритмов, заполняет пробелы и убирает ряд допущений, ограничивающих функциональность при разработке, а также вводит обоснованную количественную величину, характеризующую уровень деструктивного воздействия нарушителя на систему.

**Методика и дискуссия**

Субъект КИИ – сложная, многокомпонентная система [12–14]. Рассматривать ее можно с точки зрения разных подходов. Например, при проведении комплексной оценки ИБ субъекта КИИ учитывается оценка защищенности ИС – объектов КИИ, которые, в свою очередь, можно рассматривать как экономические системы [15].

Еще один показатель при анализе функционирования субъекта КИИ – надежность. В [16] предлагается математическое обеспечение анализа надежности сетевых ИС. Данный аппарат также возможно использовать при исследовании объектов КИИ. В качестве модели сетевой ИС используется графовое

представление, основанное на формализации описания графа скобочными проекциями. На основе результирующей комбинации проекций, полученной в результате реализации алгоритма разрезания, строится вероятностная функция надежности.

Комплексное обеспечение информационной безопасности субъекта КИИ также является примером социотехнической системы, так как здесь важнейшие управляющие решения принимает человек [17]. Важно отметить, что данная система функционирует в условиях неопределенности, характеризуемой недостатком информации, необходимой для формализации процессов, протекающих в таких системах. С одной стороны, неопределенность обусловлена недостаточностью или полным отсутствием методов и средств измерения координат объекта управления в фазовом пространстве, а с другой – незнанием закономерностей протекания процессов ввиду их сложности и малой изученности. Обозначенные в [17] факторы затрудняют аналитическое описание и построение формальных моделей, учитывающих специфику социотехнических систем. Таким образом, с учетом особенностей слабоформализуемых процессов, происходящих в социотехнических системах, в частности в системе оценки информационной безопасности субъекта КИИ решено использовать методы когнитивного моделирования.

При рассмотрении вопросов, связанных с применением когнитивного моделирования ДЗВ на субъект КИИ, опора сделана на взгляды Н.П. Садовниковой, Н.П. Жидковой [18], отмечающих важность определения оптимальных требований к показателям, характеризующим качество принимаемых решений и необходимость учета сложного характера их взаимосвязей на основе существующих требований регуляторов. Для получения прогноза развития ситуации использован метод импульсных процессов [19], относящийся к категории динамических методов.

Основным понятием теории когнитивных карт является концепт $k$. Концептом называется базовый (неделимый) элемент рассматриваемой системы. Направленность связи концептов означает, что концепт-источник влияет на концепт-приемник, т. е. изменение значений (состояний) концепта-источника приводит к изменению значений (состояний) концепта приемника.

Когнитивная карта представляет собой ориентированный граф $G = (a, b)$, где $a$ – множество вершин графа (концепты); $b$ – множество ребер. Оптимизация когнитивной карты заключается в том, что она строится не на $n$ входных данных, а на $k$, где $k < n$; $n$ – величина компонента.

Когнитивная карта может быть преобразована в формализованную модель.

Процесс построения когнитивной модели состоит из ряда процедур:

1) выделение и обоснование системы факторов рисков безопасности функционирования субъекта КИИ, в наибольшей степени влияющих на стабильность функционирования и развития объектов, с целью включения таких факторов в разрабатываемую модель в качестве вершин ($V_i$);

2) установление экспертным путем наличия причинно-следственных связей (дуг $e_{ij}$) между выделенными факторами рисков и оценкой характера их влияния (положительного, отрицательного либо нулевого) друг на друга по отношению к задаче эффективного управления;

3) построение ориентированного графа, отражающего взаимовлияние факторов с учетом установленных экспертами весов дуг $w_{ij}$ из интервала от –10 до +10.

Основные источники факторов рисков в деятельности субъектов КИИ для построения когнитивной модели представлены в соответствии с Постановлением Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (с изменениями от 13.04.2019). Кроме того, в когнитивную модель введена целевая вершина V13 «Информационная безопасность субъекта КИИ», по результатам работы в которой будет оцениваться влияние ДЗВ на информационную безопасность субъекта КИИ.

В ходе моделирования строится когнитивная карта оценки ИБ субъекта КИИ при деструктивных воздействиях (рисунок 1). Для более глубокого анализа модели в виде взвешенного орграфа выстраивается алгоритм влияния изменения значений одной вершины на величины других вершин.

В основу данного алгоритма положена идея импульсного процесса, предложенную Робертсом Ф.С. Суть ее заключается в том, что в некоторую вершину анализируемого графа вносится внешнее возмущение.

Алгоритм развития импульсного процесса можно представить следующей матричной формулой:

$$V_{(t)} = V_{(\text{исх})} + P_0 * (I + A + A^2 + \cdots + A^t),$$

где $V_{(\text{исх})}$ – вектор начальных состояний; $P_0$ – начальный импульс; $A$ – матрица смежности; $I$ – единичная матрица размером $n \times n$.

В результате работы данного алгоритма получается количественная оценка информационной безопасности субъекта КИИ. Для перевода ее в качественную предлагается использовать шкалу качественной оценки уровня информационной безопасности субъекта КИИ (таблица 1).

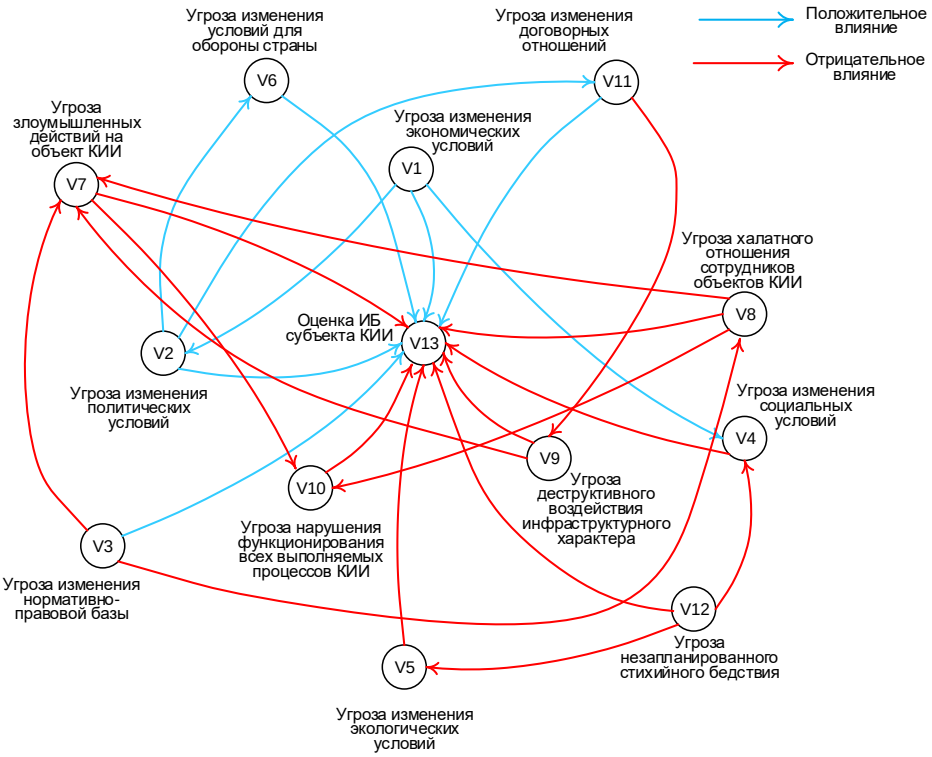


**Рис. 1. Когнитивная карта оценки ИБ субъекта КИИ при деструктивных воздействиях**

*Fig. 1. Cognitive Map of the Assessment of the Subject's IS CII in Case of Destructive Influences*

Оценка ДЗВ реализуется в модуле категорирования злоумышленника в модели когнитивной оценки ИБ субъекта КИИ при деструктивных воздействиях (рисунок 2). Для реализации данной оценки предлагается методика (см. далее).

**ТАБЛИЦА 1. Шкала качественной оценки уровня ИБ субъекта КИИ**

*TABLE 1. Scale of Qualitative Assessment of the IS Level of the Subject of the CII*

| Значение количественной оценки | Качественная оценка уровня ИБ субъекта КИИ |
|---|---|
| При положительном влиянии | |
| [0:0,33] | Низкая |
| [0,33:0,66] | Средняя |
| [0,66:1] | Высокая |
| При отрицательном влиянии (уровень снижения ИБ относительно исходного) | |
| [0:–0,33] | Незначительный |
| [–0,33:-0,66] | Значительный |
| [–0,66:-1] | Критичный |

Под деструктивным воздействием будем понимать результат реализации угрозы, приводящий к неблагоприятным и разрушительным последствиям для субъекта КИИ. Субъективным источником деструктивных воздействий является нарушитель ИБ. В качестве нарушителей информационной безопасности субъекта КИИ могут выступать лица, осуществляющие преднамеренные действия с целью доступа к информации, содержащейся на объектах КИИ. Исходя из особенностей структуры воздействия, целью воздействия в том числе может быть – нарушение функционирования объектов КИИ или обслуживающей ее инфраструктуры, имеющей доступ к объектам КИИ (преднамеренные угрозы безопасности информации), в соответствии с федеральным законом Российской Федерации № 187. При этом, достижимость нарушителем результата будет зависеть от ряда показателей. Совокупность этих показателей обеспечивает категорию нарушителя информационной безопасности.

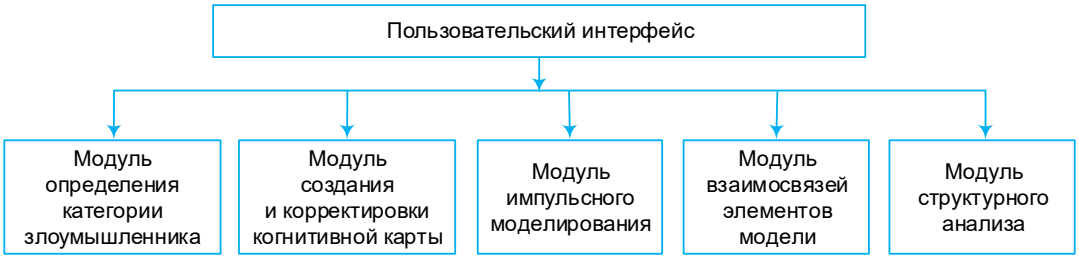


**Рис. 2. Архитектура модели оценки ИБ субъекта КИИ при деструктивных воздействиях**

*Fig. 2. Architecture of the IS Subject's is Assessment Model under Destructive Influences*

Таким образом, при моделировании действий нарушителя ИБ выстраивается формализованная модель, учитывающая параметры (потенциал) нарушителя в пространстве реализаций им деструктивных воздействий на объектах КИИ. Результатом моделирования здесь является пятиуровневая модель доступа нарушителя ИБ к информации и (или) к компонентам объектов КИИ на уровне физического доступа (PhL), логического доступа (LogL), компетенций (С) нарушителя, оснащенности (А) нарушителя, мотивации (М) нарушителя. Уровни доступа определяем согласно ПП РФ № 127 (с изменениями от 13.04.2019).

Возможности нарушителя на обозначенных уровнях доступа к информации и (или) к компонентам объектов КИИ определяют базовый потенциал ( $Pt_{BASE}$ ), которым обладает нарушитель ИБ на субъекте КИИ. Базовый потенциал используется для построения модели угроз ИБ в части оценки вероятностей их реализации. Оценка предварительного базового потенциала нарушителя производится на основе числовых значений уровней компетенции и оснащенности.

На основании вышеизложенного представим пятиуровневую модель доступа нарушителя ИБ к информации и (или) к компонентам объектов КИИ как:

$$\text{PhL:}[x]/\text{LogL:}[x]/\text{C:}[x]/\text{A:}[x]/\ /\text{M:}[x],$$

где $[x]$ – значение соответствующего параметра.

Предлагаемая методика основывается на оценке величины коэффициента ДЗВ, которая проводится в два этапа. На первом этапе определяется категория злоумышленника путем построения модели. На втором - выполняется оценка коэффициента ДЗВ на субъекте КИИ Модель злоумышленника на объекте КИИ представляет собой формальное описание потенциального нарушителя по пяти признакам, представленным выше. В общем виде модель категорирования нарушителя ИБ на объекте КИИ представима в нотации IDEF0 (рисунок 3).

Совокупность признаков определяет базовый потенциал злоумышленника при воздействии на объект КИИ. Для его оценки необходимо, во-первых, на основании числовых значений и уровня компетенции злоумышленника определить предварительный базовый потенциал с помощью таблицы 2.

**ТАБЛИЦА 2. Определение предварительного базового потенциала злоумышленника**

*TABLE 2. Determining the Preliminary Basic Potential of an Attacker*

| Показатель | Оценка [$x$] | |
|---|---|---|
| | Качественная (*qual*_[$x$]) | Количественная (*quan*_[$x$]) |
| Компетенции нарушителя | | |
| C:[$x$] | Низкий (LOW) | 0 |
| | Средний (AVERAGE) | 0,2 |
| | Высокий (HIGH) | 0,5 |
| Оснащенность нарушителя (оборудования) | | |
| A:[$x$] | Отсутствует (ABSENT) | 0 |
| | Стандартное | 0,1 |
| | Специализированное | 0,3 |
| | Заказное | 0,5 |

Предварительный базовый потенциал злоумышленника ($PREL\_Pt_{BASE}$) рассчитывается как:

$$quan\_[PREL_{Pt_{BASE}}] = quan\_C\text{:}[x] + quan\_A\text{:}[x].$$

В результате имеем:

$$(quan\_[PREL\_Pt_{BASE}] \geq 8) \Rightarrow (qual\_[PREL_{Pt_{BASE}}] := \text{HIGH}),$$

$$(quan\_[PREL_{Pt_{BASE}}] \geq 5)\text{V}(quan\_[PREL_{Pt_{BASE}}] < 8) \Rightarrow (qual\_[PREL_{Pt_{BASE}}] := \text{AVERAGE}),$$

$$(quan\_[PREL\_Pt_{BASE}] \geq 3)\text{V}(quan\_[PREL_{Pt_{BASE}}] < 5) \Rightarrow (qual\_[PREL_{Pt_{BASE}}] := \text{LOW}),$$

$$(quan\_[PREL_{Pt_{BASE}}] < 3) \Rightarrow (qual\_[PREL_{Pt_{BASE}}] := \text{ABSENT}).$$

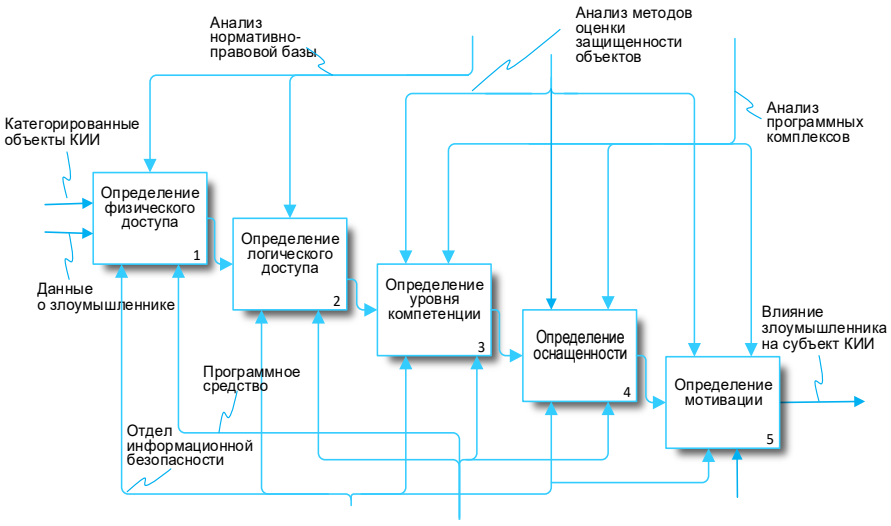


**Рис. 3. Модель категорирования нарушителя ИБ на объекте КИИ в нотации IDEF0**

*Fig. 3. Model for Categorizing an is Violator on a CII Object in IDEF0 Notation*

Последующая корректировка $PREL\_Pt_{BASE}$ производится в соответствии с таблицей 3.

**ТАБЛИЦА 3. Корректирующая матрица качественной оценки предварительного базового потенциала злоумышленника**

*TABLE 3. Corrective Matrix of Qualitative Assessment of the Preliminary Basic Potential of the Attacker*

| $quan\_[x]$/LogL | $qual\_PREL\_Pt_{BASE}$ | | | |
|---|---|---|---|---|
| | ABSENT | LOW | AVERAGE | HIGH |
| 0 | ABSENT | LOW | AVERAGE | HIGH |
| 1 | ABSENT | LOW | AVERAGE | HIGH |
| 2 | LOW | AVERAGE | HIGH | HIGH |
| 3 | LOW | AVERAGE | HIGH | HIGH |

Конечная корректировка $qual\_PREL\_Pt_{BASE}$ производится по следующим правилам:

$$(qual\_\text{M}: [x] := \text{AVERAGE}) \Rightarrow (qual\_Pt_{BASE} := +qual\_PREL\_Pt_{BASE}),$$

$$(qual\_\text{M}: [x] := \text{ABSENT}) \Rightarrow (qual\_Pt_{BASE} := -qual\_PREL\_Pt_{BASE}),$$

$$(qual\_\text{M}: [x] := \text{HIGH}) \Rightarrow (qual\_Pt_{BASE} := qual\_PREL\_Pt_{BASE}),$$

где знак «+» – переход на следующий уровень (переход от низкого или среднего на шаг выше); знак «–» означает переход на следующий уровень (переход от среднего или высокого на шаг ниже).

Для оценки коэффициента ДЗВ будем рассматривать три типа объектов КИИ (см. федеральный закон № 187):

– информационная система;

– информационно-телекоммуникационная система (ИТС);

– автоматизированная система управления (АСУ).

Для каждого объекта определим 3 возможных категории опасности при ДЗВ, где:

1 – наиболее опасный уровень нарушения функционирования;

3 – наименее опасный уровень нарушения функционирования.

Для каждого типа объектов расчет коэффициента ДЗВ производится в соответствии с таблицами 4–6.

В случае одновременного воздействия на объект КИИ нескольких злоумышленников (вариант воздействия «многие к одному» или «многие ко многим») возможны следующие ситуации:

1) выполняется согласованное деструктивное воздействие на 1 объект КИИ группой, состоящей из *n* злоумышленников;

2) выполняется не согласованное деструктивное воздействие на 1 объект КИИ группой, состоящей из *n* злоумышленников;

3) выполняется согласованное деструктивное воздействие на 1 объект КИИ группой, состоящей из *n* злоумышленников и не согласованное деструктивное воздействие на 1 объект КИИ группой, состоящей из *m* злоумышленников;

4) выполняется согласованное деструктивное воздействие на *k* объектов КИИ группой, состоящей из *n* злоумышленников;

5) выполняется не согласованное деструктивное воздействие на *k* объектов КИИ группой, состоящей из *n* злоумышленников;

6) выполняется согласованное деструктивное воздействие на *k* объектов КИИ группой, состоящей из *n* злоумышленников и не согласованное деструктивное воздействие на 1 объект КИИ группой, состоящей из *m* злоумышленников.

Для описания правил, по которым выполняется оценка коэффициента ДЗВ на субъекте КИИ введем обозначения:

*N*_CII – *N* объектов КИИ, подвергающиеся ДЗВ;

*M*_SV – *M* злоумышленников воздействуют на субъект КИИ;

$V[a]$ – вид взаимодействия между злоумышленниками, где $a$ соответствует выражению:

$$a = \begin{cases} 1, \text{если ДЗВ субъектно согласованны} \\ 0, \text{если ДЗВ субъектно не согласованны} \end{cases}.$$

**ТАБЛИЦА 4. Определение коэффициента деструктивного злоумышленного воздействия для ИС**

*TABLE 4. Determining the Coefficient of Destructive Malicious Influence for IS*

| $qual\_Pt_{BASE}$ | Категория объекта | | |
|---|---|---|---|
| | 3 | 2 | 1 |
| ABSENT | 0,1 | 0,1 | 0,1 |
| LOW | 0,2 | 2 | 0,3 |
| AVERAGE | 0,4 | 0,5 | 0,6 |
| HIGH | 0,7 | 0,8 | 0,9 |

**ТАБЛИЦА 5. Определение коэффициента деструктивного злоумышленного воздействия для ИТС**

*TABLE 5. Determining the Coefficient of Destructive Malicious Influence for ITS*

| $qual\_Pt_{BASE}$ | Категория объекта | | |
|---|---|---|---|
| | 3 | 2 | 1 |
| ABSENT | 0,1 | 0,1 | 0,1 |
| LOW | 0,1 | 0,1 | 0,2 |
| AVERAGE | 0,3 | 0,4 | 0,5 |
| HIGH | 0,6 | 0,7 | 0,8 |

**ТАБЛИЦА 6. Определение коэффициента деструктивного злоумышленного воздействия для АСУ**

*TABLE 6. Determining the Coefficient of Destructive Malicious Influence for the ASM*

| $qual\_Pt_{BASE}$ | Категория объекта | | |
|---|---|---|---|
| | 3 | 2 | 1 |
| ABSENT | 0,1 | 0,1 | 0,2 |
| LOW | 0,3 | 0,3 | 0,4 |
| AVERAGE | 0,5 | 0,6 | 0,7 |
| HIGH | 0,8 | 0,9 | 1 |

Так, правила оценки коэффициента ДЗВ на субъекте КИИ для работы в каждой из обозначенных ситуаций, можно представить в следующем виде.

Для ситуации 1 характерно [1]_CII, [$n$]_SV, V_[1]. Следовательно, имеем правило 1 для оценки коэффициента ДЗВ на субъекте КИИ:

$$(quan\_Pt_{BASE}[1,1] \mid (([1]\_CII) \wedge ([n]\_SV) \wedge (V\_[1]))) \Rightarrow (quan_{Pt_{BASE}} := \prod_{i=1,n} quan\_Pt_{BASE}[i]. \quad (1)$$

Для ситуации 2 характерно [1]_CII, [$n$]_SV, V_[0]. Следовательно, имеем правило 2 для оценки коэффициента ДЗВ на субъекте КИИ:

$$(quan_{Pt_{BASE}}[1,0] \mid (([1]\_CII) \wedge ([n]\_SV) \wedge (V\_[0])) \Rightarrow (quan\_Pt_{BASE} := quan\_Pt_{BASE}[\max\_weight[i]], \quad (2)$$

где $quan\_Pt_{BASE}[\max\_weight[i]]$ – количественная оценка потенциала злоумышленника, имеющего максимальную количественную оценку по показателю с максимальным весовым коэффициентом.

Для ситуации 3 характерно [1]_CII, [$n$]_SV и V_[1], и [$m$]_SV и V_[0]. Следовательно, имеем правило 3 для оценки коэффициента ДЗВ на субъекте КИИ:

$$(quan\_Pt_{BASE} \mid (([1]\_CII) \wedge (([n]\_SV) \wedge (V\_[1])) \wedge (([m]\_SV) \wedge (V\_[0])) \Rightarrow (quan_{Pt_{BASE}} := \max(\prod_{i=1.n} quan_{Pt_{BASE}}[i], \quad (3)$$

$$quan\_Pt_{BASE}[\max\_weight[i]].$$

Для ситуации 4 характерно [$k$]_CII, [$n$]_SV, V_[1]. Следовательно, имеем правило 4 для оценки коэффициента ДЗВ на субъекте КИИ:

$$(quan_{Pt_{BASE}}[k,1] \mid \mathrm{V}_{j=1}^{k}(([j,k]\_CII) \wedge ([j,s]\_SV) \wedge (V\_[1]))) \Rightarrow (quan\_Pt_{BASE} := \prod_{i=1,n} quan\_Pt_{BASE}[j,i], \quad (4)$$

где $j$ – номер объекта КИИ; $s$ – количество злоумышленников, воздействующих на $j$-ый объект КИИ.

В формуле (4) $quan\_Pt_{BASE}[j,i]$ рассчитывается по правилу 1 для ДЗВ по каждому объекту КИИ.

Для ситуации 5 характерно [$k$]_CII, [$n$]_SV, V_[0]. Следовательно, имеем правило 5 для оценки коэффициента ДЗВ на субъекте КИИ:

$$(quan_{Pt_{BASE}}[l,0] \mid \mathrm{V}_{j=1}^{k}(([j,k]\_CII) \wedge ([j,s]\_SV) \wedge (V\_[0]))) \Rightarrow (quan_{Pt_{BASE}}[j] := \max_{i=1.n} quan_{Pt_{BASE}}[j,i]. \quad (5)$$

Здесь $quan\_Pt_{BASE}[j,i]$ рассчитывается по правилу 1 для ДЗВ по каждому объекту КИИ.

Для ситуации 6 характерно [$k$]_CII, [$n$]_SV и V_[1], и [$m$]_SV и V_[0]. Следовательно, имеем правило 6 для оценки коэффициента ДЗВ на субъекте КИИ:

$$(quan_{Pt_{BASE}}[k,l] \mid (\mathrm{V}_{j=1}^{k}([j,k]_{\mathrm{CII}}) \wedge ([j,n]_{\mathrm{SV}}) \wedge (\mathrm{V}_{[1]})) \wedge \mathrm{V}_{j=1}^{l}(([j,l]_{\mathrm{CII}}) \wedge ([j,m]_{\mathrm{SV}}) \wedge (\mathrm{V}_{[0]})) \Rightarrow (quan_{Pt_{BASE}} := quan_{Pt_{BASE}}[k,1] * quan\_Pt_{BASE}[l,0]. \quad (6)$$

Здесь $quan\_Pt_{BASE}[k,1]$ рассчитывается по правилу 4, $quan\_Pt_{BASE}[l,0]$ – по правилу 5.

Использование представленных правил при построении когнитивной модели позволит спрогнозировать множество потенциально возможных ситуаций при построении модели ДЗВ и дать количественную оценку каждой ситуации в виде коэффициента ДЗВ на объект КИИ.

## Эксперимент

Исследование работоспособности когнитивной модели оценки ИБ субъекта КИИ при ДЗВ проводилось по результатам исследования изменений ИБ субъекта КИИ при различных видах деструктивных воздействий на объектах КИИ (таблица 7), что соответствует исследованию поведения вершины V9 в когнитивной модели. Если по результатам исследования ИБ субъекта КИИ будет находиться на низком уровне, то необходимо выбрать рекомендации к повышению уровня ИБ.

**ТАБЛИЦА 7. Планируемые эксперименты**

*TABLE 7. Planned Experiments*

| № эксперимента | Вершина – источник | Вершина получатель – V7 | | Отслеживаемая вершина | Потенциал нарушителя | Категория значимости объекта |
|---|---|---|---|---|---|---|
| | | Объект | Категория | | | |
| 1 | V9 | ИС | 3 | V13 | LOW | 1 |
| 2 | | ИС | 2 | | ABSENT | 3 |
| | | АСУ | 1 | | HIGH | 2 |
| 3 | | ИТС | 3 | | | 1 |
| | | ИСТ | 2 | | | 2 |
| | | АСУ | 1 | | | 3 |

Таким образом, исследование работоспособности предложенной модели выполнялось в ходе решения следующих задач:

– эксперимент № 1 «Исследование влияния деструктивных воздействий нарушителя с низким потенциалом на оценку ИБ субъекта КИИ, состоящего из объекта – ИС с 1 категорией значимости»;

– эксперимент № 2 «Исследование влияния деструктивных воздействий нарушителя без потенциала и с высоким потенциалом на оценку ИБ субъекта КИИ, состоящего из объекта – ИС с 3 категорией значимости и АСУ – 2 категории значимости при деструктивных воздействиях инфраструктурного характера»;

– эксперимент № 3 «Исследование влияния деструктивных воздействий нарушителей с высоким, средним и низким потенциалами на оценку ИБ субъекта КИИ, состоящего из объектов: ИС 2 категории значимости, ИТС – 1 категории и АСУ – 3 категории значимости при деструктивных воздействиях инфраструктурного характера».

В ходе экспериментального исследования построена когнитивная карта (рисунок 4).

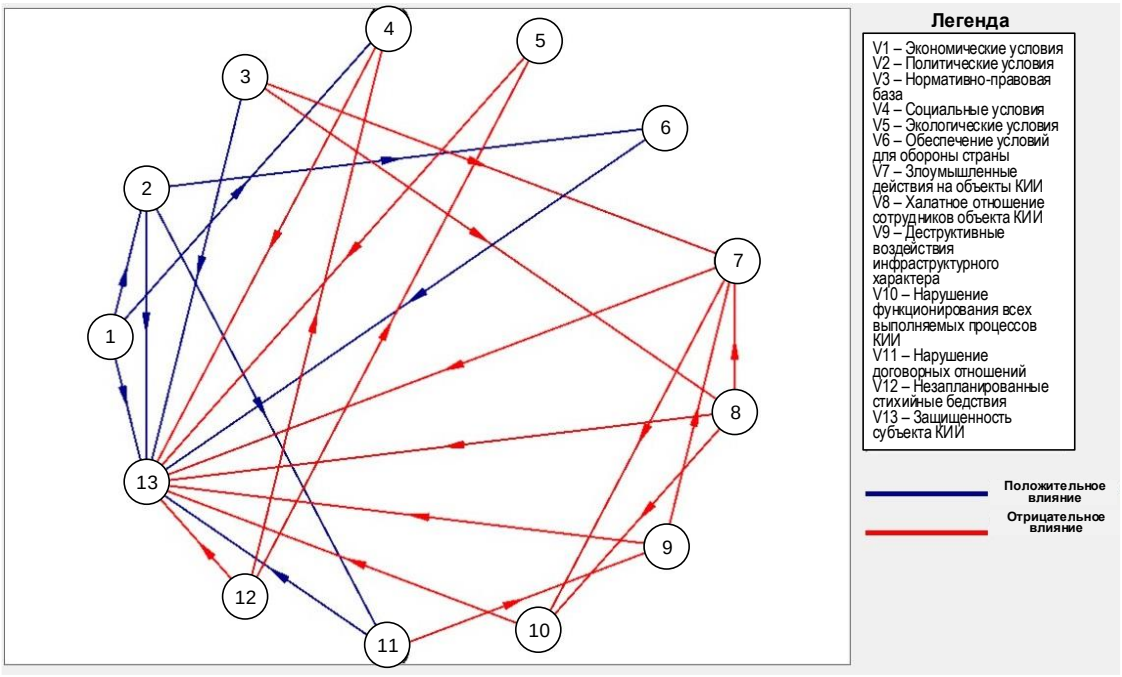


**Рис. 4. Построенная когнитивная карта оценки ИБ субъекта КИИ (экранная копия)**

*Fig. 4. Constructed Cognitive Map of the Subject's IS Assessment CII (Screen Copy)*

Результаты работы программного комплекса по решаемым задачам представлены на рисунке 5.

Методика работы с программным комплексом по оценке ИБ субъекта КИИ предполагает выполнение следующих шагов.

*Шаг 1*. Запуск программного средства выполняется из директории:

Ваш_диск:\Программа\kii\bin\Debug\kii.exe.

*Шаг 2*. Выбор категории злоумышленника из шаблона или задание значений проектировщиком.

*Шаг 3*. Оценка категории злоумышленника.

*Шаг 4*. Задание количества объектов и их категории.

*Шаг 5*. Корректировка работы по выбору объектов.

*Шаг 6*. В окне «Потенциал» выбор вида злоумышленника и установление для него сравнительного значения из окна «Категория».

*Шаг 7*. Оценка злоумышленных действий.

*Шаг 8*. Переход на вкладку «Построение когнитивной карты».

*Шаг 9*. Построение когнитивной карты.

*Шаг 10*. Визуализация когнитивной карты с легендой.

*Шаг 11*. Если построенная когнитивная карта не удовлетворяет пользователя – изменение положения вершин.

*Шаг 12*. Переход на вкладку «Построение когнитивной карты».

*Шаг 13*. Ввод значения вершин.

*Шаг 14*. Ввод количества шагов моделирования.

*Шаг 15*. Выбор вершины получателя.

*Шаг 16*. Выбор вершин для графической визуализации.

*Шаг 17*. Построение графика из выбранных вершин.

*Шаг 18*. Визуализация построенного графика по заданным вершинам.

Результаты экспериментов представлены в таблице 8.

**ТАБЛИЦА 8. Результаты экспериментального исследования работоспособности модели оценки ИБ субъекта КИИ при деструктивных воздействиях**

*TABLE 8. Results of an Experimental Study of the Performance of the IS SCII Assessment Model under Destructive Influences*

| № эксперимента | Вершина – источник | Вершина получатель – V7 | | Отслеживаемая вершина | Результат эксперимента | Оценка ИБ субъекта КИИ | Результат повторного эксперимента с учетом рекомендаций | Оценка ИБ субъекта после примененных рекомендаций |
|---|---|---|---|---|---|---|---|---|
| | | Объект/ категория объекта | Категория | | | | | |
| 1 | HIGH | ИС-1 | LOW | V13 | –0,45 | Значительный уровень снижения ИБ субъекта КИИ относительно исходного | 0,55 | Средний уровень ИБ |
| 2 | | ИС-3 | ABSENT | | –0,39 | | 0,71 | Средний уровень ИБ |
| | | АСУ-2 | AVERAGE | | | | | |
| 3 | | ИТС-1 | AVERAGE | | –0,40 | | 0,8 | Высокий уровень ИБ |
| | | ИС-2 | AVERAGE | | | | | |
| | | АСУ-3 | ABSENT | | | | | |

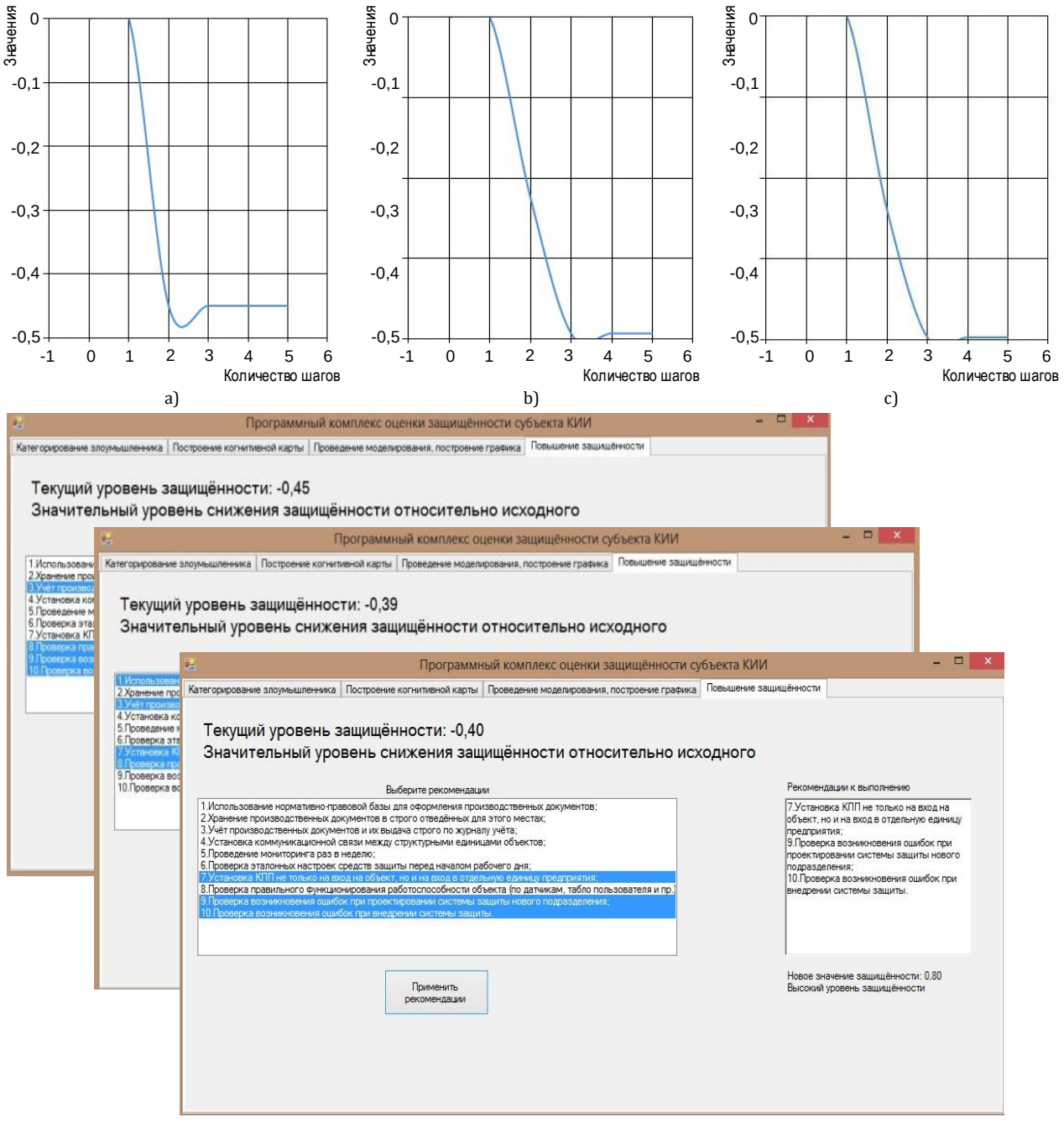


**Рис. 5. Результат эксперимента № 1 (a), эксперимента № 2 (b), эксперимента № 3 (c) и экранные копии окон выдачи рекомендаций и оценки уровня ИБ субъекта КИИ (d)**

*Fig. 5. Results of Experiment № 1 (a), Experiment № 2 (b), Experiment № 3 (c) and Screen Copies the Windows for Issuing Recommendations and Evaluating the Level of IBS (d)*

Диаграмма размещения вершин относительно импульсных процессов (рисунок 6) выстроена по результатам экспериментального исследования в формате SWOT-анализа. Использование данного формата эффективно при выполнении начальной оценки текущей ситуации в сфере ИБ на субъекте КИИ. Однако он не может заменить выработку стратегии или качественный анализ в динамике. Здесь возможно исследование ситуации, относительно которой нужно принять решение. При этом, полученные выводы могут иметь описательный характер без рекомендаций и определения целевых функций в стратегии.

Важно отметить, что предлагаемая когнитивная модель оценки деструктивных злоумышленных воздействий на объектах КИИ позволит снизить погрешность в оценки ИБ субъекта КИИ, следовательно, повысить эффективность системы защиты информации. Последнее, в свою очередь, будет достигаться за счет корректировки состава системы защиты, путем введения в нее механизмов предотвращения ДЗВ инфраструктурного характера.

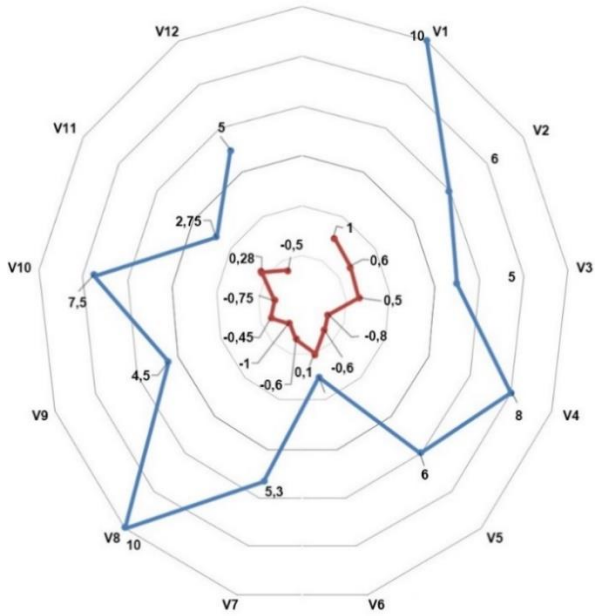


**Рис. 6. Диаграмма размещения вершин относительно импульсных процессов**

*Fig. 6. Diagram of Vertex Placement Relative to Pulse Processes*

**Выводы**

Таким образом, в ходе исследования проведена серия экспериментов, направленных на моделирование угроз, совершенных различными категориями злоумышленников на объекты КИИ. В результате работы, использование разработанной модели, позволило оценить ИБ субъекта КИИ при деструктивных воздействиях. Разработанный программный комплекс позволил провести категорирование злоумышленника, построить когнитивную карту оценки ИБ субъекта КИИ, смоделировать ДЗВ через различные вершины-источники, построить экспериментальные графики и представить рекомендации по повышению уровня ИБ субъекта КИИ. Предложенная модель и ее программная реализация могут стать активными помощниками для собственников объектов КИИ в процессе решения практических задач на всех этапах жизненного цикла субъекта КИИ. Для регуляторов – предлагаемый подход к оценке ИБ субъекта КИИ, позволит повысить достоверность предоставляемых собственниками объектов КИИ данных на этапе категорирования.

**БЛАГОДАРНОСТИ**

*Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ, проект № 3/2020).*

**Список используемых источников**

1. Yuill J., Wu F., Settle J., Gong F., Huang M. Intrusion-detection for incident-response, using a military battlefield-intelligence process // Computer Networks. 2000. Vol. 34. Iss. 4. PP. 671–697. DOI:10.1016/S1389-1286(00)00142-0

2. Jha S., Sheyner O., Wing J.M. Minimization and Reliability Analyses of Attack Graphs // CMU-CS-02-109. Pittsburgh: School of Computer Science Carnegie Mellon University, 2002.

3. Chi S.-D., Park J.S., Jung K.-C., Lee J.-S. Network Security Modeling and Cyber Attack Simulation Methodology // Proceedings of the 6th Australasian Conference on Information Security and Privacy on Information Security and Privacy (Sydney, Australia, 11–13 July 2001). Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2001. Vol. 2119. DOI:10.1007/3-540-47719-5_26

4. Базовая модель угроз персональных данных при их обработке в информационных системах персональных данных. Москва, 2008. URL: https://fstec.ru/component/attachments/download/289 (дата обращения 29.10.2020)

5. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. М.: Военное издательство, 1992.

6. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности. № 149/7/2/6-432 от 31.03.2015.

7. Бояринцев А.В., Ничиков А.В., Редькин В.Б. Общий подход к разработке моделей нарушителей // Системы безопасности. 2007. № 4. С. 50–53.

8. Спивак А.И. Оценка эффективности атак злоумышленника в процессе построения его модели // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2010. № 2(66). С. 108–112.

9. Жуков В.Г., Жукова М.Н., Стефаров А.П. Модель нарушителя прав доступа в автоматизированной системе // Программные продукты и системы. 2012. № 2(98). С. 75–78.

10. Савченко С.О., Капчук Н.В. Алгоритм построения модели нарушителя в системе информационной безопасности с применением теории игр // Динамика систем, механизмов и машин. 2017. Т. 5. № 4. С. 84–89. DOI:10.25206/2310-9793-2017-5-4-84-89

11. Гафизов Р.М., Ахматзода Ш.А. Разрабока модели нарушителя беспроводной сети // Инновации в науке. 2018. № 12(88). С. 10–12.

12. Максимова Е.А. Исследование алгоритмов безопасной передачи данных между объектами критической информационной инфраструктуры // XXIII пленум ФУМО ВО ИБ и Всероссийской научной конференции «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (Ставрополь, Россия, 1–5 октября 2019). Ставрополь: Северо-Кавказский федеральный университет, 2019. С. 157–163.

13. Шихвердиева А.Ш., Максимова Е.А. Управление эксплуатацией объектов критической информационной инфраструктуры // XVI Всероссийская школа-конференция молодых ученых «Управление большими системами» (Тамбов, Россия, 10–13 сентября 2019). Тамбов: Тамбовский государственный технический университет, 2019. С. 392–397.

14. Баранов В.В., Максимова Е.А., Лаута О.С. Анализ модели информационного обеспечения процессов и систем при реализации многоагентного интеллектуального взаимодействия // Приборы и системы. Управление, контроль, диагностика. 2019. № 4. С. 32–41.
15. Тищенко Е.Н. Анализ защищенности экономических информационных систем: монография. Ростов н/Д: М-во образования Рос. Федерации. Рост. гос. экон. ун-т, 2003. 191 с.
16. Громов Ю.Ю., Елисеев А.И., Минин Ю.В., Сумин В.И. Анализ надежности в сетевых информационных системах // Вестник Воронежского института ФСИН России. 2018. № 1. С. 33–41
17. Ажмухамедов И.М. Управление слабоформализуемыми социотехническими системами на основе нечеткого когнитивного моделирования (на примере систем комплексного обеспечения информационной безопасности). Дис. … докт. техн. наук. Астрахань: Астраханский государственный технический университет, 2014.
18. Садовникова Н.П., Жидкова Н.П. Выбор стратегий территориального развития на основе когнитивного анализа и сценарного моделирования // Интернет-Вестник ВолгГАСУ. 2012. № 7(21).
19. Робертс Ф.С. Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам / пер. с англ. М.: Наука, 1986. 496 с.
20. Дроботун Е.Б., Цветков О.В. Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действий нарушителя // Программные продукты и системы. 2016. № 3. С. 42–50. DOI:10.15827/0236-235X.115.042-050

* * *

# Cognitive Modeling of Destructive Malicious Impacts on Critical Information Infrastructure Objects

**E. Maksimova**[1]

[1]MIREA – Russian Technological University,
Moscow, 119454, Russian Federation

**Article info**
DOI:10.31854/1813-324X-2020-6-4-91-103
Received 21st September 2020
Accepted 20th October 2020

**For citation:** Maximova E. Cognitive Modeling of Destructive Malicious Impacts on Critical Information Infrastructure Objects. *Proc. of Telecom. Universities.* 2020;6(4):91–103. (in Russ.) DOI:10.31854/1813-324X-2020-6-4-91-103

**Abstract:** *The security of a subject of critical information infrastructure (CII) is one of the key issues of its life support. The current approach (legal and regulatory) regulates solutions of this issue without taking into account the influence of the violator, which can have a destructive effect on the SCII. This, in our opinion, leads to significant errors in the analysis of the information security of the CII, therefore, reduces the effectiveness of the information protection means declared information security tools for CII objects. The purpose of this work is to develop a model of an information security (IS) intruder, presented in a formalized form using the "violator's potential" parameter in the space of their implementation of destructive effects on the objects of the CII. The proposed model for assessing the capabilities of the offender to implement destructive influences on the CII subject as a set of objects is implemented in the developed cognitive map "Assessment of the IB of the CII Subject" for dynamic changes in the parameters of the "Malicious actions on the CII object" vertex.*

**Keywords:** *violator, subject, critical information infrastructure, category, destructive effects, model, cognitive model.*

**References**

1. Yuill J., Wu F., Settle J., Gong F., Huang M. Intrusion-detection for incident-response, using a military battlefield-intelligence process. *Computer Networks*. 2000;34(4):671–697. DOI:10.1016/S1389-1286(00)00142-0
2. Jha S., Sheyner O., Wing J.M. *Minimization and Reliability Analyses of Attack Graphs. CMU-CS-02-109*. Pittsburgh: School of Computer Science Carnegie Mellon University; 2002.
3. Chi S.-D., Park J.S., Jung K.-C., Lee J.-S. Network Security Modeling and Cyber Attack Simulation Methodology. *Proceedings of the 6th Australasian Conference on Information Security and Privacy on Information Security and Privacy, 11–13 July 2001, Sydney, Australia. Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer; 2001. vol.2119. DOI:10.1007/3-540-47719-5_26

4. *Basic model of threats to personal data during their processing in personal data information systems.* Moscow; 2008. (in Russ) Available from: https://fstec.ru/component/attachments/download/289 [Accessed 29th October 2020]

5. State Technical Commission of Russia. *Guidance document. Protection against Unauthorized Access to Information. Terms and Definitions*. Moscow: Voennoe izdatelstvo Publ.; 1992. (in Russ.)

6. *Methodological Recommendations for the Development of Regulatory Legal Acts that Determine Threats to the Security of Personal Data, Relevant When Processing Personal Data in Personal Data Information Systems Used in the Implementation of Relevant Activities*. Approved by the Leadership of the 8th Center of the Federal Security Service of Russia. No. 149/7/2/6-43, 31st March 2015. (in Russ.)

7. Boyarintsev A.V., Nichikov A.V., Redkin V. B. General Approach to the Development of Models of Violators. *Security and Safety*. 2007;4:50–53. (in Russ.)

8. Spivak A. The Efficiency Estimation of the Intruder Attacks in the Process of His Model Creation. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics of ITMO University*. 2010;2(66):108–112. (in Russ.)

9. Zhukov V.G., Zhukova M.N., Stepanov A.P. Model of Access Rights Violator in an Automated System. *Software & Systems.* 2012;2(98):75–78 (in Russ.)

10. Savchenko S.O., Kapchuk N.V. Algorithm for Constructing the Intruder Model in the Information Security System Using Game Theory. *Dynamics of Systems, Mechanisms and Machines*. 2017;5(4):84–89. (in Russ.) DOI:10.25206/2310-9793-2017-5-4-84-89

11. Khafizov R.M., Ahmadzade S.A. Development of a Model of a Wireless Network. *Innovatsii v nauke*. 2018;12(88):10–12. (in Russ.)

12. Maksimova E.A. Study of Algorithms for Secure Transmission of data between the objects of Critical Information Infrastructure. *Proceedings of the XXIII Plenum of the Fundamental Problems of Information Security in the Context of Digital Transformation and the All-Russian Scientific Conference, 1–5 October 2019, Stavropol, Russia*. Stavropol: North Caucasus Federal University Publ.; 2019. p.157–163. (in Russ.)

13. Shahverdiev A.S., Maksimova E.A. Management of Operation of Critical Information Infrastructure's Objects. *Proceedings of the XVI All-Russian School-Conference of Young Scientists on Management of Large Systems, 10–13 September 2019, Tambov, Russia*. Tambov: Tambov State Technical University Publ.; 2019. p.392–397. (in Russ.)

14. Baranov V.V., Maximova E.A., Lauta O.S. Analysis of the Model of Information Support of Processes and Systems in the Implementation of Multi-Agent Intellectual Interaction. *Instruments and Systems: Monitoring, Control, and Diagnostics*. 2019;4:32–41. (in Russ.)

15. Tishchenko E.N. *Analysis of Security of Economic Information Systems*. Rostov on Don: Ministry of Education of the Russian Federation. Rostov State Economic University Publ.; 2003. 191 p. (in Russ.)

16. Gromov Yu.Yu., Eliseev A.I., Minin Yu.V., Sumin, V.I. Analysis of Reliability in Network Information Systems. *Vestnik of Voronezh Institute of the Russian Federal Penitentiary Service*. 2018;1:33–41. (in Russ.)

17. Azhmukhamedov I.M. *Management of Weakly Formalized Sociotechnical Systems Based on Fuzzy Cognitive Modeling (on the Example of Integrated Information Security Systems).* D.Sc. Thesis. Astrakhan: Astrakhan State Technical University Publ.; 2014. (in Russ.)

18. Sadovnikova N.P., Zhidkova N.P. Selection of Territorial Development Strategies Based on cognitive analysis and Scenario Modeling. *Internet-Vestnik VolgGASU*. 2012;7(21) (in Russ.)

19. Roberts F.S. Discrete Mathematical Models with Applications to Social, Biological and Environmental Problems. Moscow: Nauka Publ.; 1986. 496 p. (in Russ.)

20. Drobotun E.B., Tsvetkov O.V. Modeling Information Security Threats in the Automated Control System for Crucial Objects on the Basis of Attack Scenarios. *Software & Systems.* 2016;3:42–50. (in Russ.) DOI:10.15827/0236-235X.115.042-050

## Сведения об авторе:

**МАКСИМОВА Елена Александровна**

кандидат технических наук, доцент кафедры «Прикладные информационные технологии» (КБ-2) института Комплексной безопасности и специального приборостроения МИРЭА – Российского технологического университета, maksimova@mirea.ru

https://orcid.org/0000-0001-8788-4256